सत्यमेव जयते
NITI Aayog

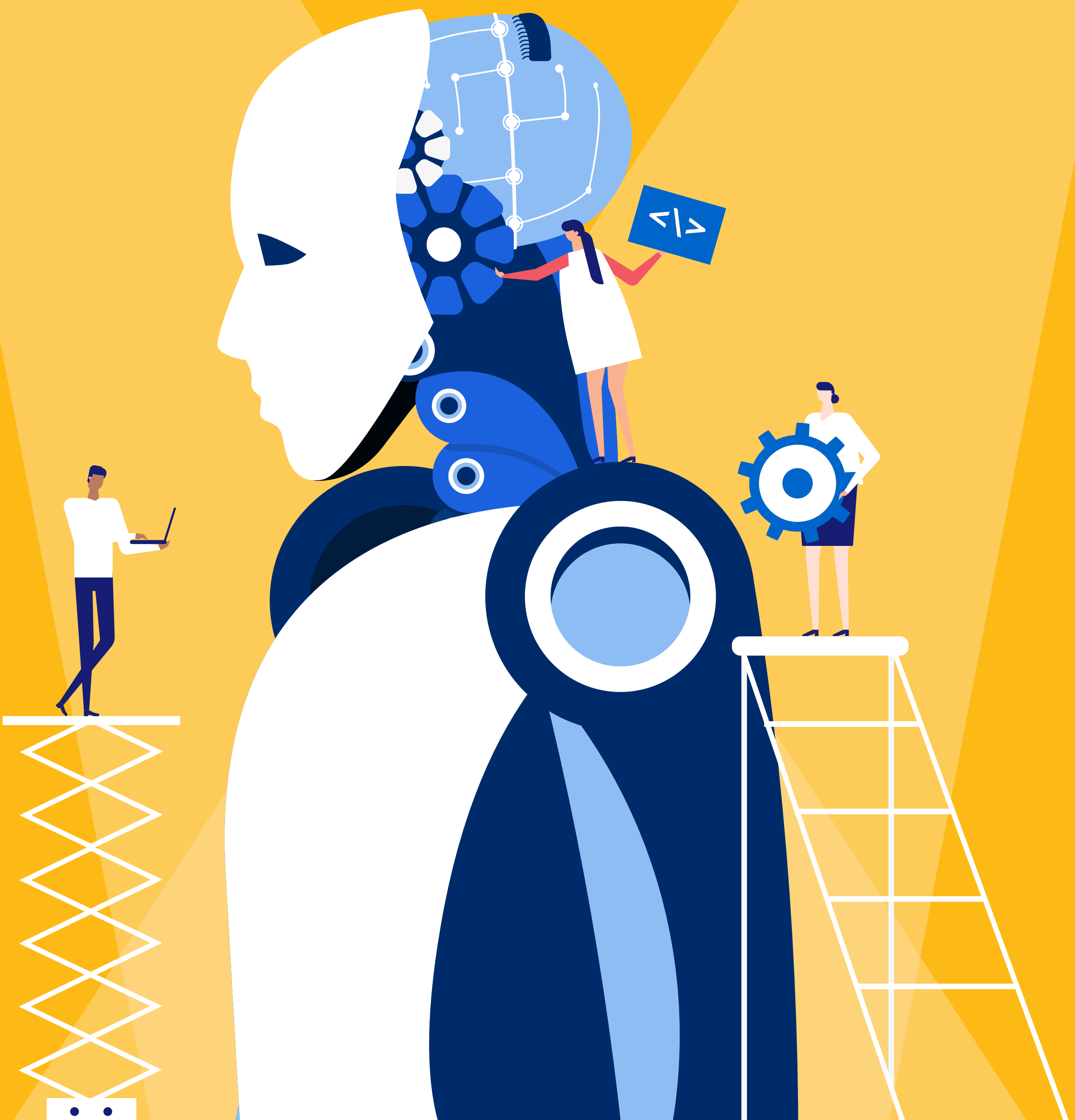
In the series of its publication on Responsible Artificial Intelligence (RAI), NITI Aayog brings the third paper titled "Responsible AI for All: Adopting the Framework – A use case approach on Facial Recognition Technology".

This draft discussion paper is being released for seeking public comments. Comments may be sent on or before 30th November 2022 addressed to Anna Roy, Senior Adviser, NITI Aayog at the email id adviserdma-niti@gov.in

RESPONSIBLE AI
#AIForAll

Adopting the Framework: A Use Case Approach on Facial Recognition Technology

Discussion Paper | November 2022



सत्यमेव जयते

NITI Aayog

RESPONSIBLE AI #AIFORALL

Adopting the Framework: A Use Case Approach on Facial Recognition Technology

DISCUSSION PAPER

November 2022

ACKNOWLEDGEMENTS

We are pleased to have collaborated with Vidhi Centre for Legal Policy as the Knowledge Partner in developing the document where the principles and mechanisms of Responsible AI from the previous publications have been tested out in the first use-case concerning Facial Recognition Technology. The valuable contributions of Mr. Ameen Jauhar, Ms. Jai Vipra, Mr. Dhruv Somayajula and Ms. Trishee Goyal from the Vidhi Centre of Legal Policy are acknowledged.

In writing this report, Responsible AI for All: Adopting the Framework – A use case approach on Facial Recognition Technology, Saurabh Thukral and Rishabh Bezbaruah from NITI Aayog has made valuable contributions.

We are also grateful for the support and contributions of several experts from India and globally including Dr. Anand S. Rao from PwC and Mr. Rohit Satish from ArtPark. Valuable inputs were also provided by various Ministries/ Departments of the Government of India and regulatory Institutions, namely, the Ministry of Civil Aviation, the Ministry of Home Affairs, the Ministry of Electronics & Information Technology, the Department of Science & Technology, the Office of the Principal Scientific Adviser to the Government of India, and the Unique Identification Authority of India.

ARoy

Anna Roy
Senior Adviser
NITI Aayog

LIST OF ABBREVIATIONS

AFRS	Automated Facial Recognition System
AHRC	Australian Human Rights Commission
AI	Artificial Intelligence
AIA	Proposed AI Act, 2021
API	Application Programming Interface
APP	Australian Privacy Principles
BBS	Biometric Boarding System
CISF	Central Industrail Security Force
DY	Digi Yatra
DYCE	Digi Yatra Central Ecosystem
DYCIMP	Digi Yatra Central Identity Management Platform
DYF	Digi Yatra Foundation
ECHR	European Convention on Human Rights
EU	European Union
FRT	Facial Recognition Technology
FTC	Federal Trade Commission
FVT	Facial Verification Technology
GDPR	General Data Protection Regulations
ICO	Information Commissioner's Office
INPOL-Z	Informationssystem der Polizei (Police Information System, Germany)
LFRT	Live Facial Recognition Technology
LIME	Local Interpretable Model-agnostic Explanations

NSAI	National Strategy on Artificial Intelligence
OAIC	Office of the Australian Information Commissioner
OTA	Online Travel Agency
PAIS	Punjab Artificial Intelligence System
PBD	Privacy by Design
PDP	Personal Data Protection Bill
PIPEDA	Personal Information Protection and Electronic Documents Act
RAI	Responsible AI
RFP	Request for Proposal
SITA	Société Internationale de Télécommunications Aéronautiques
SOP	Standard Operating Procedures
SPDI	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data and Information) Rules, 2011
SSI	Self-Sovereign Identity
VC	Verifiable Credential

CONTENTS

EXECUTIVE SUMMARY

In 2018, NITI Aayog released the National Strategy on Artificial Intelligence **(NSAI)**, that inter alia highlighted the roadmap to adopt AI in five public sectors in a manner that is safe and dispenses benefits to all citizens. The strategy document coined the "AI for All" mantra, to be the governing benchmark for future AI design, development, and deployment in India. A part of this strategy was to ensure the safe and responsible use of AI.

As a follow-up to NSAI, stakeholder consultations were initiated in collaboration with the World Economic Forums in 2019 on the proposed approach for responsible use of emerging technologies. This culminated in 2021, with the release of a two-part approach paper, identifying principles for responsible design, development, and deployment of artificial intelligence (AI) in India, and setting out enforcement mechanisms for the operationalisation of these principles **(RAI principles)**. These RAI principles come in the background of a growing call for developing governance and regulatory frameworks to mitigate potential risks of AI, while maximising its benefits for the largest number of people. As the next steps the seven principles, i.e., safety and reliability, inclusivity and non-discrimination, equality, privacy and security, transparency, accountability, and protection and reinforcement of positive human values, and the proposed needs to be tested out in a use case to determine the efficacy of the approach recommended and identify challenges thereon.

Facial recognition technology **(FRT)** has been taken as the first use case for examining the RAI principles and operationalisation mechanism proposed earlier.

FRT has garnered domestic and international debate around its potential benefits of efficient and timely execution of existing processes in different sectors; yet also the risks it poses to basic human and fundamental rights like individual privacy, equality, free speech and freedom of movement, to name a few. In India, as part of its efforts to improve travel experience, the Ministry of Civil Aviation has initiated the Digi Yatra programme under which FRT, and facial verification technology **(FVT)** will be used at different process points. FVT will be used at different airports for the purpose of identity verification of travellers, ticket validation, and any other checks as needed from time to time, based on operational needs of the airport processes. The stated objectives behind this move are to create a seamless, paperless, and contactless check-in and boarding experience for passengers.

Given the risks affiliated with FRT applications in general, the Digi Yatra programme presents an interesting use case of this technology to determine how the governments can adhere to its stated objective of responsible and safe deployment of AI and algorithmic systems. This paper will delve deeper into the framework for Digi Yatra and the processes that have been prescribed for operationalising it. It will examine these with the intent of evaluating their success in terms of meeting the aforementioned RAI principles and determining actionable next steps which can further augment the programme's compliance with these ethical benchmarks. The paper also puts forth recommendations for applications of FRT within India.

INTRODUCTION

INTRODUCTION

In an increasingly technology centric society, the surge in designing and development of artificial intelligence **(AI)** driven tech is becoming ubiquitous. Featuring in a wide array of sectors ranging from agriculture to education, AI is metaphorically and literally reengineering our lifestyles. While the origins of AI are traceable to the second half of the twentieth century, the past decade has witnessed a rapid resurgence. This is attributable, in large part, to Big Data analytics - data collection, aggregation and processing, which has spurred the growth of sophisticated technologies through techniques such as machine learning, deep learning, neural networks, natural language processing, etc.

The other side of this technological revolution is a growing apprehension on the socio-political and economic implications of AI. Specifically, there are concerns about the concomitance between these emerging technologies and core principles of modern democracies. In this context, conversations around AI ethics and the safe and responsible application of AI are becoming front and centre. In India, NITI Aayog published the seminal document enunciating India's national strategy towards harnessing the potential of AI while being mindful of its numerous pitfalls.[1] This was followed by two additional approach papers published last year, discussing how AI ethics can be conceptualised in the Indian context. Constitutional morality was envisioned as the cornerstone for AI ethics' principles in India, thus, propelling our constitutional rights and ethos to the paramount consideration for deploying AI in a responsible manner.[2]

Having established the core ethical principles, it is now crucial to examine how these get addressed in specific use cases of AI within the overall RAI

[1] *Niti Aayog, 'National Strategy for Artificial Intelligence' Discussion Paper (June 2018) <https://indiaai.gov.in/documents/pdf/NationalStrategy-for-AI-Discussion-Paper.pdf> accessed 10 November 2021*

[2] *Niti Aayog, 'Approach Document for India Part 1 – Principles for Responsible AI' (February 2021) <https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf> accessed 10 November 2021*

framework. This Paper is the third paper in the series being published by NITI Aayog, establish a framework for responsible and safe development and deployment of facial recognition technology **(FRT)** within India. FRT is a collective term referring to different kinds of technologies that are designed to identify or trace individuals using visual images (mostly in either videos or pictorial formats). The underlying algorithm in a garden variety FRT is designed and trained on large corpuses of digital images sourced from CCTV footage, the internet, existing repositories of images (especially with governmental agencies), and other sources. FRT uses key features of the face and their respective distances from one another to morph a virtual facial map.[3]

The use of FRT has witnessed a significant debate globally around its ethical, legal, and constitutional ramifications. At the same time, it has the benefits that any automation brings, which is to expedite manual efforts with more efficiency in processes. Nonetheless, given India's unequivocal commitment to pursue any AI development in a responsible manner, which aligns with constitutional tenets, it is imperative to carve out clear checks and balances on the use of FRT.

Pursuing this balance, the current Paper will examine how principles of AI ethics can be converged with the application of FRT in India. The use should be with due consent and should be voluntary, at no time should FRT become mandatory. It should further be limited to instances where both public interest and constitutional morality can be in sync. Enhanced efficiency of automation should *per se* not be deemed enough to justify the usage of FRT. For purposes of a more focussed examination the Paper will study the ongoing use of FRT in case of a specific project which is being implemented, viz. *Digi Yatra* project that envisages to streamline the passenger travel at airports. The Paper is divided into two parts:

Part 1: In this segment general risks around AI, specifically those emanating from the use of FRT, will be presented giving cross-jurisdiction regulatory overview of different countries and regions instituting laws or policies to govern FRT usage. It will also present use cases of FRT in India and the experience of different states regarding its implementation. The segment is divided into five Sections.

Section 1 maps out the prevalent discussions on ethical concerns raised by AI use. Section 2 discusses FRT as a concept, explaining how FRT operates, the factors contributing to a rise in deployment in recent years, and the broad use-case purposes. Section 3 reports on several FRT systems deployed in India and internationally, across various purposes by government agencies. Section 4 discusses the specific design-based risks and rights-based risks

[3] *Ameen Jauhar, 'Facing up to the risks of automated FRT in Indian law enforcement' (2020) Indian Journal of Law & Technology (NLSIU) Vol. 16(1), at 1-15*

emanating from use of FRT systems. Section 5 discusses the regulatory approaches adopted by various international jurisdictions to counter these risks and highlights key regulatory best practices.

Part 2: This segment of the Paper provides a deep dive into the Digi Yatra programme (**'Digi Yatra'**) with focus on its usage of FRT. Digi Yatra is a proposed biometric boarding system for use at Indian airports, intended to create a seamless, paperless, and contactless check-in and boarding experience for passengers. Digi Yatra envisages an identity management ecosystem for Indian airports which can enhance the capabilities of Indian civil aviation infrastructure, digitise manual processes at airports, improve security standards and lower the cost of operations of airports. The focus of this part is on the analysis of the Digi Yatra ecosystem from the perspective of principles of Responsible AI and Digi Yatra's risk mitigation measures.

Recommendations are also made with respect to law and policy, as well as institutional interventions necessary to ensure responsible and safe usage of FRT both specific - at Indian airports - and generally in any other use case of FRT.

The sections in Part 2 will delve into these perspectives in detail and highlight the corresponding risks and mitigation strategies present in the Digi Yatra ecosystem. *First*, it sets out the constituent elements of the Digi Yatra ecosystem by examining the passenger processes, technical aspects and legal aspects of Digi Yatra. *Second*, it utilises the principles of responsible AI, systemic risk considerations and the measures proposed within Digi Yatra to mitigate these risks.4. *Finally,* it sets out some actionable recommendations to guide the implementation of similar FRT systems in a responsible manner at a larger scale, which will maximise its potential and mitigate the risks therein to a minimum.

[4] *NITI Aayog, 'Approach Document for India: Part 2 - Operationalizing Principles for Responsible AI ' (August 2021) Responsible AI <https://www.niti.gov.in/sites/default/files/2021-08/Part2-Responsible-AI-12082021.pdf> accessed 20 February 2022*

PART I

I. RESPONSIBLE AI

Over the years, the rise in technological innovations has corresponded with the rise in computational capabilities of computers. First generation computers had programs that were implemented by humans. However, the rise of computation has led to the development of algorithms - essentially a set of instructions to perform a calculation or solve a problem that can be implemented by a computer, and key to all AI systems.[5] The rise in algorithmic abilities brings us to the present-day scenario, where an AI system can interpret a set of instructions and is capable of deciphering the required output function it needs to perform. These algorithms are trained on massive datasets, i.e., training datasets, which provide it with a certain amount of input information and output information allowing it to recognize the tasks required to be performed to generate an output based on future real-world inputs. However, its ability to self-implement instructions and carry out these functions based on its training presents us with unique ethical considerations applicable to the use of AI systems in various capacities. The increasing use of AI and algorithmic functions in both the public and the private sectors, elaborated further in this Paper, necessitate a discussion on the ethical risks emanating from these use cases. An examination into these ethical concerns over the use of AI systems is not new in India. In 2021, NITI Aayog conducted a comprehensive overview of AI ethics that discusses the need for an ethics-based review of AI deployment, keeping in mind issues such as opacity, reliability, interpretability, equality, algorithmic bias, exclusions, accountability and privacy.[6]

[5] *World Economic Forum, 'A Policy Framework for Responsible Limits on Facial Recognition: Use Case: Law Enforcement Investigations' (October 2021) White Paper, pp. 26*

[6] *Niti Aayog, 'Approach Document for India Part 1 – Principles for Responsible AI' (February 2021) <https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf> accessed 10 November 2021; Niti Aayog, 'Approach Document for India: Part 2 - Operationalizing Principles for Responsible AI' (August 2021) <https://www.niti.gov.in/sites/default/files/2021-08/Part2-Responsible -AI-12082021.pdf> accessed 10 November 2021*

II. FRT AS A CONCEPT

FRT refers to an AI system that allows identification or verification of a person based on certain images or video data interfacing with the underlying algorithm.[7] In terms of personal identification or verification, the use of FRT is set apart from other instruments of gathering or verifying biometric data as faces, or facial image data, can be captured and processed at a remote distance, including through covert means.[8] This Paper seeks to discuss the use of FRT by public authorities for verification and identification purposes, and the consequences of this use.

A. How does FRT operate?

FRT is a sophisticated data-driven aspect of artificial intelligence technology that primarily seeks to accomplish three functions- facial detection, feature extraction, and facial recognition.[9] FRT applications generally operate through the identification or verification of particular persons against a gallery of facial images, necessitating the presence and use of large facial datasets for wider use. This ecosystem is further dependent on the availability of facial data as the FRT programs, prior to their rollout, are engaged in intensive training and machine learning processes through large amounts of training datasets.[10] The availability of large datasets of previously accumulated facial data is key to the operation of FRT applications.

[7] *Smriti Parsheera, 'Adoption and regulation of facial recognition technologies in India: Why and why not?' (November 2019) Data Governance Network, Working Paper 05*

[8] *Andrew W. Senior, Sharath Pankanti, 'Privacy protection and face recognition' in Stan Li, Anil Jain (eds), Handbook of Facial Recognition Technology (Ch. 3.1.1, Springer 2011)*

[9] *Shahina Anwarul, Susheela Dahiya, 'A Comprehensive Review on Face Recognition Methods and Factors Affecting Facial Recognition Accuracy' P. K. Singh et al. (eds) (2020) Proceedings of ICRIC 2019 <https://www.researchgate.net/publication/337446642_A_Comprehensive_Review_on_Face_ Recognition_Methods_and_Factors_Affecting_Facial_Recognition_Accuracy> accessed 18 December 2021*

[10] *Priya Vedavalli et al, 'Facial Recognition Technology in Law Enforcement in India: Concerns and Solutions' (2021) Data Governance Network, Working Paper 16*

Facial detection relies on the use of algorithms to be able to detect the presence of a human face within an image. This by itself allows the application of certain technologies that are agnostic to the specific features of a face and are only concerned with the existence of a face detected within an image. However, in most instances of FRT use, facial detection is merely a first step, to be followed by feature extraction and facial recognition if necessary. Feature extraction is the use of mathematical representations of distinctive features on individual faces identified in the first stage to have unique identifiers between different faces. Lastly, the stage of facial recognition involves the automatic cross-referencing of a person's facial features with a pre-existing database of images called a gallery dataset.

This facial recognition function of FRTs is broadly used in two formats, 1:1 FRT systems and 1:n FRT systems.[11] In a 1:1 system, FRT is mainly targeted at authenticating or verifying a specific person's facial data (which is captured live) with a specific facial image data from a gallery dataset.[12] This is broadly seen in scenarios of authentication, such as the unlocking of phones or the requirement to authenticate faces prior to receiving certain public services. As can be seen, 1:1 systems exercise identification through authentication between two specific faces, and greater control over the quality of facial images taken both at the time of compiling the gallery dataset and at the time of authentication provides for greater accuracy with lesser factors that impede verification.[13] On the other hand, 1:many systems of FRT are primarily used in identification i.e., to process a large number of faces captured in either image or video format to specifically identify a particular person's face.[14] The 1:many systems are mostly used in live facial recognition technology (LFRT) applicable to law enforcement, and other mass monitoring and surveillance purposes.[15]

Pertinently, while in 1:1 systems the participants are likely to be aware of their image being captured at the time of authentication, this is usually not the case

[11] *Major Cities Chiefs Association, 'Facial Recognition Technology in Modern Policing: Recommendations and Considerations' (2021) Facial Recognition Working Group, <https://majorcitieschiefs.com/wp-content/uploads/2021/10/MCCA-FRT-in-Modern-Policing-Final.pdf> accessed 18 December 2021; see also Future of Privacy Forum, 'Privacy Principles for Facial Recognition Technology in Commercial Applications' (September 2018), <https://fpf.org/wp-content /uploads/2019/03/Final-Privacy-Principles-Edits-1.pdf> accessed 18 December 2021*

[12] *Blerim Rexha et al, 'Increasing Trustworthiness of Face Authentication in Mobile Devices by Modeling Gesture Behavior and Location Using Neural Networks' (2018) 10(2) Future Internet <https://www.mdpi.com/1999-5903/10/2/17/htm> accessed 15 December 2021*

[13] *Ibid*

[14] *Ibid*

[15] *William Crumpler, 'How Accurate are Facial Recognition Systems – and Why Does It Matter?' (14 April 2020) Center for Strategic & International Studies <https://www.csis.org/blogs/technology- policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter> accessed 15 December 2021*

with LFRT done through 1:n systems.[16] This lack of consenting participation and a resulting lack of facial data being captured in controlled circumstances can affect the quality of facial data, causing it to be of poor and inaccurate quality at times.

B. Rise in use of FRT

In recent past a continued rise in the development and use of FRT has been witnessed globally, attributable, in large part, to the vast amounts of facial images and video data in general, complemented with advancements in image recognition technology. Several government programs across the world, including India, gather biometric facial data at the time of registration for certain public services.[17] The purpose of gathering biometrics is to enable manual authentication of a person's identity at the time of furnishing particular identity documents, or at the time of availing certain services.[18] The rise in FRT computational abilities allows for such authentication to be carried out in an automated manner as opposed to manual means. Projects involving the use of biometrics and facial recognition have been launched in airports and other sectors across the world, as detailed in Chapter 3 below.

Social media platforms, and other websites on the Internet, further allow millions of images to be posted by its users across the world and permits these images to be viewed publicly. While there is a question of the ethical and privacy-related concerns on the seemingly unbridled sharing and use of these images without the consent of the uploader, social media platforms have admitted to using this large dataset to train its FRT systems, including training image-recognition and image-categorisation algorithms through the availability of tagged labels such as hashtags for these images.[19]

The use of facial recognition for public services has also benefited greatly from the ubiquitous presence of closed-circuit television (**CCTV**) cameras. India is home to some of the most surveilled cities in the world, with the use

[16] *Smriti Parsheera, 'Adoption and regulation of facial recognition technologies in India: Why and why not?' (November 2019) Data Governance Network, Working Paper 05*

[17] *PTI, 'Biometric data of 99 cr Indians collected: Govt' (New Delhi, 6 September 2016) The Hindu <https://www.thehindu.com/news/national/aadhar-bill-biometric-data-of-99-cr-indians-collected-govt/article8341976.ece> accessed 18 December 2021; See also Frederic Ho, 'Where Public and Private Meet: How Can Indonesia's e-KTP Help Citizens and Businesses?' (Jakarta, 16 April 2021) Jakarta Globe <https://jakartaglobe.id/opinion/where-public-and-private-meet-how-can-indonesias-ektp -help-citizens-and-businesses/> accessed 18 December 2021; INA, 'Al-Hindawi confirms the distribution of 13 million biometric cards' (Baghdad, 15 November 2020) Iraqi News Agency <https://www.ina.iq/eng/9950--.html> accessed 18 December 2021; Ministero dell'Interno, 'CIE Features' Carta D'identità Elettronica (Rome, Italy) <https://www.cartaidentita.interno.gov.it/en/cie/cie-features/> accessed 18 December 2021*

[18] *World Bank Group, Global Partnership for Financial Inclusion, 'G-20 Digital Identity Onboarding' presented at G20 Argentina 2018 <https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf> accessed 20 December 2021*

[19] *Tom Simonite, 'Your Instagram #Dogs and #Cats Are Training Facebook's AI' (2 May 2018) WIRED <https://www.wired.com/story/your-instagram-dogs-and-cats-are-training- facebooks-ai/> accessed 10 December 2021*

of CCTV cameras in Delhi, Chennai, Hyderabad, Indore and Bangalore ranking among the highest across the world, and an annual growth of 20-25% in India's surveillance units markets.[20] This trend is in line with global adoption of CCTV cameras, with countries such as China and Russia leading the way in the use of CCTV surveillance, followed by populous cities in the UK, South Korea and the USA.[21] The increased adoption of FRT by government entities providing public services seeks to capitalize on the gains of efficiency and accuracy.[22] Newer uses of FRT systems allow the identification of faces through masks, raising several questions on opt-outs to such services and the autonomy of a person over one of their primary identifiers- their faces.[23]

C. Categorising the applications of FRT

There are numerous examples of FRT being deployed within India by public authorities, as seen in Chapter 3 below. Given that FRT is a rapidly evolving technology, these categories are not watertight. Instead, the categories proposed below are meant to link the operation of certain kinds of FRT with their potential consequences. The broad range of applications, considerations and concerns emanating from the varied applications of FRT require a nuanced and measured approach towards its regulation, as opposed to a framework that treats all FRT alike, without considering the potential risks and benefits of each kind of application on its own merits. This serves to add value to discussions which examine such differences in nuance and influence any regulatory measures to govern the FRT ecosystem.

[20] *Paul Bischoff, 'Surveillance camera statistics: which cities have the most CCTV cameras?' (17 May 2021) <https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities> accessed 15 December 2021;See also Rahul Sachitanand, 'Sales of surveillance cameras are soaring, raising questions about privacy' (20 October 2018) The Economic Times, <https://economictimes.indiatimes.com/news/politics-and-nation/sales-of-surveillance-cameras-are-soaring-raising-questions-about-privacy-regulation/articleshow/66195866.cms?from=mdr> accessed 16 December 2021; Sudhakar Reddy, '8.3 lakh cameras in Telangana, Hyderabad turning into surveillance city: Amnesty' (10 November 2021) The Times of India <https://timesofindia.indiatimes.com/city/hyderabad/8-3l-cameras-in-t-hyd-turning-into-surveillance-city-amnesty/articleshow/87615657.cms> accessed 22 December 2021; See Also TNN, '7,000 cameras at 3,000 spots to make Bengaluru safer for women, children' (21 October 2021) The Times of India <https://timesofindia.indiatimes.com/city/bengaluru/7000-cameras-at-3000-spots-to-make-bengaluru-safer-for-women-children/articleshow/87176127.cms> accessed 22 December 2021*

[21] *Ibid; see also Thomas Ricker, 'The US, like China, has about one surveillance camera for every four people, says report' (9 December 2019) The Verge <https://www.theverge.com/2019/12/9/21002515/ surveillance-cameras-globally-us-china-amount-citizens> accessed 24 December 2021; 'Thousands of Russian Surveillance Cameras Vulnerable to Cyber attack – Reports' (12 March 2021) The Moscow Times <https://www.themoscowtimes.com/2021/03/12/thousands-of-russian-surveillance- cameras-vulnerable-to-cyberattack-reports-a73222> accessed 23 December 2021*

[22] *Varsha Bansal, 'The Hyderabad Model of CCTV Surveillance' (10 November 2020) Livemint <https://www.livemint.com/news/india/the-hyderabad-model-of-cctv-surveillance-11604926158442.html> accessed 29 November 2021*

[23] *Jane Li, 'China's Facial-Recognition Giant Says It Can Crack Masked Faces During The Coronavirus' (18 February 2020) Quartz Magazine <https://qz.com/1803737/chinas-facial-recognition -tech-can-crack-masked-faces-amid-coronavirus/> accessed 13 November 2021*

FRT applications based on the use can be divided in two broad sectors - the non-security use cases; and the security uses of FRT. This distinction acknowledges the differing benefits and risks that may result from the respective use of FRT, placing an emphasis on difference in the likelihood and severity of consequences in certain scenarios with FRT applications.

1. Non-security uses of FRT

The use of FRT for purposes of verification and authentication of the identity of an individual, or intended to provide greater ease of access to certain services (contactless onboarding at airports), or to ease usability (unlock smartphone) may be broadly categorised as non-security uses of FRT. Such FRT applications are primarily different from those applications being used in a law enforcement or a surveillance construct with differing operating models as a result. Non-security uses of FRT, relying largely on authenticating an identity, is more likely to involve 1:1 use of FRT, matching the person seeking a certain benefit from the provider with the person registered to seek that particular benefit. Examples of non-security uses of FRT range from international uses of FRT to provide greater ease of access to airport facilities[24], to educational systems using FRT to generate unique IDs to select college course options[25], and authentication to provide access to products, services, and public benefits.[26]

Given the nature of these operations and the use of FRT for 1:1 authentication, these operations typically operate with prior consent of potential users of such applications and reduce wide-ranging processing of facial data that may increase an application's inaccuracy. While these use cases broadly aim at providing greater convenience to consumers along with efficiency to the service providers, these applications are susceptible to the potential risks and concerns raised using automated FRT. These concerns must be weighed against the need for adopting FRT, its application being proportional to its intended outcomes in a narrow and tailored manner, and the overall social benefit sought to be achieved by non-security uses of FRT functions.

2. Security related uses of FRT

[24] *Madeleine Hillyer, 'World Economic Forum Consortium Launches Paperless Canada-Netherlands Travel Pilot' (26 June 2019) WEF Forum <https://www.weforum.org/press/2019/06/world-economic -forum-consortium-launches-paperless-canada-netherlands-travel-pilot/> accessed 22 December 2021; Ashok Upadhyay, 'Facial recognition tech at 4 airports to cost Rs 165 crore' (New Delhi, 3 January 2022) India Today <https://www.indiatoday.in/india/story/facial-recognition-tech-airports -1895426-2022-01-03> accessed 9 January 2022; Elaine Gusac, 'Your Face Is, or Will Be, Your Boarding Pass' (11 January 2022) The New York Times <https://www.nytimes.com/2021/12/07/travel/biometrics-airports-security.html> accessed 14 January 2022*

[25] *Ravikant Reddy, 'Facial recognition system introduced in Degree admissions' (Hyderabad, 22 June 2020) The Hindu <https://www.thehindu.com/news/national/telangana/facial-recognition-system -introduced-in-degree-admissions/article31892709.ece> accessed 15 December 2021*

[26] *Unique Identification Authority of India, 'Aadhaar Paperless offline e-KYC' <https://uidai.gov.in/2-uncategorised/11320-aadhaar-paperless-offline-e-kyc-3.html> accessed 20 December 2021*

As opposed to the non-security applications, FRT in the security context encompasses a wider role in image identification and live monitoring. These functions may typically include the use of FRT for general law and order considerations, like investigation, identification of missing persons27, identifying persons of interest to the law enforcement[28], monitoring of crowds,[29] and more recently, for even screening public spaces for finding violations of masking protocols given the COVID-19 pandemic[30]. Within these use cases too, there are certain distinctions in the application of FRT. The use of automated FRT for identification of persons for offences against witness sketches or an existing set of suspects may constitute post facto FRT. On the other hand, monitoring for crowd control or the use of FRT in real time to identify violations or absconding violators is a feature of LFRT. A prime example of LFRT is the implementation of real time FRT in Surat aimed at integrating video surveillance systems with a watchlist of suspected individuals.[31]

Even in surveillance, it is the use of live FRT, which is increasingly being debated from legal and ethical standpoints, globally. As discussed in further depth in Chapter 5 below, the nature of live FRT compounds existing risks of security FRT such as lack of consent, inaccuracy, bias and attendant concerns of misidentification with various externalities to the FRT system capturing facial images from live surveillance systems. The Information Commissioner Office in the UK has called for a higher legal bar for the use of live FRT, flagging concerns over principles of proportionality and necessity being violated by technologies that automatically and indiscriminately collect biometric facial data.[32]

[27] *Anuradha Nagraj, 'Indian police use facial recognition app to reunite families with lost children' (14 February 2020) Reuters <https://www.reuters.com/article/us-india-crime-children-idUSKBN2081CU> accessed 10 November 2021; Special Correspondent, 'Face-recognition technology helps find missing woman despite mask' (Bengaluru, 9 September 2021) The Hindu <https://www.thehindu.com/news/cities/bangalore/face-recognition-technology-helps-find-missing-woman/article36372677.ece> accessed 17 November 2021*

[28] *Alexandra Ulmer, Zeba Siddiqui, 'India's use of facial recognition tech during protests causes stir' (Mumbai/ New Delhi, 17 February 2020) Reuters <https://www.reuters.com/article/us-india-citizenship -protests-technology-idUSKBN20B0ZQ> accessed 17 November 2021*

[29] *Vijaita Singh, '1,100 rioters identified using facial recognition technology: Amit Shah' (New Delhi, 12 March 2020) The Hindu <https://www.thehindu.com/news/cities/Delhi/1100-rioters-identified-using-facial-recognition-technology-amit-shah/article31044548.ece> accessed 1 December 2021*

[30] *Lucy Ingham, 'Facial recognition applied to social distancing, mask control' (13 July 2020) Verdict <https://www.verdict.co.uk/facial-recognition-social-distancing/> accessed 3 December 2021*

[31] *Yagnesh Bharat Mehta, 'In a first, real-time facial recognition system launched by Surat police' (Surat, 19 July 2015) The Times of India <https://timesofindia.indiatimes.com/city/surat/in-a-first-real- time-facial-recognition-system-launched-by-surat-police/articleshow/48135306.cms> accessed 9 December 2021*

[32] *Information Commissioner's Office, 'The use of live facial recognition technology in public places' (18 June 2021) Information Commissioner's Opinion <https://ico.org.uk/media/2619985/ico-opinion- the-use-of-lfr-in-public-places-20210618.pdf> accessed December 3, 2021*

The major concerns with security uses of FRT stem from these applications used in a 1:n identification paradigm, with each additional variable a hindrance to accurate and effective identification. Security uses of FRT systems also do not explicitly rely on the consent of a participant through a registration process to process their biometric facial data for compiling its gallery dataset, placing these applications outside the notice-and-consent framework of traditional data protection norms.[33] Legislation permitting access to recorded data for law enforcement for prevention, detection or investigation of crimes allows the compilation of vast facial datasets.[34] These datasets may include faces of any regular person, whether or not that person is aware that their face may be matched against the face of any suspected criminal based on the accuracy of an FRT system. Additionally, due to the nature of the actors implementing FRT systems for security uses, the consequences of inaccuracy due to misidentification, perturbations, or bias within the FRT system may lead to gross violations of a person's right to life and liberty.[35] Further, there is potentially flawed incentivisation in the deployment of FRT systems, the consequences of which can be dire. For instance, incentivising a private security operator for flagging suspicious people without adequate checks and balances, can arguably result in an overly excessive usage of FRT systems for monitoring and surveillance. Security uses of FRT applications have now started being recognised for their increased likelihood of consequences as well as the added severity of consequences based on its various concerns, as elaborated in Chapters 4 and 5 of this Paper. The use of ring-fencing and regulation based on certain uses of FRT systems, as seen in the European Union's Artificial Intelligence Bill, hasfurther been discussed in Chapter 5.[36]

[33] *Smriti Parsheera, 'Adoption and regulation of facial recognition technologies in India: Why and why not?' (November 2019) Data Governance Network, Working Paper 05*

[34] *For example, see Section 3(2), Andhra Pradesh Public Safety (Measures) Enforcement Act, 2013 that states 'Every owner/manager/person or the persons who are running an establishment shall save/store video footage properly for a period of 30 days and provide the same as and when required by an Inspector of Police having jurisdiction over the area or any other authority as may be notified by the Government'*

[35] *Jai Vipra, 'The Use of Facial Recognition Technology for Policing in Delhi', Vidhi Centre for Legal Policy, Working Paper <https://vidhilegalpolicy.in/research/the-use-of-facial-recognition-technology- for-policing-in-delhi/> accessed 10 November 2021; Kashmir Hill, 'Wrongfully Accused by an Algorithm' (3 August 2020) The New York Times <https://www.nytimes.com/2020/06/24/technology/ facial-recognition-arrest.html> accessed 11 December 2021*

[36] *Proposal For a "Regulation of the European Parliament and of the Council laying down harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts", COM (2021) 206 final, European Commission, 2021/0106(COD)*

III. EXAMPLES OF FRT USE IN INDIA AND GLOBALLY

As discussed above, the ubiquitous nature of videos, and other graphic data has created an abundance in data sources for the development of FRT across the globe. The use cases range from more commercial products like facial scans to unlock cell phones, to reports of large-scale state surveillance. For instance, Chinese companies have come under repeated scrutiny for aiding the government's surveillance capacity against Uyghurs in the Xinjiang region.[37] Similarly, in reported recognition of its risks, several tech giants like IBM, Microsoft and others, have taken some proactive steps to limit their development of said technology. Nonetheless, there are private entities like Clearview. Ai, which have been at the forefront of building cutting edge FRT systems for governments and private corporations across the globe and have come under heavy scrutiny for their disregard of local data protection laws, and privacy concerns of citizens.

This ever-increasing adoption and use of FRT systems across the world must be kept in mind while discussing the concepts, risks, and global regulation of FRT systems. The section briefly lists a few national and international examples of FRT systems currently operational (elaborated in greater detail in **Annexures 1 and 2**, respectively, of this Paper) which will help contextualise the discussions elsewhere within the Paper on FRT systems.

A. FRT systems launched in India

FRT systems have seen an uptick in adoption in recent years. FRT systems have been deployed in the public sector by various state agencies in India for the purposes that include law enforcement, monitoring, and ease of access to public benefits and services. This chapter discusses a few prominent examples

[37] Johana Bhuiyan, 'US sanctioned China's top facial recognition firm over Uyghur concerns. It still raised millions', (7 Jan 2022) the Guardian <https://www.theguardian.com/world/2022/jan/06/china-sense-time-facial-recognition-uyghur-surveillance-us-sanctions> accessed on 27 July 2022

of FRT systems deployed in India. These FRT systems are being used for (a) law enforcement purposes by police in the state of Punjab, Gujarat and Tamil Nadu, (b) admissions processes in educational institutions in Andhra Pradesh, and (c) recording biometric attendance for workers employed by the local government body in Mumbai, Maharashtra. A non-exhaustive list of FRT systems being launched or deployed in India has been attached in Annex 1 of this paper.

B. FRT applications deployed in foreign jurisdictions

In foreign jurisdictions, FRTs are being adopted in a broad range of contexts. The deployment of FRT systems is prominently seen in security, surveillance and law enforcement purposes, and for the purposes of access controls in airports. In a survey of the hundred most populated countries of the world, it was found that only six countries had *no evidence* of use of FRT, which was probably attributable to lack of budget / technology, rather than a principled opposition to the technology. It further concluded that seven out of ten governments, in the hundred most populated countries, had deployed FRT on a large-scale basis.[38] A non-exhaustive survey of FRT applications being used in these fields by different countries has been attached in **Annex 2** of this paper.

[38] *Paul Bischoff, 'Facial recognition technology: 100 countries analysed' (8 June 2021) Comparitech <https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/> accessed 16 January 2022*

IV. RISKS OF FRT

The rising adoption of FRT for both security or non-security purposes requires a deeper examination of the risks associated with, and inherent to such use cases. In addition to the ethical considerations inherent to the use of AI systems39, the use of FRT systems raises specific risks based on its particular use-case operations and consequences. This chapter seeks to elaborate on the design-based risks and rights-based challenges arising from the widespread use of FRT systems.

A. Design-based risks of FRT systems

The application of FRT systems by public authorities presents certain ethical risks which are unique to the FRT paradigm. While the concerns of automation bias, discrimination, exclusion or lack of accountability are generally applicable across all uses of AI systems, the specific operations and consequences inherent to FRT systems require a separate analysis of the design-based risks of FRT systems. The twin concerns of accuracy and interpretability in the use of AI systems are affected by increasing complexity in computational algorithms which tend to provide more accurate, but less explainable results. At this stage, it is pertinent to review the concerns of misidentification due to inaccuracy, its potential causes and its real-world consequences. The key points relating to the design-based risks are set out below in Table 1.1, with detailed explanations attached in **Annex 3** of this Paper.

[39] *Niti Aayog, 'Approach Document for India Part 1 – Principles for Responsible AI' (February 2021) <https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf> accessed 29 July 2022;*

Table 1.1- *A quick guide to the design-based risks of FRT systems*

S. No	Design-based risks
1.	**Inaccuracy due to technical factors:** a. Intrinsic factors: facial expression, aging, plastic surgery, disfigurement; or b. Extrinsic factors: illumination, pose variation, occlusion, or quality of image
2.	**Inaccuracy due to bias caused by underrepresentation:** a. Colour-based: Existing international studies indicate disparities error rate based on skin tone. b. Gender-based: Studies on FRT systems in India indicate disparity in error rate based on identification of Indian men and Indian women. c. Accentuated by import of FRT system: FRT systems process facial images and rely on categorisation. An FRT system, if developed outside India, may rely on categories that may not make sense in the Indian context. d. The issue of racial bias is particularly challenging in India, where even within the country there are many different communities with a diverse array of physical and facial features. In such a context, having access to a pan-India database of facial information and biometrics, is essential to create a robust FRT system. e. Assessment in Indian context: It is important for the FRT systems to be specifically assessed for the Indian context. The validation mechanism must simulate a real-world scenario, where both intentional and unintentional unconstrained disguises are encountered by a face recognition system.
3.	**Inaccuracy due to lack of training of human operators:** a. The methodology of FRT systems requires a human operator to either verify or act on outputs provided by FRT systems. Potential of misidentification due to inaccuracy thus makes it necessary for a trained human operator to use the FRT system.
4.	**Inaccuracy due to glitches or perturbations:** a. FRT systems are vulnerable to sabotage by addition of tiny tweaks, immaterial to a human agent, that render the FRT system useless.
5.	**Security risks due to data breaches and unauthorised access:** a. The vast amount of facial data processed by companies that develop or deploy FRT systems presents a financially valuable target for hackers. b. Additionally, weak institutional data security practices may expose massive amounts of personal data to data leaks, affecting the privacy of the concerned individuals.
6.	**Accountability, legal liability and grievance redressal:** a. FRT systems suffer from the 'many hands problem' in terms of various entities involved in developing, testing, training and deploying the FRT system. b. This raises issues on accountability measures and legal liability for harms caused by an FRT system's inaccuracies. c. Trade secret and intellectual property protections may further hamper grievance redressal efforts by affected individuals, due to difficulties in being able to prove discrimination or bias.

7.	**Opaque nature of FRT systems:** a. The deployment of FRT systems may involve use of personal data other than for which it was shared or may result in usage of FRT systems in manners contrary to or in addition to its stated purpose. An overly opaque FRT system may prevent independent scrutiny that seeks to avoid these uses. To counter this, a robust transparency framework encompassing the deployment and use of the FRT system may be set in place.

B. Rights-based challenges to use of FRT systems

The use of FRT systems presents further challenges from a rights-based perspective, when the benefits of FRT systems are viewed against the costs from a privacy and liberty perspective. The processing of biometric facial data, an identifier for any person, is the essence of any FRT system, which places any legal analysis on FRT systems squarely within the ambit of personal data protection and privacy law. The potential for its use by state entities to control or threaten free speech by rapidly reducing the scope for anonymity in public and private spheres, on the other hand, prompt a discussion from a liberty perspective. The key points relating to the rights-based risks are set out in Table 1.2 below, with detailed explanations attached in **Annex 4** of this Paper.

Table 1.2- *A quick guide to the rights-based risks of FRT systems*

S. No	Rights-based challenges
1.	**Puttaswamy on privacy and informational autonomy:** a. The Supreme Court in Justice K Puttaswamy v. Union of India (2017) has recognised the right to informational autonomy as a facet of the right to privacy within Article 21 of the Constitution. b. The operation of FRT systems in real-world scenarios is contingent on the FRT system consuming and computing vast amounts of biometric facial data, both in its training and in its operation. c. An individual may not be aware or in control of the extent of their biometric facial data being processed for training or operating an FRT system, as seen in cases of CCTVs, governmental programs, 1:n systems. d. As such, questions of privacy and informational autonomy have been raised, and shall foreseeably continue to be raised, both in India and across the world on the very nature of FRT. e. FRT systems shall be required to operate within the boundaries established by Puttaswamy, and future judicial pronouncements on the emerging concepts discussed in this Paper.
2.	**Issues of informational autonomy:** a. Biometric facial images collected for one purpose and subsequently used for another purpose falls against the concept of informational autonomy. b. A person having consented to giving his facial data for the first purpose may not be aware of the second purpose, and is unable to know, control, or consent to the second purpose.

	c. This raises a concern flagged by many as 'purpose creep', undermining the control and consent of the individual involved in the collection of facial images for the first purpose. d. Making facial recognition mandatory for access to public services, public benefits or rights undermines meaningful consent, if the individual is left without adequate alternative means to those services and rights. e. Consent cannot be implied by mere awareness of facial data being processed.
3.	**Threat to non-participants in deployment of FRT systems:** a. Operationalisation of an FRT system by a government agency, even if kept voluntary, continues to threaten individuals who have not consented or enrolled in the FRT system. b. This threat shall arise when a person has consented to their facial image being processed by a government agency for one purpose, and a dataset containing that image is used by either the same agency or a different agency for a different purpose. c. The use for the second purpose may either be for training an FRT system, or to help the FRT system populate a gallery image dataset. d. A gallery image dataset is typically used by the FRT system to compare against facial images of the voluntary enrolees for authentication or identification. e. As long as the gallery image dataset contains the image of a person who has not signed up for the second purpose, there continues to remain a possibility of an FRT system falsely identifying another person as that non-consenting individual through misidentification (a false positive), even though the non-consenting individual is not a part of the program. f. Depending on the use-case in question of the FRT system, the government agency and/or the non-participant now must suffer the consequence of this misidentification.
4.	**Legal thresholds applicable to FRT systems:** a. In addition to informational autonomy, the Supreme Court in 2017 set out a three-pronged test of: i. legal validity, ii. legitimate interests, and iii. proportionality for cases involving restraints on privacy by the State which include national security and legitimate state interests. d. In 2018, the Supreme Court has expanded the proportionality test to a four-part test which includes testing whether the measure restraining the right to privacy: i. has a legitimate goal, ii. is a suitable means of furthering that goal, iii. is the least restrictive while being equally effective among its alternatives, and iv. does not have a disproportionate impact on the right holder.

5.	**Anonymity as a facet of privacy** a. FRT systems rely on significant amounts of sensitive personal data processing and computation and increasing applications of FRT systems further incentivize sensitive personal data processing and computation. b. This cycle of incentives raises apprehensions on the decreasing space for anonymity and its effect on the larger erosion of privacy. c. FRT systems have been used to suppress dissent and protests across the world. d. Countries have commenced enacting laws that prohibit a person from wearing masks or other occlusions. These measures seek to suppress an individual's right to exercise their right not to have their facial data processed by FRT systems. e. These concerns must be considered in view of legal standards of proportionality, necessity and suitability prescribed for the processing of sensitive personal data by state agencies.

The breadth of capabilities possible through application of FRT makes it essential for robust safeguards and institutional frameworks that temper and regulate the transfer, usage, and retention of the biometric personal data. The following chapter look at safeguards and institutional frameworks devised globally in response to the risks and challenges posed by the use of FRT systems.

V. REGULATORY ASPECTS OF FRT

FRT regulation is still evolving in most jurisdictions. This is primarily a result of two simultaneous developments; first, the varied applications in which FRT is being used and second, the kinds of regulatory tools that are at the disposal of the relevant national authority. Most commonly, across jurisdictions, FRT related issues are still primarily regulated under the aegis of their respective privacy laws. Apart from the EU, which only recently passed a proposal for standalone AI regulation, there is no dedicated FRT / AI law that is in effect in most of the jurisdictions. Therefore, a study of AI / FRT regulation is a study of the concomitant laws and regulatory frameworks. FRT legislations typically involve three elements. First, they restrict the purposes for which FRT can be used. Second, they specify certain pre-deployment requisites such as written authorisations and judicial application of mind. Third, they specify safeguards for the deployment of this technology. These include facets such as maintenance of records, human review, periodic assessment, and transparency in functioning of the FRT.

The following cross-jurisdiction analyses of different FRT regulations will aid in a deeper understanding of such frameworks. It will allow lawmakers relying on this handbook to adopt and adapt pertinent ideas to the Indian context. Details of domestic legislation, guidelines, action points of each jurisdiction, are part of Annex 5 of this Paper.

1. European Union

The EU's approach to FRT regulation has been to consider it as a subset of AI regulation. For the latter, the EU does not start from a blank state in building up its regulations but rather takes the approach of updating its existing laws to meet with AI related challenges.[40] The General Data Protection Regulations

[40] *European Commission, On Artificial Intelligence - A European approach to excellence and trust (COM(2020) 65) <https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf> accessed 16 January 2022*

(GDPR), and its Data Protection Directive, are two primary sets of regulations which govern the collection and processing of sensitive personal data like biometrics. Additionally, the EU has now proposed an AI Act which will establish a risk-based compliance framework. Under this proposed AI Act, FRT systems have been categorised as "high risk" with the highest level of compliance requirements.

2. United Kingdom

In the UK, deployment of FRT would be covered under its data protection framework. This includes the Charter of the Fundamental Rights of the European Union, 2000, Data Protection Act, 2018 and the UK-GDPR.[41] In 2020, the Court of Appeal held that the use of live automated FRT was unlawful. Following this, the Information Commissioner (**ICO**) issued an opinion laying down principles for live FRT deployment in public places.

3. United States

In the US, the regulation of FRT can be examined at three levels - the federal, state and city level. Since regulation of FRT is seldom a standalone exercise, and draws from existing laws in place, there is a more detailed regulatory framework at the state level which have their respective privacy laws. The models adopted by different laws on FRT range from bans, time bound or directive moratoriums and regulation of FRT.

4. Australia

In Australia, the regulation of FRT primarily comes from its privacy law i.e., the Privacy Act, 1988. Currently, it does not have specific laws to regulate FRT and AI.[42] Australia's regulation of FRT comes from the Office of the Australian Information Commissioner's **(OAIC)** investigation into the usage of FRT by law enforcement and private entities. Parallelly, the Australian Human Rights Commission, has also been engaged in developing a standpoint on the manner in which FRT deployments should be regulated.

5. Canada

Canada regulates FRT under its privacy and data protection laws. It does not have a law, at present, dedicated specifically to FRT or AI. There are two federal privacy laws i.e., the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA).

[41] *The UK-GDPR is the domestic retention of the GDPR, 2016 which ceased to apply post Brexit.*

[42] *Department of Industry, Science, Energy and Resources Australia's Artificial Intelligence Action Plan 2021 <https://www.industry.gov.au/data-and-publications/australias-artificial-intelligence-action-plan> ccessed 16 January 2022*

Australia has formulated the Artificial Intelligence Action Plan. A part of the Action Plan is the development of ethical AI. These principles are that AI systems should benefit individuals, they should imbibe human centred values, be fair, respect privacy and security, be reliable and safe, be transparent and explainable, be contestable and imbibe accountability measures.

PART II

A CASE STUDY OF DIGI YATRA

Digi Yatra (**'Digi Yatra'**) (**'DY'**) is a proposed biometric boarding system (**'BBS or DY-BBS'**) for use at Indian airports, intended to create a seamless, paperless, and contactless check-in and boarding experience for passengers. It envisages an identity management ecosystem for Indian airports which can enhance the capabilities of Indian civil aviation infrastructure, digitise manual processes at airports, improve security standards and lower the cost of operations of airports.[43]

Digi Yatra proposes use of FRT to authenticate a passenger's travel credentials, which allows other checkpoints in an airport to be operated in an automated form with minimal human involvement.[44] The use of FRT has the potential to eliminate several inefficiencies at Indian airports and provide tangible benefits to the civil aviation ecosystem. At the same time, it is necessary to ensure that any deployment of FRT is privacy-protecting, non-discriminatory, legally compliant, and consistent with the principles of RAI as laid down in the approach papers.[45]

The Ministry of Civil Aviation constituted a Technical Working Committee to conceptualise the Digi Yatra project.46 A Digi Yatra policy was released in 2018, which sets out the passenger processes and technical features of Digi Yatra, which was subsequently updated from being the Digi Yatra Central Identity Management Platform (DYCIMP) to Digi Yatra Central Ecosystem which is a Distributed Ecosystem proposed on W3C standards, Self-Sovereign

[43] *Ministry of Civil Aviation, '"Digi Yatra Biometric Boarding System" Reimagining Air Travel in India' (4 March 2021) v 7.5*

[44] *Ministry of Civil Aviation, '"Digi Yatra Biometric Boarding System" Reimagining Air Travel in India' (4 March 2021) v 7.5*

[45] *NITI Aayog, 'Approach Document for India Part 1 – Principles for Responsible AI ' (February 2021) Responsible AI <https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf> accessed 20 February 2022*

[46] *Ministry of Civil Aviation, '"Digi Yatra Biometric Boarding System" Reimagining Air Travel in India' (4 March 2021) v 7.5*

Identity (SSI), the use of Verifiable Credentials (VCs) and Decentralised Identifiers with a trust layer of Distributed Ledger. The Digi Yatra Foundation ('DYF'), a not-for-profit company under Section 8 of the Companies Act, 2013 was established in 2019 for the implementation of the Digi Yatra Central Ecosystem.[47]

In 2021, the DYF approached NITI Aayog to identify a start-up for the development of Digi Yatra Central Ecosystem and assess the usability of the same and promote Indian start-ups. This was conceived as a pilot to explore the functionality and efficacy of the Digi Yatra Central Ecosystem for sharing the identity, travel, health and other credentials to airports, airlines and other agencies who enable air travel. This sharing shall be consistent with measures that are privacy-protecting, non-discriminatory, legally compliant, and consistent with the principles of RAI.[48] In this regard the following steps were taken:

1. NITI Aayog constituted a multi-disciplinary committee with experts across face biometrics, machine learning, computer science, legal, policy, engineering, standards and domain. The committee was tasked with defining the risks in the technology, recommend measures to ensure responsible AI principles are adhered, oversee the technical requirements and guide the development of a proof of concept.
2. Based on the recommendations of the committee, NITI Aayog launched a challenge in collaboration with Atal Innovation Mission, DYF and Amazon Web Services.
3. The committee had identified that performance of FRT in Indian context and ensuring privacy and security by design must be the key considerations. Accordingly, evaluation and selection processes were identified for start-ups to be short listed and a protocol was established to showcase their abilities in critical technology components, platform architecture and solution design. Furthermore, a roadmap was developed for the piloting of the designed solution, at three airports.

This Paper explains the process followed in this regard with focus on RAI principles and frameworks. It further uses this case study to provide actionable recommendations in general, with the objective of facilitating deployment of FRT in a limited, legitimate, safe, and responsible manner in public projects.

[47] *Digi Yatra Foundation has been incorporated on 20 February 2019 <dyce.niti.gov.in> accessed 24 February 2022*

[48] *NITI Aayog, 'Approach Document for India Part 1 – Principles for Responsible AI ' (February 2021) Responsible AI <https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf> accessed 20 February 2022*

To this end, *first*, this part discusses some key processes and elements of the Digi Yatra Cental Ecosystem. *Second*, relying on the RAI principles, it examines the robustness of existing checks in Digi Yatra, and makes specific recommendations on how to further improve the project's compliance with these principles. *Finally*, it sets out some actionable recommendations to guide the implementation of responsible FRT in a legal, purpose specific, and responsible manner in future public projects, aimed at maximising its potential and mitigating the risks therein to a minimum.

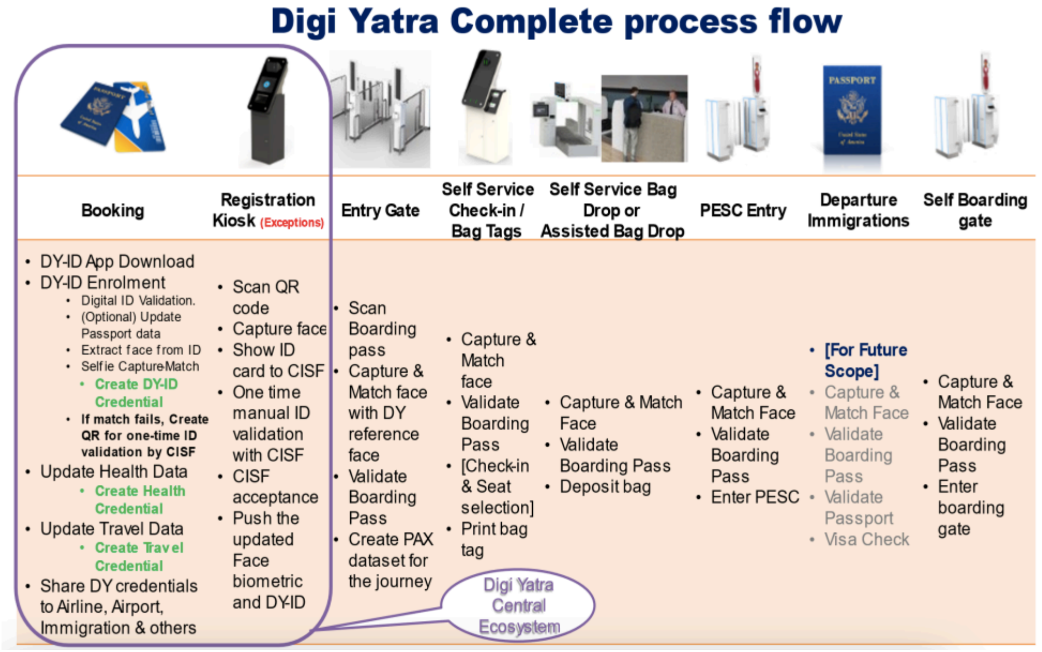
A. The Digi Yatra programme

The Digi Yatra programme envisages a biometric boarding system. In the context of an airport, this can be understood as involving two components: the authentication and creation of a digital identity of a passenger, and the subsequent verification of this identity at different checkpoints in an airport.[49] The traditional passenger process at an airport involves both components, which are largely performed manually. For example, in India, CISF personnel are staffed at airports and are responsible for identity verification, travel documentation checks, etc., at entry gates.[50] CISF personnel as well as airline staff manually perform the verification of identity at subsequent checkpoints in the airport. An identity management system has the potential to supplement and assist this human involvement, and consequently, ease congestion and operational costs at airports. Further, the automation of the subsequent verification of identity at different checkpoints has the potential to also create a seamless, paperless, and contactless experience for passengers.

The Digi Yatra Central Ecosystem is envisaged to be a set of modules that enable operationalisation of this biometric boarding system. Detailed standard operating procedures (SOPs) related to the Digi Yatra Central Ecosystem, in relation to both domestic and international travel, have been set out in the Digi Yatra policy. Illustratively, the operation of the Digi Yatra platform, from the perspective of a passenger, can be understood broadly from the following schematic:

[49] *Ministry of Civil Aviation, '"Digi Yatra Biometric Boarding System" Reimagining Air Travel in India' (4 March 2021) v 7.5*

[50] *Ministry of Civil Aviation, '"Digi Yatra Biometric Boarding System" Reimagining Air Travel in India' (4 March 2021) v 7.5*



Digi Yatra Complete process flow

Booking	Registration Kiosk (Exceptions)	Entry Gate	Self Service Check-in / Bag Tags	Self Service Bag Drop or Assisted Bag Drop	PESC Entry	Departure Immigrations	Self Boarding gate
• DY-ID App Download • DY-ID Enrolment • Digital ID Validation. • (Optional) Update Passport data • Extract face from ID • Selfie CaptureMatch • Create DY-ID Credential • If match fails, Create QR for one-time ID validation by CISF • Update Health Data • Create Health Credential • Update Travel Data • Create Travel Credential • Share DY credentials to Airline, Airport, Immigration & others	• Scan QR code • Capture face • Show ID card to CISF • One time manual ID validation with CISF • CISF acceptance • Push the updated Face biometric and DY-ID	• Scan Boarding pass • Capture & Match face with DY reference face • Validate Boarding Pass • Create PAX dataset for the journey	• Capture & Match face • Validate Boarding Pass • [Check-in & Seat selection] • Print bag tag	• Capture & Match Face • Validate Boarding Pass • Deposit bag	• Capture & Match Face • Validate Boarding Pass • Enter PESC	• [For Future Scope] • Capture & Match Face • Validate Boarding Pass • Validate Passport • Visa Check	• Capture & Match Face • Validate Boarding Pass • Enter boarding gate

Pertinently, the Digi Yatra programme is conceptualised as a purely voluntary mechanism, and therefore, at various stages, the Digi Yatra Policy sets out the alternative means in which the boarding process will operate for a passenger that does not opt-in to the Digi Yatra programme – namely, physical verification of their travel ID documents would continue to be done by CISF personnel at an airport. The current Digi Yatra process will, therefore, supplement human involvement at airports, and in time may be upscaled to all airports, with necessary legal frameworks in place.

B. Potential benefits

The use of FRT for the purpose of identity verification has some potential benefits which are discussed in this section. It should be noted that while there may be significant benefits, two propositions must be carefully considered: first, the costs of this policy must also be simultaneously evaluated – particularly from the perspective of the potential risks in the policy and its impact on citizen interests.51 The following chapters undertake this analysis from the lens of the principles of Responsible AI; secondly, for these benefits to materialise, it is important to develop the correct operational and organisational measures to enable these benefits to be realised.52 This aspect is studied, in the following chapters, from the lens of systems failure analysis. **Some of the potential**

[51] *NITI Aayog, 'Approach Document for India Part 1 – Principles for Responsible AI ' (February 2021) Responsible AI <https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf> accessed 20 February 2022*

[52] *NITI Aayog, 'Approach Document for India: Part 2 - Operationalizing Principles for Responsible AI ' (August 2021) Responsible AI <https://www.niti.gov.in/sites/default/files/2021-08/Part2-Responsible-AI-12082021.pdf> accessed 20 February 2022*

benefits of the Digi Yatra ecosystem are:

1. Lower congestion at airports

a. The use of FRT for authentication and subsequent verification at an airport can reduce waiting times and queues at airports that are caused due to human inefficiencies and human errors.[53] The automation of identity verification may eliminate bottlenecks in the passenger process at airports.[54]

b. It should be noted that since (i) Digi Yatra is a completely voluntary policy and alternative methods of check-in and boarding will continue to be provided; and (ii) in the instance of unsuccessful authentication or other technical problems with the FRT, human assistance may continue being necessary.[55]

2. Seamless, paperless and contactless passenger experience

The Digi Yatra platform can also simplify the passenger experience at airports by eliminating the need for their credentials to be manually verified at each stage. This has the potential to create a seamless, paperless, and contactless experience for passengers. Particularly in the context of Covid-19, or potentially similar scenarios in the future, the development of contactless capabilities in civil aviation can make the passenger experience safer, through the adoption of health-risk free processes.[56]

3. Lower operational costs and enhanced civil aviation capabilities

a. The supplementing of human efforts through automation will consequently lower operational costs, both for airport operators, airlines as well as State agencies responsible for identity verification. These lower operational costs of airports are likely to have a knock-on beneficial effect on the Indian civil aviation industry.

b. The increased automation is likely to reduce human errors and inefficiencies which will consequently lead to a better experience for passengers at airports. Better efficiencies are likely to also enhance the civil aviation capabilities, with airports being able to cater to a larger number of passengers due to lower congestion.

[53] *Ministry of Civil Aviation, '"Digi Yatra Biometric Boarding System" Reimagining Air Travel in India' (4 March 2021) v 7.5*

[54] *Ministry of Civil Aviation, '"Digi Yatra Biometric Boarding System" Reimagining Air Travel in India' (4 March 2021) v 7.5*

[55] *Ministry of Civil Aviation, '"Digi Yatra Biometric Boarding System" Reimagining Air Travel in India' (4 March 2021) v 7.5*

[56] *PTI, 'Mumbai airport rolls out contactless check-in system for passengers' (8 September 2020) Business Standard <https://www.business-standard.com/article/current-affairs/mumbai-airport-rolls-out-contactless-check-in-system-for-passengers-120090801106_1.html> accessed 3 March 2022*

C. Legal aspects of Digi Yatra

In light of the foregoing discussion, it may be prudent to highlight some legal aspects related to Digi Yatra, particularly in relation to data privacy, the use of Aadhaar biometrics for authentication, and information security within the Digi Yatra platform.

1. Data privacy

a. The Digi Yatra Policy envisages Digi Yatra as a completely voluntary scheme. In a voluntary scheme, where the passengers sign up and consent to use Digi Yatra for the purpose of check-in and boarding, this agreement would have the legal character of a voluntary agreement for the temporary collection, temporary storage and use of data. This agreement must comply with existing laws and rules on data privacy. These rules are set out presently under the Information Technology Act, 2000,[57] and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data and Information) Rules, 2011 ('**SPDI Rules'**). Given that the Digi Yatra Foundation, which operationalised the Digi Yatra Central Ecosystem, is established under the Companies Act, 2013,[58] it would amount to a 'body corporate' for the purposes of the SPDI Rules. Therefore, it would be necessary for Digi Yatra to comply with the SPDI rules.

b. The SPDI Rules define 'biometric information' as 'sensitive personal data or information'.[59] Consequently, a higher degree of protection applies to such data and must be adhered to. Therefore, the collection of data under Digi Yatra must satisfy the requirements of Rule 5 of the SPDI rules.[60]

c. Looking ahead, the proposed Personal Data Protection Bill ('**PDP Bill**') is expected to establish the principles, rules and standards related to data protection which would have to be complied with.[61] The chapter on High Level Data Privacy in the Digi Yatra Policy outlines some of the expected measures in this regard, particularly in relation to privacy impact assessments and ensuring data privacy by design.[62]

[57] *S. 43, Information Technology Act, 2000*

[58] *https://dyce.niti.gov.in/*

[59] *Rule 3, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ('SPDI Rules')*

[60] *Rule 5, SPDI Rules*

[61] *'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (2018) Committee of Experts under the Chairmanship of Justice Srikrishna ; See also Report of the Joint Committee on the Personal Data Protection Bill, 2019*

[62] *Ministry of Civil Aviation, '"Digi Yatra Biometric Boarding System" Reimagining Air Travel in India' (4 March 2021) v 7.5*

There are some additional issues which may be highlighted in relation to data privacy:

i. While the Digi Yatra Policy states that it is completely voluntary in nature, if the use of Digi Yatra is made mandatory in any way, then the same must comply with the principles laid down in *K.S. Puttaswamy v. Union of India* relating to the legality, necessity, and proportionality of the policy.[63]

ii. The Digi Yatra Policy states that facial biometrics are deleted from the local airport's database 24 hours after the departure of the passenger's flight.[64] However, the rules related to deletion of other information collected from the passengers, as well as any facial biometrics that are stored in other registries, must be clearly set out in the Policy.

iii. The Digi Yatra Policy mentions that users may also be able to provide consent for value-added services at the airport, for which purpose their data may be shared with other entities like cab operators and other commercial entities. There must be specific care taken to ensure that such consent is meaningfully provided and is not bundled by default.[65] This may require such consent to be provided as an 'opt-in' instead of an 'opt-out'. This would set the default to a passenger's data not being shared with a third party, unless they authorise and consent to such sharing through the opt-in. Opt-in mechanisms reduce the chances of consent being provided under ignorance of the implications.

2. Aadhar based authentication

a. The Digi Yatra Policy states that the Digi Yatra Foundation shall obtain the licence to act as an Authentication User Agency ('AUA') under Section 4 of the Aadhaar Act, 2016 and regulations thereunder.[66]

b. In its capacity as an AUA, the Digi Yatra Foundation must comply with all provisions of the Aadhaar Act, 2016 and its regulations, including the Aadhaar (Authentication) Regulations, 2016, in relation to issues such as user consent, storage of data, maintenance of logs and data security.

[63] *Justice KS Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, Part S, para 180*

[64] *Ministry of Civil Aviation, '"Digi Yatra Biometric Boarding System" Reimagining Air Travel in India' (4 March 2021) v 7.5*

[65] *Ministry of Civil Aviation, '"Digi Yatra Biometric Boarding System" Reimagining Air Travel in India' (4 March 2021) v 7.5*

[66] *Sec 4, Aadhaar Act, 2016*

3. Information security

a. The collection, storage and use of sensitive personal data, such as facial biometrics, enhances the need to ensure robust and state-of-the-art information security throughout the Digi Yatra Central Ecosystem. The legal requirements in relation to information security practices are presently set out in the SPDI Rules, particularly, under Rule 7 of the SPDI Rules.[67]

b. The Digi Yatra Policy states that it shall adopt end-to-end, peer-to-peer encrypted communication which complies with existing legal standards. It also makes reference to privacy-by-design and privacy-by-default, and outlines some envisaged measures related to data security in the chapter on High Level Data Privacy.[68]

c. Importantly, there must be frequent cybersecurity audits and vulnerability testing of the Digi Yatra platform to ensure that reliability, usability, information security in the ecosystem is a subject of continuous engagement and is adaptive to the rapidly evolving threats that exist in this sphere. In addition to cybersecurity audits, it is imperative to establish a mechanism for performing algorithmic audits by independent and accredited auditors, prior to system deployment at periodic intervals.

d. Successful passenger enrolment on the Digi Yatra app shall create a secure digital identity wallet on the smartphone of the user, using public-private key pair encryption. Additional measures such as the use of self-sovereign identity to provide for greater individual control over digital identities, and the use of blockchain technology to help verify the credentials provided by Indian passengers (which are already part of the Digi Yatra Central Ecosystem) seek to improve the security and reliability of the Digi Yatra process.

While these are some crucial legal issues likely to emerge from the Digi Yatra ecosystem's interaction with Indian legislation, per the scope of this Paper, it is not deep diving into a detailed analysis of compliance vis-à-vis the Aadhaar Act, 2016 or the IT Act, 2000. Therefore, these points are merely highlighted here without offering detailed analysis of the same.

[67] *Rule 7, SPDI Rules*

[68] *Ministry of Civil Aviation, '"Digi Yatra Biometric Boarding System" Reimagining Air Travel in India' (4 March 2021) v 7.5*

D. RAI principles and Digi Yatra: Evaluation and Recommendations

The responsible AI principles discussed earlier in this Paper, have been developed by first identifying systemic considerations prevalent among AI systems across the world, and identifying principles that may be used to mitigate the identified considerations. The following table contains brief explanations of how each of these principles are relevant and links them to the proposed SOP emerging from the Digi Yatra policy document(s). It also examines Digi Yatra against the aforementioned systems considerations, sets out existing mitigation measures and recommends additional measures to mitigate the risks relating to various responsible AI principles.

Table 2.1: Digi Yatra and RAI principles: Evaluation and measures to improve compliance

Responsible AI principle + explanation	Relevant systems failure considerations	Risk mitigation measures currently under Digi Yatra	Recommendations for further mitigation of risks under Digi Yatra
Principle of Safety and Reliability: AI systems must ensure reliability regarding their intended functions and must have built-in safeguards to ensure the safety of stakeholders.	Understanding functioning for safe and reliable deployment Security risks	The policy specifies that FRT readers must comply with the 'ISO/IEC 19794-5:2011' standard, which is the ISO standard for qualitative dimensions of face image data, which contains guidelines such as the standard way to capture facial images.	• An agency must be identified as responsible for publishing the standards to be followed by the FRT model relating to explainability, bias and errors. • False negatives and false positives can arise from mislabelling data in the training dataset or the actual dataset in use. Creation of standardised, annotated, high quality images to train and evaluate face recognition technologies for Indian context must be encouraged. • A mechanism must be instituted to ensure customer feedback can be obtained in an ongoing manner. This could be through usage monitoring, in-app-feedback mechanism, etc.

Principle of Equality: AI systems must be built keeping in mind that similar people in similar circumstances are treated equally.	Consistency across stakeholders	There are exceptional handling processes for persons with disabilities and for senior citizens. Introduction of DY-BBS system should not impact passengers with valid travel credentials from travelling. In case of non-enrolment or technology failures, passengers have an option to undergo manual checking.	• Consent for creating a credentials should not be given by the 'head of the family' in lieu of adults such as spouses or dependent parents, as the latter are capable of exercising their right to consent. • A prospective data protection law should clarify the requirement of explicit consent. This would be similar to clause 11(2)(c) of the (now withdrawn) PDP Bill requiring consent to be clear, i.e., meaningful consent indicated through affirmative action. • Explicit consent of spouses or adult dependents by the Digi Yatra program prior to creating their credentials, should be a mandatory prerequisite to processing sensitive personal data in a legal and authorised manner.

Principle of Inclusivity and Non-discrimination: AI systems must be developed to be inclusive of all stakeholders, and must not discriminate through bias between stakeholders on religion, race, caste, sex, descent, place of birth or residence in matters of education, employment, access to public spaces etc.	Incorrect decisions leading to exclusion from access	• The DYCE Challenge was launched by Niti Aayog in order to invite entities to submit algorithms for evaluation. In this process, the challenge provides training sets and validation sets from the Disguised Faces in the Wild dataset, containing 11,157 face images of 1,000 subjects with varying levels of intentional and unintentional distortions to mimic real-world scenarios and improve accuracy.69 • The first authentication is carried out by human involvement (CISF personnel at the airport), and an individual can opt-out of the Digi Yatra program and go through a non-biometric process offering human (CISF security officer) authentication.	• Standards to avoid bias in the FRT model must be developed, and a body must be identified to create and maintain the standard. The standards for representativeness of the datasets used for training the FRT system must be identified. • While at present Digi Yatra offers a continued alternative to get identity verification, ticket checking etc. to be conducted manually, this should be a feature retained in the long run. This is particularly important keeping in mind the digital divide across sections of population in India and ensuring the Digi Yatra Central Ecosystem does not become exclusionary at any point of its implementation. • Notice and information around collection of data and its processing, at all stages of the Digi Yatra life cycle, must be furnished in a clear and concise format, preferably in English and at least one local vernacular, to ensure meaningful consent and to emphasise the voluntary aspect of the Digi Yatra project

[69] Maneet Singh et al, *'Recognizing Disguised Faces in the Wild'* (21 November 2018) <https://arxiv.org/pdf/1811.08837.pdf> accessed 23 June 2022

Principle of Privacy and Security: AI systems must ensure that the personal data of data subjects must be safe and secure, such that only authorised persons must access personal data for specified and necessary purposes, within a framework of sufficient safeguards to ensure this process.	Privacy risks Security risks	• The policy explains its compliance with data protection laws and standards. • The travel credential is stored locally on the passenger's smartphone. • Passengers have the choice of opting out of the Digi Yatra process. • Travel data is deleted 24 hours post departure.	• Internal SOPs for handling personal and sensitive personal data must be identified. • Although DY-BBS is required to delete biometric data 24 hours after the passenger's journey, the privacy guidelines states that "DYBBS shall have an ability to change the data purge settings based on security requirements on a need basis." • The Digi Yatra SOP must specify timelines and purposes for retention of different types of data within the Digi Yatra Central Ecosystem, beyond which personal data is deleted. • Any security-based exceptions should be clearly identified by the proposed ethics committee and must be set out within the SOPs. This should be a continuous process that is updated regularly as deemed necessary. The Ethics Committee can undertake this periodic review. • 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. Opting in provides the user with a more active choice and less transactional costs for protecting their privacy. While the Digi Yatra policy provides this presently, such status should remain consistent.
Principle of Transparency The design and training of AI systems is key for its functioning. The system must be audited and be capable of external scrutiny to ensure that the deployment of the AI system is impartial, accountable	Post-deployment explainability	There is a provision for audits and assessments by "independent teams" and government agencies to assess security, privacy, and system resilience.	• The nature of the independent teams that will perform security audits must be clearly specified, including provisions for non-governmental audits. • Explainability of model must be considered and the extent and level of necessary transparency must be identified. • The possibility and likelihood of errors, and the SOP in case of such errors should be specified in the policy.

impartial, accountable and free from bias or inaccuracies.			
Principle of Accountability Since there are various actors in the process of developing, deploying and operationalizing an AI system, the accountability structures for any effects, harms or damages by the AI system must be clearly set out in a publicly accessible and understandable manner.	Accountability of AI decisions	A complaints API system is conceptualised as part of the open API ecosystem for Digi Yatra. This system exists for passenger complaints towards airlines or OTAs.	• The Digi Yatra ecosystem should have an adequate grievance redressal mechanism, with clear first instance complaints' framework, and an appellate process. This should be in addition to the complaints API system currently discussed in the Policy. • There must be a provision for the ongoing monitoring of the performance of the entire system. • Vendors providing the additional value-added services (with explicit consent) must be obligated to ensure protections for facial data and other relevant subject data. This may be achieved by setting out clear licensing requirements between Digi Yatra Foundation and the third-party vendors prior to sharing any sensitive personal data. • Terms of reference for soliciting third party vendors providing value-added services should include a requirement to agree with the licensing agreements and data security agreements with Digi Yatra Foundation.

Principle of Protection and Reinforcement of Positive Human Values: This principle focuses on the possible deleterious effects of AI systems through collection of personal data for profiling, the use of AI systems in manners contrary to fundamental rights guaranteed by the constitution of India.			• If newer data processing future, an individual shoul their consent or delete th ecosystem. This prescriptio limitation sought to be ach protection regimes. • The privacy guidelines und for the sharing of passen agency, the central gove agency based on curre existing at that time.[70] It i such data sharing must be and privacy principles lai judgement, and the existing in conformity with the thre this judgement. • In this regard, the foregoin Digi Yatra SOP must set o norms and the protocols in data is shared. The ethic appropriate entity to dra sharing protocols.

[70] P 47, 50, Ministry of Civil Aviation, '"Digi Yatra Biometric Boarding System" Reimagining Air Travel in India' (4 March 2021) v 7.5

E. Actionable recommendations to ensure responsible use of FRT in future applications

While the previous sections delve specifically into the Digi Yatra use case, it is imperative to also establish more common actionable recommendations around the use of facial recognition in other avenues by the state. Based on the Responsible AI principles, as well as the risks associated with FRT systems, this section prescribes the following recommendations regarding i). legislation and policymaking; ii). design and development of FRT systems for public sector; iii) procurement processes; and iv). consumers impacted. As a handbook document, it is the intention of this Paper to serve as a template for future frameworks envisioning enforcement of the aforementioned principles.

1. Recommendations for governing legislation and policy

FRT systems are inherently data intensive technologies (mostly algorithmic in design). Given the need for sensitive biometric datasets for the design and development of these systems, and also their subsequent usage on potential visual or graphic data sets for verification or monitoring purposes, there is an imperative need for a strong legal framework for personal data protection. Furthermore, to ensure holistic governance, a whole-of-government approach to legislation and regulation should be adopted, rather than piecemeal statutes emerging in silos and in conflict of each other. Accordingly, the following recommendations are made for legislation and policies around the use of FRT systems:

A. Legal Reform

a. Principle of privacy and security

i. **Establishing a data protection regime:** In 2019, the Indian government introduced the PDP Bill in Parliament, which has subsequently been withdrawn this year. The government has clarified that this withdrawal is temporary, and a new data protection bill will be reintroduced in the Parliament. It is pertinent to mention that FRT like other intelligent algorithms, is fundamentally a data intensive technology. In order to ensure propriety and legality in the manner in which data processing happens to train and develop FRT systems, it is imperative to have a codified data protection regime in the country at the earliest. The new data protection bill must retain the framework to ensure data protection, including obligations, enforcement mechanisms, a regulatory agency, penalties, and remedies from the PDP Bill, 2019. Furthermore, such a regime must not be limited to regulating data processing by private entities but must adequately

on is in line with the purpose
hieved under established data

der the Digi Yatra SOP allow
nger data with any security
rnment or any government
ent protocols or protocols
s important to note that any
e in accordance with the law
d down in the Puttaswamy
g protocols must be designed
e-pronged test established in

ng protocols specified in the
out inter-agency data sharing
n place when such passenger
cs committee could be the
aft these inter-agency data

codify protections for fundamental right to privacy against state agencies (including law enforcement). Sensitive personal data should be protected under the new data protection law, including biometric data such as facial images and scans. Consequently, it is recommended that rigorous standards for data processing, as well as the storage and retention of sensitive biometric data should be adequately addressed in any proposed data protection regime, to address privacy risks associated with FRT systems.

ii. **Legality, reasonability, proportionality:** In addition to the PDP Bill, the Supreme Court has adequately set out a three-pronged test of legality, reasonability, and proportionality in the Puttaswamy judgement. Furthermore, to determine proportionality, as discussed earlier in this paper, the Supreme Court stipulated four identifiers (i.e., legitimate goal; the suitability of the proposed intervention in furthering that goal; whether it is the least restrictive but effective alternative; and whether it does not have a disproportionate impact on the right holder). These tests must be used to evaluate any state action restraining the fundamental right to privacy. Any ongoing or future application of FRT systems by governments in India, must be compliant with the three-pronged test, as well as the aforementioned proportionality identifiers, in order to ensure constitutional validity. The RAI principles also place high value on constitutional morality, i.e., compliance with constitutional ethos, and as such, an application directly of the three-pronged test, would fail to align with the idea of responsible AI.

b. Principle of accountability

Regulating non-privacy risks of FRT systems: While the PDP Bill aims to address the privacy related risks, it does not, and should not directly address issues including transparency, algorithmic accountability, and AI bias emanating from the use of AI systems. These issues warrant separate regulation, either through codes of practice, industry manuals and self-regulation, or through more formal modes like statue and rules made thereunder. The objective is to create a holistic governance framework addressing the multifaceted challenges posed by FRT systems.

B. Policy reform

a. Principle of transparency

Ensuring transparency in the deployment of public FRT systems: A significant concern around FRT systems is the surreptitious nature of their deployment. With Digi Yatra, the disclosure of its systems and its intricate functionalities, which have been captured in the Digi Yatra Policy, has proven to be a strong positive, allowing clarity of its usage as well as building an infrastructure of trust. Other ongoing and prospective applications of FRT systems must follow similar suit of putting adequate information in the public domain. There are some obvious exemptions to this recommendation, for instance when time sensitive surveillance may be necessary to offset some critical security threat or diffuse a law-and-order situation. That said, transparency around the deployment of FRT systems in the public domain must be a norm followed at the central and state level. This is necessary for individuals to exercise their informational autonomy (and the right to privacy) as well as securing public trust in the development and deployment of such systems, which is intrinsic to the concept of responsible AI.

b. Principle of protection and reinforcement of positive human values

Constituting an experts' committee: NITI Aayog's Responsible AI approach paper recommends that organisations deploying an AI system can constitute an ethical committee to assess the ethical implications and oversee mitigation measures. Specifically, for FRT systems, it is imperative that such committees are constituted and given adequate autonomy to prescribe guidelines and codes of practice to ensure compliance with RAI principles. This is also crucial for ensuring India develops and leads thought leadership around FRT governance and regulation at an international level as well. Specifically, such committees should be responsible for:

a. Drafting guidelines for explainable and transparent FRT within the proposed use case.

b. Drafting standards for training database representativeness, public audits for fairness and acceptable error rates for the facial recognition system.

c. Serving as the first layer of oversight regarding the use of FRT, to ensure compliance with the proposed SOPs.

d. Developing the document establishing the aforementioned accountability structure, including details of grievance redressal frameworks, possible remedies available, and other pertinent details for setting out this structure.

e. Publishing annual report(s), *inter alia*, setting out details around procurement processes and use of FRT in a year.

f. Having residuary powers to prescribe standards, guidelines, or measures with evolving use of FRT.

2. Recommendations for developers and vendors of FRT systems

In addition to the policy and legislative recommendations, it is crucial to identify the other stakeholders in the life cycle of deploying an FRT system. Foremost among these are the developers and vendors who are responsible for mitigating design biases, usage of adequate and high-quality datasets in compliance with data protection norms and embedding ethics-by-design in such systems. With respect to developers and vendors, the Paper proposes the following recommendations:

a. **Principle of transparency**

i. **Explainable FRT systems:** Developers must build FRT systems that are explainable, i.e., the decision-making process of the system regarding a particular case output can be accurately explained to an auditor or judge. In this regard, the explainability of the AI system can be based on the following principles[71]:

- *Self-explainable:* The AI system must be developed in a manner that it is *per se* capable of providing an explanation, evidence, or reasoning for each of its outputs, in a lucid and clear manner. This does not necessarily mean disclosure of the entire algorithm, but disclosure of details about the input factors that were considered in the decision-making process. For a FRT system, this would include denoting the facial regions that contributed to the match and the degree of their contribution[72];
- *Meaningful:* The AI system must be developed in a manner that it is capable of providing explanations, evidence or reasoning which are meaningful and understandable to the operators as well as the recipients of outcomes produced by such an AI system. For a FRT system, this would mean providing a humanly understandable map of facial regions according to their contribution to the match; and
- *Explanation accuracy:* The explanations provided by the AI system must correctly reflect the actual decision-making process due to which the AI system arrived at its output.

Vendors may utilise different models for explainability or interpretability of underlying algorithmic models, like Local Interpretable Model-agnostic Explanations (LIME). Fundamentally, these models can indicate the why certain predictions or outputs were generated by an FRT system, and what variables it relied upon, while formulating this output.

ii. **Knowledge limits:** The AI system must only operate and provide its output (i) under the conditions for which it was designed (to avoid errors based on technical factors such as occlusion, poor

[71] These principles have been adapted from the 'Four Principles on Explainable Artificial Intelligence' developed by the National Institute of Standards and Technology under the aegis of the US Department of Commerce, available at <https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8312.pdf>

[72] Jonathan Williford et al 'Explainable Face Recognition' (August 2020) <https://arxiv.org/pdf/2008.00916.pdf>

lighting etc.) and (ii) when it reaches a certain percentage or level of confidence in its output or actions. For a FRT system, this would mean that if a predetermined confidence level is not reached, the software may not provide an output**.** The design of the AI system must include adequately stated knowledge limits, or areas for which the base algorithm is untested for, and consequently, wherein the AI system may fail to act due to lack of sufficient knowledge or any perturbations.

b. Principle of accountability

i. **Internal ethical committees:** The developer entity (typically a start-up or private company) must constitute an independent, internal ethics committee which serves as an oversight board to ensure ethical design and development of FRT systems. This committee would be separate from the ethics committee discussed previously, which would most like be established by the procuring state agency, rather than the developer/vendor. Such ethics committees should be responsible for establishing robust internal governance processes for vendors, addressing issues like sourcing of data in a lawful manner, building ethical and responsible FRT systems, incorporating privacy by design, and maintaining records and audit trails on AI models developed while designing the final FRT system.

ii. **System audits:** A key component to establish accountability and safety of AI systems in general, and FRT systems specifically, would be to subject the underlying algorithm, training datasets, and other functional features of the system, to periodic, external, technical audits. Audits serve as a self-regulatory, light touch measure which can meaningfully evaluate any flaws or risks in the FRT system in a timely manner and ensure rectification of the same. They also serve as independent measures of the risks posed by a particular FRT system, which allows an informed decision around its deployment. Such audits may also cover the internal governance process that includes how they source, build, deploy, and maintain their data and AI models.

c. Principles of inclusion and non-discrimination

i. **Customised for Indian use cases:** Developers must consider the realities of the Indian population in training the AI model. The model must ensure accurate and inclusive identification, for e.g., based on gender. The vendor must provide accuracy rates according to segments of Indian face types, genders, age, and so on.

ii. **Human in the loop:** There must be an integral mechanism for human review built into the AI system for specific cases wherein its utility and accuracy may be in question. A human reviewer should be enabled to take over such specific cases and prevent AI systems from making decisions without having sufficient expertise in the data presented to it.

d. Principle of privacy and security

i. **Privacy by design (PBD):** PBD principles must be followed, and a document explaining the PBD policy and other privacy, and data protection principles used by the developers in developing the AI system must be made publicly accessible. Such a document should have a summary version available in a clear and concise manner.

PBD would include collection of the user's consent prior to processing personal information; collection of the user's explicit consent if the collected data (including the reference biometric datasets and the live biometric data) is being used for a different purpose than for which it was collected by the organisation, and in no circumstances such consent for biometrics should be inferred from conduct of a data principal; and collection of consent while collecting and processing the facial data and any insights gleaned from it, including transferring, licensing, or permitting external agencies to access the data, when the collection or processing is not for the purpose consented to by the user.

ii. **Additional value-added services:** Vendors providing the additional value-added services (with explicit consent) must be obligated to ensure protections for facial data and other relevant subject data. This may be achieved by setting out clear licensing requirements between the procuring agency and the third-party vendors prior to sharing any sensitive personal data. Further, the terms of reference for soliciting third party vendors providing value-added services must include a requirement to agree with the licensing agreements and data security agreements which bind the original vendor/developer.

The use of facial recognition data and other relevant subject data for providing value added services must be activated through an opt-in rather than an opt-out method of consent with an ability to revoke consent at any time. Opting in provides the user with a more active choice and less transactional costs for protecting their privacy.

3. Recommendations for procurement

Responsible and accountable procurement processes for FRT can minimise harms by filtering out substandard technology. Accordingly, the following recommendations are made for the procurement process for any prospective usages of FRT systems. The following recommendations have also been sourced from the procurement norms followed globally[73], as well as from global best practices[74]:

a. Principle of transparency

i. **Transparent procurement processes:** The procurement of the facial recognition technology must be carried out in a transparent manner with periodic public disclosures of the criteria and processes followed. The responsibilities of the vendor of the facial recognition system (if any) with respect to effectiveness, errors, bias and transparency, must be clearly specified in the contract and as a matter of public record.

ii. **Detailed RFPs:** The procuring entity must provide a clear problem statement while issuing a call for Request for Proposals (RFPs), as opposed to seeking a specific solution. This allows vendor entities to suggest alternative approaches to the problem statement and provides options to the procuring entity. The RFP must set out the need for AI and clearly show how public benefit is better achievable through the use of AI. This clarifies and reiterates the purpose of public benefit and necessity in introducing the AI system to vendor entities. Further, the RFP must be informed by an initial risk and impact assessment before starting the procurement process, which must be revised at future decision points.

iii. **Error rate disclosures:** The overall error rate and error rate for different demographics for the facial recognition technology must be continuously evaluated and disclosed to the public.

b. Principle of safety and reliability

i. **Access controls:** The procuring entity must decide and define data governance and access terms for the project prior to selecting a vendor. The access control terms determine how data shall be shared with vendors for the project, while the data governance

[73] *Office for Artificial Intelligence, United Kingdom 'Guidelines for AI Procurement' (June 2020) v1.7x <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/990469/Guidelines_for_AI_procurement.pdf>*

[74] *World Economic Forum 'White Paper- Guidelines for AI Procurement' (September 2019) <https://www3.weforum.org/docs/WEF_Guidelines_for_AI_Procurement.pdf>*

aspect shall provide greater accountability and transparency on how the shared data is processed by the vendor.

ii. **Risk mitigation requirements:** The RFP must highlight susceptible risks and ethical issues in the potential operations of the AI system and seek mitigation strategies from vendors as part of the proposal. In selecting the vendor, the procuring entity must ensure that the AI system is interoperable with current and future system upgrades. The procuring entity must also remain open for collaboration with other vendors and avoid vendor lock-in issues. Vendors that provide AI systems which are interoperable must therefore be prioritised.

c. Principle of accountability

i. **Compliance with RAI principles:** The procuring entity must ensure that the RFP and the AI system being deployed under this project is in line with government strategy papers such as the National Strategy for AI, 201875 and the Responsible AI 2021 papers[76].

ii. **Compliance with governing laws:** The procuring entity must seek proposals that allow for scrutiny into the AI system during its life cycle such that its operational life-cycle is compatible with current laws, codes of practice or government AI policies.

iii. **Performance monitoring and evaluation:** The performance and use of the facial recognition system must be monitored by governmental and non-governmental independent agencies regularly against a set of defined criteria, with provisions for policy change in response to the monitoring. It is important that the criteria, as well as such evaluations, are undertaken by independent and accredited bodies, in line with international best practices.

4. Recommendations for Impacted consumers

The final set of stakeholders pertinent to this discussion around actionable recommendations, are consumers who are likely to be impacted by the use of FRT systems. It is crucial that such consumers are able to hold the deployers and developers of FRT systems, accountable. As such the following recommendations are made.

[75] Niti Aayog 'National Strategy for Artificial Intelligence' (June 2018) <https://indiaai.gov.in/documents/pdf/NationalStrategy-for-AI-Discussion-Paper.pdf>

[76] Niti Aayog 'Approach Document for India Part 1 – Principles for Responsible AI' (February 2021) <https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf>; Niti Aayog 'Approach Document for India: Part 2 - Operationalizing Principles for Responsible AI' (August 2021) <https://www.niti.gov.in/sites/default/files/2021-08/Part2-Responsible-AI-12082021.pdf>

ANNEXURES

a. Principle of accountability

i. **Grievance redressal frameworks:** For ensuring accountability in the development and deployment of an FRT system, it is crucial to establish an easy-to-use and accessible grievance redressal system. Such a mechanism must allow for the adjudication of any problems (including, but not limited to inaccurate outcomes denying access to an individual). As aforementioned, there are innate functional risks posed by FRT systems. Some of these may have constitutional remedies (say violation of privacy, or discriminatory outcomes) but some may require a more informal first instance complaints mechanism. In this regard, having an ombudsman allows for a simple and accessible point for grievance redressal, and depending on the severity of the complaint, the same may be elevated to a constitutional court. Ongoing and future applications of FRT systems must ensure that their deployment is accompanied with adequate grievance redressal frameworks, facilitating meaningful accountability, and a system of checks and balances.

ii. **Feedback loops:** Interlinked to accountability is the notion of infrastructure of trust. A common critique against FRT systems is the lack of public faith and confidence in their responsible use, with purpose and scope limitation. Any application of FRT systems, especially in the public sector, must be in concomitance with trust building measures. Crucial to this exercise are feedback loops and surveys. Public agencies or institutions deploying FRT systems must integrate appropriate feedback mechanisms into their ecosystem, which in turn must feed into periodic impact evaluations of such systems.

ANNEX 1- *EXAMPLES OF FRT SYSTEMS DEPLOYED IN INDIA*

S. No.	Region	Project Name	Sector it operates on	Status of Project	Commence-ment of the Project	Organization
1.	India	**National Automated Facial Recognition System (AFRS)**	Law enforcement- prevention and detection of crime and fast track document verification	Proposed project; Request for Proposal has been released to public[77]	Yet to commence	National Crime Records Bureau
2.	India	**Face Matching Technology**	Educational- identity authentication to access academic documents[78]	Implemented[79]	2020	Central Board for Secondary Education
3.	Telangana	**Degree Online Services Telangana**	Educational- identity authentication to access academic documents for Telangana State Board of Intermediate Education students.[80]	Implemented	2020	Telangana State Board of Intermediate Education
4.	Punjab	**PAIS**	Law enforcement- real-time identification of criminals, phonetic search and gang analysis	Implemented[81]	2018	Punjab Police

[77] *National Crime Records Bureau, 'Request for Proposal to procure National Automated Facial Recognition System (AFRS)' 02/001, Ministry of Home Affairs <https://ncrb.gov.in/sites/default/files/tender/AFRSRFPDate22062020UploadedVersion.pdf> accessed 17 November 2021*

[78] *Director IT & Projects 'Availability of Digital Academic Documents using "Face Matching Technology"' Central Board of Secondary Education <https://www.cbse.gov.in/cbsenew/documents/Face%20Matching%20Technology.pdf> accessed 17 November 2021*

[79] *Education Desk, 'CBSE introduces facial recognition system for accessing digital documents' (New Delhi, 22 October 2020) The Indian Express <https://indianexpress.com/article/education/cbse-introduces-facial-recognition-system-for-accessing-digital-documents-cbse-nic-in-6838840/> accessed 17 November 2021*

[80] *ETGovernment, 'Telangana: Degree admissions process through facial recognition system' (23 June 2020) Economic Times <https://government.economictimes.indiatimes.com/news/technology/ telangana-degree-admissions-process-through-facial-recognition-system/76525867> accessed 24 November 2021*

[81] *HT Correspondent, 'Patiala Police nab 2 criminals using face recognition app' (Patiala, 1 June 2020) Hindustan Times <https://www.hindustantimes.com/chandigarh/patiala-police-nab-2-criminals -using-face-recognition-app/story-ZiGYD3Bh0GzUbSPls5S2JJ.html> accessed 19 November 2021*

5.	Chennai and Madurai, Tamil Nadu	**FaceTagr**	Law enforcement- mobile application to match suspect photos against pre-existing crime records and CCTV footage.[82]	Implemented83	2017	Tamil Nadu Police
6.	Uttar Pradesh	**Trinetra**	Law enforcement- real-time identification of criminals	Implemented[84]	2018	Uttar Pradesh Police
7.	Maharashtra, Gujarat	**Indian Protocol Surveillance System**	Law enforcement- surveillance of individuals with the objective of ensuring women safety at railway stations[85]	Pilot project	2021	Indian Railways
8.	Telangana	**Face Recognition Application**	Authentication- additional tool in authenticating individuals in civic elections against the electoral rolls[86]	Pilot project	2020	Telangana State Election Commission
9.	India	**Authentication Based Facial Recognition**	Authentication: ease of authentication for Aadhar card[87]	Pilot project	2018	UIDAI

[82] *Jayanthi Pawar 'Facetagr app: Chennai police's bright spark helps nab elusive criminals' (4 July 2018) The New Indian Express <https://www.newindianexpress.com/cities/chennai/ 2018/jul/04/facetagr-app-chennai-polices-bright-spark-helps-nab-elusive-criminals-1837928.html> accessed 23 November 2021*

[83] *ANI, 'Madurai Police Launches Facial Recognition App To Reduce Crime Rate' (Tamil Nadu, 26 September 2020) NDTV <https://www.ndtv.com/tamil-nadu-news/madurai-police-launches-facial- recognition-app-facetagr-to-reduce-crime-rate-2301538> accessed 23 November 2021*

[84] *Newsdesk, 'Staqu launches TRINETRA, an AI app for UP Police Department' (29 December 2018) Deccan Chronicle <https://www.deccanchronicle.com/technology/in-other-news/291218/staqu-launches-trinetra-an-ai-app-for-up-police-department.html> accessed 17 November 2021*

[85] *Bharat Sharma, 'Indian Railways Has Installed 500 Face Recognition Cameras In Gujarat, Maharashtra' (29 August 2021) India Times <https://www.indiatimes.com/technology/news/indian-railways-face-recognition-cameras-gujarat-maharashtra-548157.html> accessed 18 November 2021*

[86] *Telangana State Election Commission, 'TSEC-Face Recognition Application' (18 January 2020) Circular 111/TSEC- ULBs/2020 <https://tsec.gov.in/pdf/ULBS_MPLTS/circulars/2020/Cir_No_111_TSEC-ULBs_2020_dated_18.01.2020_1401.pdf> accessed 10 December 2021*

[87] *Newsdesk, 'UIDAI introducing facial recognition for Aadhaar authentication will ensure greater inclusion' (New Delhi, 25 August 2018) Financial Express <https://www.financialexpress.com/opinion/uidai-introducing-facial-recognition-for-aadhaar-authentication-will-ensure-greater-inclusion/1291516/> accessed 18 November 2021*

10.	India	**Authentication Based Facial Recognition**	Authentication- biometric authentication of Covid-19 vaccine recipients	Pilot Project launched in Jharkhand88	2021	UIDAI
11.	Telangana	**Real Time Digital Authentication of Identity**	Authentication- Authenticating the 'dead-or-alive' status of pension claimants under the T-folio app.[89]	Implemented as a voluntary program	2020	ITE&C Department, Telangana
12.	Prayagraj, Uttar Pradesh	**Pan Tilt and Zoom Surveillance Cameras**	Law enforcement- surveillance and maintenance of large crowds[90]	One-time functional project used in Kumbh Mela, 2021	2021	Uttar Pradesh Police
13.	New Delhi	**AI Vision**	Law enforcement- identifying criminals and detecting lost children	Functional Project[91]	2017	Delhi Police
14.	Vijayawada, Andhra Pradesh	**Facial Recognition Software**	Authentication- Attendance of sanitary workers[92]	Pilot Project	2021	Vijayawada Municipal Corporation

[88] *India Today Tech, 'Aadhaar face recognition could be made mandatory for COVID vaccination, pilot testing is on' (New Delhi, 9 April 2021) India Today <https://www.indiatoday.in/technology/news/story/aadhaar-face-recognition-could-be-made-mandatory-for-covid-vaccination-pilot-testing-is-on-1789024-2021-04-09> accessed 18 November 2021*

[89] *TSTRANSCO, 'Pensioners Life Authentication using T App Folio (Submission of Digital Life Certificate) Help Document' Transmission Corporation of Telangana Limited <https://www.tstransco.in/it_uploads/Help_Pensioners.pdf> accessed 24 November 2021*

[90] *Web Desk, 'Artificial Intelligence real showstopper of Kumbh Mela 2019' (New Delhi, 14 March 2019) India Today <https://www.indiatoday.in/india/story/kumbh-2019-mela-artificial-intelligence-record-1477774-2019-03-14> accessed 5 December 2021*

[91] *Alexandra Ulmer, Zeba Siddiqui, 'India's use of facial recognition tech during protests causes stir' (Mumbai/ New Delhi, 17 February 2020) Reuters <https://www.reuters.com/article/us-india-citizenship -protests-technology-idUSKBN20B0ZQ> accessed 17 November 2021*

[92] *Express News Service, 'Face recognition attendance system for VMC sanitary workers' (Vijayawada, 15 April 2021) The New Indian Express <https://www.newindianexpress.com/cities/vijayawada/2021/apr/15/face-recognition-attendance-system-for-vmc-sanitary-workers-2290095.html> accessed 18 November 2021*

14.	Pune, Maharashtra	**Selfie-App Based Face Recognition**	Monitoring- drones used to monitor quarantine adherence by COVID-19 positive patients[93]	Pilot Project	2020	Pune Municipal Corporation and Pune Police
15.	Telangana	**Darpan**	Identification- Used to match photos and identify missing children.[94]	Implemented[95]	2018	Telangana Police
16.	Surat, Gujarat	**Surat Safe City Project**	Surveillance: LFRT that integrates live video surveillance feeds[96] against a watchlist of suspected individuals.[97]	Implemented	2015	Gujarat Police

[93] *Steffy Thevar, 'Drones, video calls, GPS tracking app and even personal visits: Pune admin out on a limb to track those home quarantined' (Pune, 1 April 2020) Hindustan Times <https://www.hindustantimes.com/pune-news/drones-video-calls-gps-tracking-app-and-even-personal-visits-pune-admin-out-on-a- limb-to-track-those-home-quarantined/story-HOuhjXE7kmVvH3OICIM0BM.html> accessed 11 December 2021*

[94] *Women Safety Wing, Telangana Police <http://www.womensafetywing.telangana.gov.in/facial_recognition.html> accessed 15 December 2021*

[95] *Staff Reporter, 'TS police's tracking tool helps reunite teen with kin' (Hyderabad, 17 December 2018) The Hindu <https://www.thehindu.com/news /cities/Hyderabad/ts-polices-tracking-tool-helps-reunite-teen-with-kin/article25759403.ece> accessed 18 December 2021*

[96] *Rashi Varshney, 'eGov Watch: What does Face Recognition System in Surat mean?' (31 August 2015) Express Computer, <https://www.expresscomputer.in/features/egov-watch-what-does-face-recognition-system-in-surat-mean/13390/> accessed 3 January 2022*

[97] *Yagnesh Bharat Mehta, 'In a first, real-time facial recognition system launched by Surat police' (Surat, 19 July 2015) The Times of India <https://timesofindia.indiatimes.com/city/surat/in-a-first-real-time-facial-recognition-system-launched-by-surat-police/articleshow/48135306.cms> accessed 9 December 2021*

ANNEX 2- *Examples of FRT Systems Deployed in Other Jurisdictions*

S. No.	Region	Project Name	Sector it Operates on	Status of Project
1.	United Kingdom	**eGates**[98]	Immigration and Border Control System	Started in 2008
2.	United States of America	**Global Entry Program**[99]	Custom and Border Protection from Immigrants	Started in 2008. Plans to convert to a complete facial recognition method which will eliminate the need for presently used biometric fingerprints and passports.
3.	Dubai, UAE	**Biometric Passenger Journey**[100]	Immigration Sector	New project announced in 2018 in association with Emirates.
4.	Beijing, China	**SITA's Smart Path Facial Recognition System**[101]	Entire Passenger Journey- Check-in, Baggage Drop, Immigration, Security, Boarding	Started in 2020
5.	China	**Auxiliary Facial Recognition System**[102]	Check-in and Security Clearance	Adopted in 2018

[98] *UK Border Force, 'Guide to faster travel through the UK border' (14 October 2021) Government of UK <https://www.gov.uk/government/publications/coming-to-the-uk/faster-travel-through-the-uk-border#:~:text=There%20are%20over%20270%20eGates,quicker%20travel%20into%20the%20UK.&text=are%20either%3A,Korea%2C%20Switzerland%20or%20the%20USA> accessed 16 January 2022*

[99] *US Customs and Border Protection, 'ORD and MDW encourages travelers to use facial recognition' (2 August 2021) US Customs and Border Protection <https://www.cbp.gov/newsroom/local-media-release/ord-and-mdw-encourages-travelers-use-facial-recognition> accessed 16 January 2022*

[100] *Ali Al Shouk, 'Video: Retracing Dubai Airport's smart journey: From e-gates in 2002 to smart tunnel in 2018 and biometrics now' (23 Feburary 2021) Gulf News <https://gulfnews.com/uae/video-retracing-dubai-airports-smart-journey-from-e-gates-in-2002-to-smart-tunnel-in-2018-and-biometrics-now-1.77394030> accessed 16 January 2022*

[101] *Press Release, 'SITA Smart Path transforms the passenger experience at Beijing Capital International Airport' (20 August 2020) SITA AERO <https://www.sita.aero/pressroom/news-releases/sita-smart-path-transforms-the-passenger-experience-at-beijing-capital-international-airport-bcia/#:~:text=International%20Airport%20(BCIA)-,SITA%20Smart%20Path%20transforms%20the%20passenger,Beijing%20Capital%20International%20Airport%20(BCIA)&text=Biometrics%20and%20contactless%20technologies%20mean,in%20an%20entirely%20touchless%20experience.> accessed 16 January 2022*

[102] *Huaxia, 'China's civil aviation industry becomes smarter' (11 January 2022) Xinhua Net <http://www.xinhuanet.com/english/20220111/16d5e0f4c17f4bb69c74add-73b5ead39/c.html> accessed 16 January 2022*

6.	Japan	**Face Express**[103]	Check-in and Security Clearance	Operational since July 2021, pilot project
7.	Taiwan	**Biometric Boarding**[104]	Boarding	Started in March 2021, pilot project
8.	Canada	**Faces on the Move**[105]	Border Protection by prevention of people entering the country using fake identification	Pilot Project in 2016
9.	Brazil	**Embarque + Seguro 100% Digital Boarding System106**	Boarding Process	Started in June 2021, pilot project
10.	China	**Social Credit System**[107]	Identification and Large-Scale Tracking of Individuals	Started in 2014
11.	China	**Skynet Project**[108]	Surveillance and law enforcement	Started in 2005; expansion phase
12.	Germany	**INPOL-Z**[109]	Forensic identification	2009

[103] *Japan Times, 'Narita and Haneda airports start wider use of facial recognition' (19 July 2021) Japan Times <https://www.japantimes.co.jp/news/2021/07/19/national/japan-airports-facial-recognition/> accessed 16 January 2022*

[104] *Taiwan Today, 'Taiwan rolls out touchless boarding trials at Taipei Songshan Airport' (24 March 2021) Taiwan Today <https://taiwantoday.tw/news.php?unit=2,6,10,15,18&post=196718> accessed 16 January 2022*

[105] *Tom Cardoso and Colin Freeze, 'Ottawa tested facial recognition on millions of travellers at Toronto's Pearson airport in 2010' (19 July 2021) The Global and Mail <https://www.theglobeandmail.com/canada/article-ottawa-tested-facial-recognition-on-millions-of-travellers-at-torontos/#:~:text=exclusive-,Ottawa%20tested%20facial%20recognition%20on%20millions%20of,Toronto's%20Pearson%20airport%20in%202016&text=In%20an%20effort%20to%20identify,Pearson%20International%20Airport%20in%202016.> accessed 16 January 2022*

[106] *Business Wire, 'Brazil tests the world's first facial recognition shuttle service' (12 June 2020) Business Wire <https://www.businesswire.com/news/home/20210616005505/en/Brazil-Tests-the-Worlds-First-Facial-Recognition-Shuttle-Service> accessed 16 January 2022*

[107] *Victoria Adelmant, 'Social credit in China: Looking beyond the "Black Mirror" nightmare' (20 April 2020) Centre for Human Rights and Global Justice <https://chrgj.org/2021/04/20/social-credit-in-china-looking-beyond-the-black-mirror-nightmare/> accessed 16 January 2022*

[108] *Thomas J Ackerman, 'What is China's SKYNET (yes: it is what you think it is)' (10 May 2019) BGP4 <https://www.bgp4.com/2019/05/10/what-is-chinas-skynet-yes-it-is-what-you-think-it-is/> accessed 16 January 2022*

[109] *Matthias Monroy, 'Facial recognition at German police authorities increased by more than a third' <https://digit.site36.net/2021/01/20/facial-recognition-at-german-police-authorities-increased-by-more-than-a-third/> accessed 16 January 2022*

ANNEX 3- DESIGN-BASED RISKS

(Referencer to table 1.1)

13.	Florida, USA	**FACES**	Identification of Unknown Persons and Suspects	Started in 2001
14.	France	**TAJ**[110]	Forensic identification	Ongoing since 20
15.	Finland	**KASTU**[111]	Forensic identification	Started in May 20
16.	Hong Kong	**iOmniscient**[112]	Surveillance and law enforcement	Started in 2016
17.	Hungary	**Szitaköt**[113]	Surveillance and law enforcement	Started in 2019
18.	EU	**iBorderCtrl**[114]	Immigration and border management	Started in 2020

[110] *La Quadrature du Net, 'Facial recognition of protestors is already allowed' (18 November 2019) <https://www.laquadrature.net/2019/11/18/la-reconnaissance-faciale-des-manifestants-est-deja-autorisee/> 16 January 2022*

[111] *YLE News, 'Finnish police denied, then admitted using controversial face recognition app' (23 April 2021) YLE News <https://yle.fi/news/3-11899325> accessed 16 January 2022*

[112] *Rohit Yadav, 'Hong Kong police has facial recognition and citizens are worried about what comes next' (27 October 2019) Analytics India Magazine <https://analyticsindiamag.com/hong-kong-police-has-facial-recognition-citizens-are-worried-about-what-comes-next/> accessed 16 January 2022*

[113] *Abraham Vass, 'CCTV: Is it big brother or the eye of providence' Hungary Today <https://hungarytoday.hu/cctv-is-it-big-brother-or-the-eye-of-providence/> accessed 16 January 2022*

[114] *About Intel, 'EU funded technology violates fundamental rights' (22 April 2021) About Intel <https://aboutintel.eu/transparency-lawsuit-iborderctrl/> accessed 16 January 2022*

1. Inaccuracy due to technical factors

A typical FRT system works through the steps of face detection, feature extraction and face recognition. This involves detection of a face through image identification software, extraction and conversion of facial features into numerical representations, and the eventual mapping of that test image against the templatized or actual facial image present in the gallery image dataset. There are several factors that may affect the accuracy of an FRT system- which have broadly been categorised as 'intrinsic' and 'extrinsic' factors.[115]

Intrinsic factors are factors inherent to the person which may affect the accuracy of the FRT system. These include facial expression, aging, plastic surgery, or any disfigurement suffered by the person between the recording of their face in the gallery dataset and its generation as a test image on which an FRT system carries out its functions.[116] On the other hand, extrinsic factors indicate certain factors concerning the environment of the test image, including illumination, pose variation, occlusion, or quality of image.[117] The use of an FRT system may be affected by occlusion- a partial or complete obstruction, either natural or artificial, of the facial image. This may include growing a beard, wearing sun-glasses, masks, veils or scarves, or the placement of a mobile phone or any such object in front of the face.[118]

Occlusion gains relevance in the use of live FRT or use of FRT in security and monitoring applications where a person is not aware of, or is aware but has not consented to, the processing of their facial image and acts to protect their privacy. In an uncontrolled environment, recording the test image, gallery image, or a training image, would suffer due to issues of illumination and the lack of control over the pose and profile of the person.[119] As a result, illumination and occlusion are frequently cited as major factors that pose a

[115] *Muhammad Sharif et al, 'Face Recognition: A Survey' (2017) 10 (2) Journal of Engineering Science and Technology Review <https://pdfs.semanticscholar.org/bb86/bed5f8b98c65a4f882858 523bb8ee12ad6ba.pdf> accessed 11 November 2021; see also Jyri Rajamäki et al, 'Facial Recognition System as a Maritime Security Tool' (2009) delivered at Proceedings of the 8th WSEAS International Conference on Signal Processing <https://www.researchgate.net/profile/Jyri-Rajamaeki/publication/229016694_Facial_recognition_system_as_a_maritime_security_tool/links/53fec09f0cf283c3583be46d/Facial-recognition-system-as-a-maritime-security-tool.pdf> accessed 17 November 2021*

[116] *Shahina Anwarul, Susheela Dahiya, 'A Comprehensive Review on Face Recognition Methods and Factors Affecting Facial Recognition Accuracy' P. K. Singh et al. (eds) (2020) Proceedings of ICRIC 2019 <https://www.researchgate.net/publication/337446642_A_Comprehensive_Review_on_Face_ Recognition_Methods_and_Factors_Affecting_Facial_Recognition_Accuracy> accessed 18 December 2021*

[117] *Ibid; see also Piyush Choudhary, Poorva Agrawal and Gagandeep Kaur, 'Survey on SVM Based Method for Identification and Recognition of Faces by Using Feature Distances' (December 2019) <https://easychair.org/publications/preprint_open/cxp5> accessed 18 December 2021*

[118] *Piyush Choudhary, Poorva Agrawal and Gagandeep Kaur, 'Survey on SVM Based Method for Identification and Recognition of Faces by Using Feature Distances' (December 2019) <https://easychair.org/publications/preprint_open/cxp5> accessed 18 December 2021*

[119] *Smriti Parsheera, 'Adoption and regulation of facial recognition technologies in India: Why and why not?' (November 2019) Data Governance Network, Working Paper 05*

problem to the accuracy of an FRT system.[120] The propensity of these factors, and the consequences of inaccuracy, prompt careful reconsideration on the scenarios where an FRT system's outputs may be reliable and accurate.

2. Inaccuracy due to bias or underrepresentation

Further, racial and ethnic biases have been reported in various testing phases of FRT systems, with significant spikes of error rates for darker-skinned individuals. As explained in Section 1, AI systems are trained using machine learning, deep neural networks or other such models that rely extensively on training the computational ability and results of the system. In this regard, FRT systems are dependent on the neural networks developed through the training datasets to extract features and recognise faces. The accuracy of these exercises thus depends on the FRT system's prior experience, gained through training, on various types of facial samples.

This becomes an issue when an AI system encounters facial samples that it is unfamiliar with or has had little training on, and can be seen in instances where the training data underrepresents certain types of facial samples. For example, a study conducted on an FRT system tasked with binary gender classification- identifying whether an image was that of a male or a female, showed error rates of 0.8% for light-skinned men in contrast with 34% for dark-skinned women.[121] The FTR system used for this experiment was assessed based on a dataset which was over 77% male and over 83% white.

Further, racial categories have a contextual element to them, i.e. what would neatly be classified in one racial category in one geographical region (for example, Asian or South Asian in USA) would not be applicable or would be too broad a category in another region due to the breadth of that category, the *inter se* differentiation of various sub-categories in other regions, and the normative difficulty in categorising people based on sub-racial or sub-ethnic features.[122] An FRT system trained in one context, therefore, may have serious problems of underrepresentation when it is used in another context, as it may not be trained to evaluate the *inter se* distinctions within South Asians or East Asians, and is limited to the categories written into it.

The use of FRT systems in India thus requires both an awareness of the potential types of facial features prevalent across the country, and an

[120] SB Thorat et al, *'Facial Recognition Technology: An analysis with scope in India' (2010) 8(1) International Journal of Computer Science and Information Security <https://arxiv.org/ftp/arxiv/papers/1005/1005.4263.pdf> accessed 16 November 2021*

[121] *Larry Hardesty, 'Study finds gender and skin-type bias in commercial artificial-intelligence systems' (February 11, 2018) MIT News Office <https://news.mit.edu/2018/study-finds-gender-skin-type-bias- artificial-intelligence-systems-0212> accessed 22 November 2021*

[122] *Zaid Khan, Yun Fu, 'One Label, One Billion Faces: Usage and Consistency of Racial Categories in Computer Vision' delivered in proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency <https://arxiv.org/pdf/2102.02320.pdf> accessed 19 December 2021*

understanding of how certain facial features may be under-represented within training datasets used to train or evaluate the FRT system. Such studies could help reduce any bias inherent to FRT systems used within India, and identify necessary improvements to the FRT system to ensure inclusivity and fairness in its operations. These studies may be designed as iterative processes, with periodic reviews of data regarding the algorithmic accuracy, error rate and confidence levels chosen by the FRT system.[123] An audit conducted on four commercial FRT systems against Indian electoral rolls recently showed, on average, a gap in the error rate for identifying Indian men at 0.5% as against Indian women at 3%.[124] Given how the digital experience and access of each individual may vary based on a variety of factors including gender, ethnicity, class, caste, and religion, the development and use of FRT systems for public functions by the Indian government must account for a local understanding of algorithmic fairness in India.[125]

3. Inaccuracy due to lack of training of human agents

As discussed in Section 2, the decisions made by a human operator using any AI system are susceptible to automation bias or algorithmic complacency due to overcompliance or over-reliance on its abilities. In addition to these, FRT systems generally require engagement by a human operator who takes action on the basis of its results. The use of FRT systems by human operators has been observed to increase human bias in favour of the results by the FRT system.[126] Alternatively, the incorrect application of FRT systems may induce misidentification. Real-time instances of misidentification by FRT systems due to incorrect implementation have been noted in recent years.

In 2019, the photograph of a Brown University student in USA featured in a list of suspects wanted for questioning released to the press, following the Easter Sunday terrorist attacks in Sri Lanka. The photograph was soon retracted from the list as a mistake, with officials reportedly having used an FRT program which provided this result.[127] This was followed by a wrongful arrest made

[123] *Ameen Jauhar, 'Indian Law Enforcement's Ongoing Usage of Automated Facial Recognition Tech – Ethical Risks and Legal Challenges' (August 2021) Vidhi Working Paper 1*

[124] *Karishma Mehrotra, 'Indian faces were run through facial recognition tech tools. Here's why you should be concerned' (5 August 2021) Scroll <https://scroll.in/magazine/1001836/facial-recognition-technology-isnt-wholly-accurate-at-reading-indian-faces-find-researchers> accessed 18 December 2021*

[125] *Nithya Sambasivan et al. 'Re-imagining Algorithmic Fairness in India and Beyond' (2021) Presented at ACM Conference on Fairness, Accountability, and Transparency March 1-10, 2021, Canada <https://storage.googleapis.com/pub-tools-public-publication-data/pdf/d18d2d7bf595598199 5924af8f8fad60ca29199c.pdf> accessed 7 December 2021*

[126] *John Howard, 'Human-algorithm teaming in face recognition: How algorithm outcomes cognitively bias human decision-making' (2020) 15(8) PloS ONE <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7444527/pdf/pone.0237855.pdf> accessed 10 December 2021*

[127] *Mujib Mashal et al. 'Errors Raise Questions About Sri Lankan Response to Bombing' (Colombo, 26 April 2019) The New York Times <https://www.nytimes.com/2019/04/26/world/asia/sri-lanka-bombing- investigation.html> accessed 11 December 2021*

in Detroit, USA of a person accused of shoplifting in 2019, based on an FRT system being used on CCTV footage which provided a potential match. In this instance, the prosecutor dropped the lawsuit and the police department acknowledged that there were shortcomings by the investigating officer in their application of the FRT system.[128] These instances indicate that as much as it is essential to weed out the biases and risks inherent to FRT systems and AI systems as a whole, it is also important to train human operators on the application of these technologies to avoid harmful misidentifications.

4. Inaccuracy due to deliberate tweaks in images

The growing excitement towards the adoption of FRT systems has recently been tempered with the exposure of key vulnerabilities that affect algorithmic accuracy. The use of perturbations to cause an algorithm to 'glitch', i.e., failing to identify the image due to addition of certain patches that cause errors in translating the chosen image to its representational numeric value, has been evidenced to show a higher error rate.[129] Research indicates that AI systems, taught with machine learning or deep-learning, are susceptible to misidentification or 'hallucination' by tiny tweaks, indistinguishable to the human eye.[130] With automated self-learning algorithms such as FRT systems taught to recognise and authenticate faces based on numerical representations and patterns, these issues leave any further real-world uses of FRT systems in India vulnerable to sabotage, rigging, or malicious misidentification.

5. Security risks due to data breaches and unauthorised access

The vast amount of biometric facial data processed by FRT systems necessitates stringent security measures to protect that data.[131] The need for security arises from the twin concerns of privacy protection and economic value. A trove of facial data is economically valuable for companies developing or deploying FRT systems, and is part of their intellectual property.[132] Additionally, facial data consensually shared by a data subject is typically based on assurances of data security, privacy protection and access control. Any unauthorised access, use or theft of this facial data for any purpose automatically vitiates

[128] *Adi Robertson, 'Detroit man sues police for wrongfully arresting him based on facial recognition' (13 April 2021) The Verge <https://www.theverge.com/2021/4/13/22382398/robert-williams-detroit-police-department-aclu-lawsuit-facial-recognition-wrongful-arrest> accessed 12 December 2021*

[129] *Niti Aayog, 'Approach Document for India Part 1 – Principles for Responsible AI' (February 2021) <https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf> accessed 10 November 2021*

[130] *Mai Schotz, 'AI Has a Hallucination Problem That's Proving Tough to Fix' (9 March 2018) WIRED <https://www.wired.com/story/ai-has-a-hallucination-problem-thats-proving-tough-to-fix/> accessed 17 December 2021*

[131] *Niti Aayog, 'Approach Document for India Part 1 – Principles for Responsible AI' (February 2021) <https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf> accessed 20 February 2022*

[132] *Olivia Solon, 'Facial recognition's 'dirty little secret': Millions of online photos scraped without consent' (17 March 2019) NBC News <https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921> accessed 20 February 2022*

the informational autonomy of the data subject.

On the other hand, the aggregated and collected form of facial data presents a valuable target for hackers, third party agents or insiders seeking to use that data for any other purpose than for which it was collected. FRT systems can be particularly vulnerable if they are deployed by sub-contracted parties or third-party affiliates as part of a larger program. In 2020, the Department of Homeland Security, USA admitted to a leak of approximately 184,000 traveller images from the facial recognition pilot program launched by the US Customs and Border Protection.[133] This follows news of a facial recognition firm based in China having reportedly exposed personal data of 2.5 million people, by placing the live database on an online server without a login password for six months.[134] Therefore, the deployment of FRT systems automatically raises a risk of data breaches and unauthorised access. can only be tackled with stringent security practices, access limitations, data minimisation principles to reduce risks of personal data exposure, and regular audits to ensure best practices.

6. Accountability, legal liability and grievance redressal

FRT systems are based on the automated verification or identification of a person based on their facial data and its correlation with any previous reference image.[135] However, as discussed above, this processing of matching is fraught with risks of inaccuracies due to various factors. A failure to provide for adequate measures that provide for grievance redressal and legal accountability signals a major risk of being unable to identify or correct such inaccuracies.

As discussed previously, FRT systems may suffer from the *'many hands problem'*, with inputs received at various stages of designing the software, training the system and testing its functionality. Indian law enforcement agencies that have deployed FRT systems, for example, have refused to share details regarding the FRT system or the databases, citing protections under trade secrets and intellectual property rights.[136]

Grievance redressal becomes an uphill battle in light of such difficulties in proving bias or discrimination and narrowing down the party responsible for any inaccuracy by the FRT system. Individuals who may suspect inaccuracy or bias within FRT systems require assistance from institutional norms in order to obtain legitimate relief on their grievances.

[133] *Office of Inspector General, 'Review of CBP's Major Cybersecurity Incident during a 2019 Biometric Pilot' (21 September 2020) OIG-20-71, Department of Homeland Security <https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf> accessed 20 February 2022*

[134] *Yuan Yang, Madhumita Murgia, 'Data leak reveals China is tracking almost 2.6m people in Xinjiang' (17 February 2019) Financial Times <https://www.ft.com/content/9ed9362e-31f7-11e9-bb0c-42459962a812> accessed 20 February 2022*

[135] *Smriti Parsheera, 'Adoption and regulation of facial recognition technologies in India: Why and why not?' (November 2019) Data Governance Network, Working Paper 05*

[136] *Shouvik Das, 'Facial Recognition and 'Trade Secrets': What Exactly are Police Forces Doing with Surveillance Tech?' (4 December 2020) News18 < https://www.news18.com/news/tech/facial-recognition-and-trade-secrets-what-exactly-are-police-forces-doing-with-surveillance-tech-3145223.html> accessed 21 February 2022*

Parallelly, grievance redressal problems need to incorporate a human-in-the-loop aspect as well, in order to provide immediate relief to affected individuals, along with reporting and auditing mechanisms to ensure long-term accuracy and reliability of the FRT system.

7. Opaque nature of FRT systems

FRT systems, following the trend of AI systems generally, tend to be opaque systems that do not easily lend themselves to public independent scrutiny.[137] Moreover, individuals being subject to discrimination due to FRT bias may face an uphill task in proving inaccuracy or bias, given the closed nature of training datasets and code where an FRT system may have picked up its bias.[138] Such concerns may lead to doubts on the reliability of FRT systems and a lack of trust on the accuracy of its results. Further, this opacity may undermine the implementation of regulatory checks and balances on the use of FRT systems keeping in mind privacy and accuracy concerns and general data minimisation norms such as collection, storage, and processing limitations. This is particularly relevant when FRT systems are deployed by government agencies, which base decisions on the results provided by FRT systems, such as law enforcement, access to public services, airport and train access, attendance in government offices etc. In these instances, it is important to be able to show substantive fairness in the governmental use of FRT systems to minimize allegations of bias, inaccuracy, or violations of privacy.

Transparent terms explaining the profiling, functioning of the FRT system, data processing nd privacy protection practices may mitigate these concerns to a large extent.[139] Additionally, a regulatory model that allows for scrutiny of the training databases to evaluate likelihood of bias, and periodic audits on the error rates by FRT systems being deployed in the public sector by authorised independent experts can further address these concerns.

[137] *Niti Aayog, 'Approach Document for India Part 1 – Principles for Responsible AI' (February 2021) <https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf> accessed 21 February 2022*

[138] *Ewert v. Canada, [2018] 2 SCR 165, Supreme Court of Canada; Teresa Scassa, 'Supreme Court of Canada Decision Has Relevance for Addressing Bias in Algorithmic Decision-Making' (14 June 2018)*

<http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=278:supreme-court-of-canada-decision-has-relevance-for-addressing-bias-in-algorithmic-decision-making&Itemid=80> accessed 21 February 2022

[139] *Future of Privacy Forum, 'Privacy Principles for Facial Recognition Technology in Commercial Applications' (September 2018), <https://fpf.org/wp-content /uploads/2019/03/Final-Privacy-Principles-Edits-1.pdf> accessed 21 February 2022; similar steps have been for automated decision-making in Petra Molnar, Lex Gill 'Bots at the gate: A human rights analysis of automated decision-making in Canada's immigration and refugee system' (2018) International Human Rights Program and the Citizen Lab <https://citizenlab.ca/wpcontent/uploads/2018 /09/IHRP-Automated-Systems-Report-Web- V2.pdf> accessed 22 February 2022*

ANNEX 4- RIGHTS-BASED RISKS

(Referencer to table 1.2)

1. Puttaswamy on privacy and informational autonomy

The Supreme Court, in 2017, recognized the right to privacy as a constitutional right, reading it within Article 21 of the Indian constitution.[140] Within this right to privacy, a majority of the judges ruled that the right to privacy comprises, among other principles, the right to autonomy over one's choices and one's information. As previously discussed, the essential nature of AI systems involves the processing of a vast amount of data. The essential nature of FRT systems is based on its ability to process biometric data points which can identify any person, i.e., their facial image. This functionality of FRT systems raises concerns regarding the potential challenges posed by FRT systems to one's privacy rights.

2. Issues of informational autonomy

Firstly, the right to informational autonomy, inherent to the right to privacy, is violated by deployment of FRT systems in manners inconsistent with consent-based frameworks or other prescribed legal manners. The use of automated FRT systems for government programs shall require the creation of gallery datasets which may be sourced from existing biometric facial datasets present with a government entity.[141]

This deployment raises concerns on the propriety of a biometric dataset, ostensibly collected for one purpose, now being processed for another future purpose. In this case, the person in question may not control or consent to their data being used for any other purposes.

[140] *Justice K Puttaswamy (Retd.) vs Union of India, (2017) 10 SCC 1*

[141] *For example, the FRT system for the Global Entry program in the USA relied on historic facial data collected from visa, passport and other Department of Homeland Security interactions to create gallery datasets of face templates.*

- In this scenario, the fact that personal data can be collected and tracked across databases, outside a consent-based framework, is itself a violation of the right to informational autonomy. This concern has been echoed during discussions regarding the usage of live FRT systems, used to track or identify individuals within a gallery dataset against a moving video or visual feed.[142]
- It was observed that the use of live FRT for surveillance purposes encourages 'surveillance creep', wherein data gathered for one purpose is repurposed for another, and undermines the premise of informed consent both due to the difficulties in withdrawing or refusing consent to being surveilled. Additionally, it undermines an individual's choice to be left alone from data processing, as avoidance of cameras and surveillance tools may be construed as evasive or suspect behaviour by law enforcement agencies tasked with using live FRT to prevent or detect crime.
- Implementation of FRT systems and live FRT to allow access to public benefits such as access to airports, education, food and economic benefits, prevents a person from giving meaningful consent, as the lack of a feasible alternative forces an individual to give consent. In 2017, the European Court of Justice ruled that a citizen could not be said to have given meaningful consent to collection of biometric data, when such processing was the only way to access services such as travel.[143]
- Consent is also not seen as implied purely based on the knowledge that one's data is currently being processed. This was affirmed by the guidance note issued by the European Data Protection Board in its 'Guidelines 3/2019 on processing of personal data through video devices', where it was clarified that entering an area marked as undergoing monitoring is not to be taken as a sign of implied consent.[144]

3. Threat to non-participants in deployment of FRT systems:

Even in a scenario where the government body tasked with storing the biometric datasets is permitted through legislation to share their data with another government agency seeking to process the facial dataset for its FRT system, it raises concerns of misidentification and harm. Given the massive

[142] *Pete Fussey, Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019) The Human Rights, Big Data and Technology Project <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/ 07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 29 December 2021*

[143] *Schwarz v Stadt Bochum (CJEU, 2013) 2 C.M.L.R. 5*

[144] *Guidelines 3/2019 on processing of personal data through video devices (29 January 2020) European Data Protection Board <https://edpb.europa.eu/sites/default/files/files/file1/edpb_ guidelines_201903_ video_devices_en_0.pdf> accessed 21 December 2021*

amounts of data collection, data storage and data transfers that are part of training an FRT system to be used by the government for its citizens, such a transfer raises concerns of whether a person may suffer harm due to misidentification despite not having consented to being part of that program. An example of this consequence to a non-participant in the second government program is shared below.

Illustration: Consequences of purpose creep to non-participant

A person is enrolled in a national ID program and has submitted his facial image as part of the biometric data points gathered during the ID registration. The entity processing and storing this database is then exempt from consent requirements under a national data protection law, which allows this database to be shared with another government body using FRT systems for the latter's gallery dataset.

The first person has not consented to this transfer of data, and may not even be aware of their facial data being processed by the second agency. However, the person may still face consequences if the FRT system misidentifies another person as them (a false positive), if the identification would then lead to monitoring, arrests or other forms of digital profile contamination for that person.

4. Legal thresholds applicable to FRT systems

In addition to a consent-based framework for privacy, the Supreme Court in *Puttaswamy* sets out a three-fold test of legal validity, legitimate interests, and proportionality for cases involving restraints on privacy by the State which include national security and legitimate state interests.[145] In 2018, the Supreme Court has expanded the proportionality test to a five-part test which includes testing whether the measure restraining the right to privacy- (a) has a legitimate goal, (b) is a suitable means of furthering that goal, (c) is the least restrictive while being equally effective among its alternatives, and (d) does not have a disproportionate impact on the right holder.[146] These twin tests lay down necessary considerations to keep in mind while introducing FRT systems to any particular domain, especially in a public sector context, as these thresholds directly apply to state action. Given its nature, measures taken by government agencies to use FRT systems must square with the tests laid out in both *Puttaswamy* (2017) and *Puttaswamy* (2018) discussed above.

5. Anonymity as a facet of privacy

Lastly, the expansion of data collection and data processing, along with a potential ubiquity of AI systems including FRT systems, raises ethical questions regarding the shrinking of a person's right to anonymity. As the use of FRT systems in suppressing dissent, monitoring activists, and identifying protesters increases, a parallel distrust towards surveillance systems and

[145] *Justice K Puttaswamy (Retd.) vs Union of India, (2017) 10 SCC 1*

[146] *Justice K Puttaswamy (Retd.) vs Union of India, (2019) 1 SCC 1*

FRT applications develops due to its perceived usage and harms. In this space, anonymity is an aspect of privacy, seen as necessary to secure other freedoms including the freedom of speech, freedom to dissent and freedom of movement.[147] The adoption of FRT in a manner that does not account for its necessity, proportionality and harm would further shrink the space for anonymity through pervasive surveillance tools and data collection.

These concerns are grounded in examples seen in contemporary legal and political developments across the world. Recent data leaks and leaks involving access to CCTVs installed in Moscow have raised questions over implementation of safeguards in FRT in Russia.[148] This follows reports of the widespread implementation of FRT against protesters in Hong Kong[149], in Uganda[150], in India[151], and in the USA[152] to quell dissent. The use of FRT systems to suppress free speech and dissent, and its resultant unpopularity, resulted in Amazon[153], Microsoft[154] and IBM[155] ceasing supply of FRT systems to law enforcement agencies in the USA. Lastly, the use of facial masks and coverings as protest tools in the age of FRT created or resurrected laws

[147] Office of the High Commissioner 'Artificial intelligence risks to privacy demand urgent action – Bachelet' (Geneva, 15 September 2021) United Nations Human Rights Commission

<https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27469&LangID=E> accessed 10 January 2022

[148] Umberto Bacchi, 'Face for sale: Leaks and lawsuits blight Russia facial recognition' (9 November 2020) Reuters <https://www.reuters.com/article/us-russia-privacy-lawsuit-feature-trfn- idUSKBN27P10U> accessed 19 December 2021; see also 'Russia Expands Facial Recognition Despite Privacy Concerns' (October 2, 2020) Human Rights Watch <https://www.hrw.org/ news/2020/10/02/russia-expands-facial-recognition-despite-privacy-concerns> accessed 19 December 2021

[149] Zak Doffman, 'Hong Kong Exposes Both Sides Of China's Relentless Facial Recognition Machine' (26 August 2019) Forbes <https://www.forbes.com/sites/zakdoffman/2019/08/26/hong-kong-exposes-both-sides-of-chinas-relentless-facial-recognition-machine/> accessed 20 December 2021

[150] Stephen Kafeero, 'Uganda is using Huawei's facial recognition tech to crack down on dissent after anti-government protests' (28 November 2020) Quartz <https://qz.com/africa/1938976/uganda-uses -chinas-huawei-facial-recognition-to-snare-protesters/> accessed 23 December 2021

[151] Reuters, 'Delhi, UP Police use facial recognition tech at anti-CAA protests, others may soon catch up' (Mumbai/ New Delhi, 18 February 2020) India Today <https://www.indiatoday.in/india/story/delhi -up-police-use-facial-recognition-tech-at-anti-caa-protests-others-may-soon-catch-up-1647470-2020-02-18> accessed 3 January 2022

[152] Shira Ovide, 'A Case for Banning Facial Recognition' (1 August 2021) The New York Times <https://www.nytimes.com/2020/06/09/technology/facial-recognition-software.html> accessed 17 December 2021

[153] Amazon Staff, 'We are implementing a one-year moratorium on police use of Rekognition' (11 June 2020) Amazon <https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition> accessed 17 December 2021

[154] Jay Greene, 'Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM' (11 June 2020) The Washington Post <https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/> accessed 17 December 2021

[155] Jay Peters, 'IBM will no longer offer, develop, or research facial recognition technology' (8 June 2020) The Verge <https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software> accessed 17 December 2021

banning face coverings in China[156], Sri Lanka[157] and the USA[158] so as to not undermine investigative efforts. These legislations portray grave implications on the right to determine whether to have one's facial image processed by an FRT system.

[156] *John Leicester, 'For Hong Kong protesters, masks shield against Big Brother' (Hong Kong, 5 October 2019) AP News <https://apnews.com/article/international-news-asia-pacific-hong-kong- b411b9c-205da4b34a5aafded7ae50122> accessed 17 December 2021*

[157] *Theresa Waldrop, 'Sri Lanka bans all face coverings for 'public protection' after bomb attacks' (29 April 2019) CNN <https://edition.cnn.com/2019/04/29/asia/sri-lanka-face-coverings-ban/index.html> accessed 17 December 2021*

[158] *Jay Stanley, 'America's Mask Bans in the Age of Face Recognition Surveillance' (26 November 2019) American Civil Liberties Union <https://www.aclu.org/news/free-speech/americas-mask-bans- in-the-age-of-face-recognition-surveillance/> accessed 17 December 2021*

ANNEX 5- CROSS JURISDICTIONAL REGULATORY COMPARISION

A. European Union

S. No.	Title	Description
1.	General Data Protection Regulations, 2016 (GDPR)	The GDPR forms the framework law on data protection and privacy for the EU member states. With respect to FRT, it classifies facial data as a "special category" of personal data, which cannot be processed for uniquely identifying a person. Furthermore, for facial data's processing, consent must be given explicitly, and such processing must only be for a "lawful purpose"[159]
2.	Data Protection Law Enforcement Directive (Directive)	The Directive lays down specific rules for the processing of personal data of natural persons by competent authorities for the purposes, prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties by competent authorities. Like the GDPR, the Directive also identifies biometric data as "special category" of personal data. It lays three exceptions for using biometric data for unique identification of a natural person - first, when it is authorised by law; second, to protect vital interests of the data subject or another natural person, and third, where facial data has been manifestly made public by the data subject. It prohibits use of biometric data for profiling.

[159] *Article 9, General Data Protection Regulation, 2016*

3.	Proposed AI Act, 2021 (AIA)[160]	The AIA takes a strict approach to regulating FRT, and given the risks associated with real-time remote biometric identification. Generally, there is a ban on its usage in publicly accessible spaces for the purposes of law enforcement.[161] It provides three exhaustive and narrowly defined exceptions to this - targeted search for specific potential victims of crime; prevention of a specific, substantial and imminent threat to life or physical safety of natural persons; detection, localisation, identification or prosecution of a suspect of a criminal offence.[162]

B. United Kingdom

S. No.	Title	Description
1.	Bridges v. Chief Constable of South Wales Police163	Challenging the use of automated FRT, the petitioner filed a case claiming violation of rights under the European Convention on Human Rights (ECHR), the Data Protection Act, 2018, and the Equality Act, 2010. The takeaway from this judgement seems to be that the deployment of FRT was held to be irregular not because it was based on certain sensitive categories of data or that the purpose for which it was deployed, but because there was noncompliance with certain provisions of the law, i.e., the discretion related provisions and conducting of a data protection impact assessment. Therefore, objections that the Court had from privacy and data protection were such that did not go to the root of the deployment of FRT.

[160] *European Commission, Proposal for Regulation of the European Parliament and the Council: Laying down harmonised rules on AI (AI Act) and amending certain Union legislative Acts, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>, accessed January 16, 2022.*

[161] *Article 5, Council Proposal for a Regulation on Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts 2021*

[162] *European Commission, Proposal for Regulation of the European Parliament and the Council: Laying down harmonised rules on AI (AI Act) and amending certain Union legislative Acts, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>, accessed January 16, 2022.*

[163] *([2020] EWCA Civ 1058)*

2.	Information Commissioner's Office (ICO)	The ICO has issued two opinions on the use of live automated FRT, in October 2019,[164] and June 2021,[165] respectively. The first opinion focused on live FRT and "sensitive processing" of personal, biometric data. This opinion was issued for the law enforcement agencies with regard to the compliance of the provisions of the Data Protection Act, 2018. The second opinion assessed fourteen examples of deployment of LFRT, aimed towards curbing unwanted behaviours in public places, surveillance purposes and prevention of crime. The ICO observed that it can capture the biometric data of all individuals passing within its range automatically and indiscriminately. This is accompanied with a lack of awareness, choice or control for the individual.

C. United States

S. No.	Title	Description
1.	Federal level regulation	Presently, there is no federal level legislation or regulation regarding FRT in the United States. Although several bills have been introduced in the Congress between 2019 to 2020, most of these are at the introduction stage. Out of these, the George Floyd Justice in Policing Act, 2020 has moved beyond the stage of introduction and has been passed by the House of Representatives.[166] There are four other bills on FRT but all of them are at the stage of introduction.[167]Apart from legislative proposals, at the federal level, the Federal Trade Commission (FTC) has played an active role in regulating FRT.

[164] *Information Commissioner, Opinion on the use of live facial recognition technology by law enforcement in public places 2019 / 01 Page 2 <https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf> accessed 16 January 2022*

[165] *Information Commissioner, Opinion on the use of live facial recognition technology in public places 2021 <https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf > accessed 16 January 2022*

[166] *George Floyd Justice in Policing Act of 2020 H.R. 7120 <https://www.congress.gov/bill/116th-congress/house-bill/7120/text> accessed 16 January 2022*

[167] *The Advancing Facial Recognition Act, H.R.6929 <https://www.congress.gov/bill/116th-congress/house-bill/6929/text?r=1&s=1> accessed 16 January 2022. This Bill was introduced in 2020 and requires the Secretary of Commerce and the Federal Trade Commission to undertake a study on the impact of FRT on businesses and present the report to Congress.*

The Commercial Facial Recognition Privacy Act S. 847 <https://www.congress.gov/bill/116th-congress/senate-bill/847> accessed 16 January 2022. It was introduced in 2019 and regulates processing of facial data by private entities. Data processors are prohibited from using facial data to discriminate between users, for purposes not reasonably foreseeable, sharing without affirmative consent and conditioning its availability in a manner that requires affirmative consent.

2.	State and local level regulation	Numerous states like Washington, Virginia, Massachusetts, and Illinois, have proposed or passed regulation through their respective state legislatures. Other states that have proposed FRT related legislations are Maryland and Alabama. In Maryland, the Facial Recognition Privacy Protection Act has been introduced, which aims at regulating governmental use of FRT.[168]At the level of cities, regulation of FRTs is mostly in the nature of bans being imposed. Several municipalities, especially in the states of California and Massachusetts, have banned the use of FRT. These include the cities and towns of Alameda,[169] Berkeley,[170] Boston,[171] Brookline,[172] Cambridge,[173] Easthampton,[174] Northampton,[175] Oakland, San Francisco[176] and Somerville.[177]

[168] Facial Recognition Privacy Protection Act 587 <https://mgaleg.maryland.gov/2021rs/bills_noln/sb/fsb0587.pdf> accessed 16 January 2022

[169] Peter Hegarty, 'East Bay City becomes latest to ban use of facial recognition technology' (18 December 2019) East Bay Times <https://www. eastbaytimes.com/2019/12/18/east-bay-city-becomes-latest-to-ban-use-of-facial-recognition-technology> accessed 16 January 2022

[170] Tom McKay, 'Berkeley becomes fourth U.S. city to ban face recognition in unanimous vote' 16 October 2019 Gizmodo <https://gizmodo.com/berkeley-becomes-fourth-u-s-cityto-ban-face-recogniti-1839087651> accessed 16 January 2022

[171] Nik DeCosta-Klipa, 'Boston City Council unanimously passes ban on facial recognition technology' (24 June 2020) Boston.com <https://www.boston.com/news/local-news/2020/06/24/boston-face-recognition-technology-ban> accessed 16 January 2022

[172] ACLU of Massachusetts, 'Brookline bans municipal use of face surveillance' ACLU of Massachusetts (11 December 2019) <https://www.aclum.org/en/news/brookline-bans-municipal-use-facesurveillance> accessed 16 January 2022

[173] Nik DeCosta-Klipa, 'Cambridge becomes the largest Massachusetts city to ban facial recognition' Boston.com (24 January 2020) <https://www.boston.com/news/local-news/2020/01/14/cambridge-facial-recognition/> accessed 16 January 2022

[174] Michael Connors, 'Easthampton bans facial recognition technology' (3 July 2020) Daily Hampshire Gazette <https://www.gazettenet.com/Easthampton-City-Council-passes-ordinance-banning-facial-recognition-survaillance-technology-35048140> accessed 16 January 2022

[175] Jackson Cote, 'Northampton bans facial recognition technology, becoming third community in Massachusetts to do so' (27 February 2020) MassLive <https://www.masslive.com/news/2019/12/northampton-bans-facial-recognition-technology-becoming-third-community-in-massachusettsto-do-so.html> accessed 16 January 2022

[176] Dave Lee, 'San Francisco is first US city to ban facial recognition' BBC News (15 May 2019) https://www.bbc.com/news/technology-48276660 accessed 16 January 2022

[177] Katie Lannan, 'Somerville bans government use of facial recognition tech' WBUR (28 June 2019) <https://www.wbur.org/news/2019/06/28/somerville-bans-government-use-of-facial-recognition-tech> accessed 16 January 2022

D. Australia

S. No.	Title	Description
1.	OAIC decision (Clearview case)	In November 2021, the Office of the Australian Information Commissioner issued a direction against Clearview AI. Clearview is a private organisation scraping images of people from across the Internet. Following the investigation, it was found that Clearview had breached citizens' privacy. It was found that Clearview's practices resulted in violation of multiple Australian Privacy Principles (APP), for collecting sensitive information,[178] unfair collection and processing of information,[179]and failure to ensure that data processed was accurate[180]. Clearview was ordered to withdraw from the Australian market.181 and destroy all scraped images, probe images, scraped image vectors, probe image vectors and opt out vectors that it has collected from individuals in Australia in breach of the Privacy Act, 1988.
2.	OAIC Decision (7-11 case)	7-11 is a convenience store, with around 700 outlets, across Australia. It deployed FRT across these stores as part of a customer feedback mechanism. OAIC conducted an inquiry into such use of FRT by 7-11 to determine its compliance with the Privacy Act, 1988.[182] The OAIC determined that 7-11 was processing sensitive personal data (facial images) without consent, and was not transparent in its privacy policy about its FRT systems. Accordingly, the OAIC directed 7-11 to destroy all facial data it had collected and ensure that the practice was discontinued.[183]

[178] *The definition of sensitive information extends to biometric information that is used for the purpose of automated biometric identification or verification and biometric templates.*

[179] *Office of Australian Information Commissioner, Commissioner initiated investigation into Clearview AI, Inc (Privacy) [2021] AICmr 54 Para 172*

[180] *Office of Australian Information Commissioner, Commissioner initiated investigation into Clearview AI, Inc (Privacy) [2021] AICmr 54 Para 218*

[181] *Office of Australian Information Commissioner, Commissioner initiated investigation into Clearview AI, Inc (Privacy) [2021] AICmr 54 Para 238*

[182] *Office of Australian Information Commissioner, Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) [2021] AICmr 50 <https://www.oaic.gov.au/__data/assets/pdf_file/0021/10686/Commissioner-initiated-investigation-into-Eleven-Stores-Pty-Ltd-Privacy.pdf> accessed 16 January 2022*

[183] *Office of Australian Information Commissioner, Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) [2021] AICmr 50 Para 135*

3.	Australian Human Rights Commission	In March 2021, the Australian Human Rights Commission (AHRC) finalised a report laying out the roadmap for Australia to protect human rights in the context of development and use of new technologies.[184] Regarding the use of FRT in the context of biometric surveillance and privacy,[185] the report proposed federal, state and territorial legislation, further proposing a moratorium against FRT till such laws were enacted.

E. Canada

S. No.	Title	Description
1.	Clearview AI investigation	An investigation of Clearview AI in 2020, by Privacy Commissioners of Canada and British Columbia, assessed violations by the company under multiple privacy laws. Rejecting Clearview's argument that it used publicly available facial data, it was held that publicly available data is not always accessible, and consent of data principals was necessary. Second, the questionable collection and processing to create FRT systems for law enforcement was determined to not have an appropriate purpose. First, the images were originally shared online for different purposes, second, these were to the detriment of the individual (for example, surveillance in unwarranted situations) and third, they may lead to significant harm to the individual (for example, misidentification, data breaches). In light of the above observations, Clearview was ordered to cease offering FRT in Canada, cease processing of images and biometric facial arrays and delete facial data collected from individuals in Canada.
2.	Draft privacy guidance on FRT for police agencies	The Privacy Commissioner of Canada issued guidance for the use of FRT specifically by federal, provincial, regional, and municipal state agencies.[186] It laid down principles like lawful authority, necessity and proportionality, privacy by design, accuracy, data minimisation and purpose limitation.

[184] *Corrs, 'Unpacking the Australian Human Rights Commission's recommendation for AI regulation' Corrs (9 July 2021) <https://www.corrs.com.au/insights/unpacking-the-australian-human-rights-commissions-recommendations-for-ai-regulation?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration> accessed 16 January 2022*

[185] *Australian Human Rights Commission Human Rights and Technology 2021 <https://tech.humanrights.gov.au/sites/default/files/2021-05/AHRC_RightsTech_2021_Final_Report.pdf> accessed 16 January 2022*

[186] *Office of the Privacy Commissioner of Canada, Draft privacy guidance on facial recognition for policy agencies 2021 <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/gd_frt_202106/#toc5> accessed on 16 January 2022*