Facial Recognition Technology in India

August 31, 2021

By **Elonnai Hickok, Pallavi Bedi, Aman Nair and Amber Sinha**

Reviewed by **Daragh Murray, Peter Fussey, Amy Stevens and Arindrajit Basu**

The Centre for Internet and Society, India

https://cis-india.org

The Human Rights, Big Data and Technology Project, University of Essex, UK

https://hrbdt.ac.uk

Template designed by Saumyaa Naidu

Shared under the **Creative Commons Attribution 4.0 International license**

Introduction 5

Use cases of FRT by the State 9

Legislative Discussions on the Implementation of FRT 17

FRT through the lens of Right to Privacy 19

Legal Frameworks and FRT in India 22

International Perspectives 44

Observations and Conclusions 47

Executive Summary

Over the past two decades there has been a sustained effort at digitising India's governance structure in order to foster development and innovation. The field of law enforcement and safety has seen significant change in that direction, with technological tools such as Closed Circuit Television (CCTV) and Facial Recognition Technology (FRT) increasingly being deployed by the government.

Yet for all its increased use, there is still a lack of a coherent legal and regulatory framework governing FRT in India. Towards informing such a framework, this paper seeks to document present uses of FRT in India, specifically by law enforcement agencies and central and state governments, understand the applicability of existing legal frameworks to the use of FRT, and define key areas that need to be addressed when using the technology in India. We also briefly look at how the coverage of FRT has increased beyond law enforcement; it now covers educational institutions, employment purposes, and it is now being used for providing Covid-19 vaccines.

We begin by examining use cases of FRT systems by various divisions of central and state governments. In doing so, it becomes apparent that there is a lack of uniform standards or guidelines at either the state or central level - leading to different FRT systems having differing standards of applicability and scope of use. And while the use of such systems seems to be growing at a rapid rate, questions around their legality persist.

It is unclear whether the use of FRT is compliant with the fundamental right to privacy as affirmed by the Supreme Court in 2017 in *Puttaswamy*. While the right to privacy is not an absolute right, for the state to curtail this right, the restrictions will have to comply with a three-fold requirement— first, being the need for explicit legislative mandate in instances where the government looks to curtail the right. However, the FRT systems we have analysed do not have such a mandate and are often the result of administrative or executive decisions with no legislative blessing or judicial oversight.

We further locate the use of FRT technology within the country's wider legislative, judicial and constitutional frameworks governing surveillance. We also briefly articulate comparative perspectives on the use of FRT in other jurisdictions. We further analyse the impact of the proposed Personal Data Protection Bill on the deployment of FRT. Finally, we propose a set of recommendations to develop a path forward for the technology's use which include the need for a comprehensive legal and regulatory framework that governs the use of FRT. Such a framework must take into consideration the necessity of use, proportionality, consent, security, retention, redressal mechanisms, purpose limitation, and other such principles. Since the use of FRT in India is also at a nascent stage, it is imperative that there is greater public research and dialogue into its development and use to ensure that any harms that may arise in the field are mitigated.

Introduction

The 2010s have seen the rapid development and subsequent adoption of biometric technologies by corporations and governments alike. Of these emerging technologies, not many have managed to entrench themselves into global systems in the manner that facial recognition technology (FRT) has. Despite fears surrounding privacy, numerous governments across the globe have adopted FRT with the stated purpose of improving surveillance, preventing crime and ensuring safety.

Over the last few years, India has been one of the most noted countries in terms of implementing this technology into various levels of its governance and policing infrastructure. With the growing use of FRT in the country, there is a need to understand the manner in which this technology has been adopted by the state. This article looks to address that gap by acting as an introductory resource that outlines the present use of FRT in India for individuals who may be interested in understanding the current scenario in India.

We begin by first identifying the projects that are currently utilising FRT in India, and determining how this technology fits into the country's wider legislative, judicial and constitutional frameworks relating to surveillance. We also briefly articulate international perspectives on the use of FRT in comparison to India and ultimately prescribe a set of recommendations to develop a path forward for the technology's use.

What is Facial Recognition Technology?

FRT is an automated process of comparing two images of faces to determine whether they represent the same individual. A picture first is uploaded on the facial recognition technology software and by the use of a feature analysis algorithm, certain distinctive features of the face such as nose, eyes, lips and the distance between the eyes and the chin or lips are measured and converted into a mathematical representation known as a face template. This is then compared against the facial data collected in a database, to see if law enforcement agencies can find a match. It can also be used for face verification, whereby the captured image is compared against a known template. The software then provides the user with a score or percentage that represents the likelihood that the individual in the captured image is the same as the one in the template.

The accuracy of the results depends on a number of factors, such as the quality of the photograph uploaded or captured (in the case of live automatic facial recognition technology), use of makeup, quality of the lighting, distance/angle from which the picture was captured. Variations in pose, illumination, and expression, among other factors, adversely impact the accuracy of automated facial analysis.[1]

[1] Aayush Rathi and Ambika Tandon, "The Digital Identification Parade," *The Indian Express* (blog), July 29, 2019, available at https://indianexpress.com/article/opinion/columns/digital-identification-facial-recognition-system-ncrb-5859072/.

Though FRT can potentially be a useful tool in assisting with the identification of individuals, it can also be misused depending on who uses the technology, for what purposes, in what configuration, and in the absence of a requisite legal and regulatory framework for governing its use. Poorly designed and trained FRT systems can result in inaccurate, discriminatory, and biased decisions. A study conducted by the Center for Privacy and Technology of Georgetown Law observed that public facial recognition disproportionately affects African Americans as the training set used to develop the facial recognition software was skewed disproportionately against African Americans.[2] Research conducted on the publicly available facial recognition technology systems have shown that these systems show up false positives, i.e when the technology incorrectly identifies a positive match for a person's face with an image on the database. In a test conducted by the American Civil Liberties Union[3] in 2018 on Amazon's facial recognition tool known as Rekognition, the software incorrectly identified 28 members of the United States Congress as people who have been arrested for a crime. The false matches were disproportionately higher when it came to people of colour.In UK, concerns regarding the misuse of the technology, have been considered by the Science and Technology Committee of the House of Commons[4] who recommended that automatic facial recognition technology should not be deployed until concerns regarding the technology's effectiveness and potential for bias have been fully resolved among others. Factors which could influence the efficacy, accuracy and potential biases of FRT in India include skin colour, geography, religion and caste.

FRT can also be used to restrict and suppress political dissent. The technology makes it possible for Government and the law enforcement agencies to identify people who attend or participate in rallies or in any other form of political or social dissent and thereafter potentially put them under surveillance to track their movement. The problem is further exacerbated when the technology being employed by the law enforcement agencies has the potential of confirming the bias of the police when it comes to dissent and criminal activities.[5] The possibility of such outcomes transforms the issue of FRT from one of merely an individual's right to privacy being affected to one that affects a much wider range of fundamental rights including the right to dissent, protest and peaceful assembly.

In 2016, Wu and Zhang published a paper titled "Automated Inferences on Criminality using Face Images' ' where they used machine learning techniques to predict (from random drivers license photographs) the likelihood that a person is a convicted criminal, with a claimed 90% accuracy. This paper even went so far as to specify that the inference is "free of any biases of

[2] Georgetown Law- Center on Privacy and Technology 'The Perpetual Line-Up, Unregulated Police Face Recognition in America', October 18, 2016. available at https://www.perpetuallineup.org/

[3] ACLU- "Amazon's Face Recognition Falsely Matched 28 members of Congress with Mugshots' available at https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

[4] House of Commons- Science and Technology Committee, "The work of the Biometric Commissioner and the Forensic Science Regulator", July 18, 2019 available at https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/1970.pdf

[5] David Reiner, "Algorithmic Bias and Facial Recognition," An Introduction to Technology Policy (blog), November 28, 2020, available at https://techpolicymphil.blog.jbs.cam.ac.uk/2020/11/28/bias-frt/.

subjective judgments of human observers.” They claimed that their motive in building this model was to examine whether ML has the potential of acquiring human-like social perception of faces; in being able to identify faces not just by biometric dimensions, but also by socio-psychological features. The researchers concluded that the model, by assessing varied facial features, discovered that the criminals have a higher degree of dissimilarity in appearance than the non-criminals, proving that “being a criminal requires a host of abnormal (outlier) personal traits.” This sounds astonishingly similar to (widely discredited) physiognomy claims of the 19th century.

In 2017, Michal Kosinski, a researcher affiliated with Stanford University, co-authored a paper that claimed that facial recognition technology along with deep neural networks could be used on profile pictures uploaded on social media to predict sexual orientation. What Kosinski’s paper actually showed was that algorithms could detect a pattern in the appearance of a small subset of out white gay and lesbian people on dating sites, thus conflating pattern identification with prediction. The algorithm detected differences and similarities in facial structure, and tried to predict sexual orientation on the assumption that gay men’s faces were more feminine than heterosexual men, and lesbian women’s faces were more masculine than heterosexual women. According to the paper, this finding was based on the prenatal hormone theory of sexual orientation. This theory suggests that our sexuality is, in part, determined by hormone exposure in the womb. Kosinski’s critics pointed out that factors such as less facial hair in the case of gay male subjects may as easily be a consequence of fashion trends and cultural norms as prenatal hormonal exposure. In addition to noting such scientific shortcomings, critics felt the paper was dangerous and irresponsible because it could be used to support an authoritarian and brutal regime’s efforts to identify and/or persecute people they believed to be homosexual. After the paper was published, Kosinski went on to claim that similar algorithms could help measure intelligence quotient, political orientation, and criminal inclinations of people from their facial images alone.

What these researchers completely fail to account for is that who gets tagged “criminal” or problematic by such ML algorithms is rarely the result of objective and unbiased processes. Impressions formed by the police, and other members of the criminal justice system on what a “criminal appearance” is — which is seemingly the entire purpose of the research experiment — play a big role in persons’ convictions. As a result, the disproportionate number of convictions of those that appear criminal will in turn reinforce the idea, through an “unbiased” AI, that criminals often look like this. AI models often exhibit discriminatory tendencies largely because of biased data collection or data labelling methods. If the data set used to train the model overrepresents or underrepresents a certain community, then the resulting model will reproduce the same bias. In this example, the data set may be skewed by disproportionate convictions caused by intense policing of particular communities, or inequality of access to legal representation. For instance, the COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) algorithm, used by judges in the US to predict whether defendants should be detained or released on bail pending trial, was found to be biased against African-Americans. This was linked with the historical racism, disproportionate surveillance, and other inequalities in police practises, and the criminal system that makes African Americans more likely to be arrested or incarcerated in the US. These arrests are then reflected in the training data used to make models that will suggest whether a defendant should be detained. The ML model, while associating certain facial features with criminality, is influenced by biased data to "criminalise " certain features associated with already marginalised communities. This is closely tied with surveillance, as surveillance data would directly feed into over or under representing marginalised communities.

In the Indian context, this can be used to target communities which have historically been discriminated against and targeted by law enforcement such as Muslims, Scheduled Castes and Scheduled Tribes. These groups constitute approximately 39% of India's population, but they constitute a much higher percentage of the prison population-55% of the undertrial population as per a 2015 NCRB Report on Prison Statistics.[6] The more recent 2019 NCRB report on the subject has only served to reiterate the disproportionate rate of trial and incarceration faced by minority communities in India.[7] A study conducted by Common Cause and the Center for Developing Societies on the state of policing in India found that nearly 38% of the people covered by the study believed that the police falsely implicate Dalits in petty crimes such as theft and robbery.[8] Such a high number of Muslims and Dalits undertrials and convictions demonstrates the targeting of these groups by law enforcement and criminal justice agencies. Introducing FRT into these contexts could lead to the technology being biased from its very inception.

The government's recent history with data breaches, specifically in the case of Aadhaar, throws into question the vulnerability of any potential FRT system. Issues of individuals Aadhaar data being made publicly available[9] and being accessible to government officials who lacked proper authorization[10], represent just some of the cybersecurity issues that any future database will be required to overcome. Furthermore, the existence of fraud and

[6]National Crime Records Bureau, "Prison Statistics India 2015" (Ministry of Home Affairs, Government of India, 2015), https://ncrb.gov.in/sites/default/files/PSI-2015-%2018-11-2016_0.pdf. Indian Express- 'Over 55 per cent of undetrials, Muslim, Dalits or Tribals: NCRB' , November 1, 2016 available at https://indianexpress.com/article/india/india-news-india/over-55-per-cent-of-undertrials-muslim-dalit-or-tribal-ncrb-3731633/

[7] FP staff, "NCRB Data Shows Muslims, Dalits, Tribal Population in Prisons Disproportionate to Their Numbers Outside - India News , Firstpost," *Firstpost*, September 2, 2020, sec. India, https://www.firstpost.com/india/ncrb-data-shows-muslims-dalits-tribal-population-in-prisons-disproportionate-to-their-numbers-outside-8775161.html.
National Crime Records Bureau, "Prison Statistics India 2019" (Ministry of Home Affairs, Government of India, 2019), available at https://ncrb.gov.in/sites/default/files/PSI-2015-%2018-11-2016_0.pdf.

[8] 'Status of Policing in India Report 2018- A study of Performance and Perceptions', available at https://www.tatatrusts.org/upload/pdf/spir-2018-common-cause.pdf

[9] Tech2 Staff, "Aadhaar Security Breaches: Here Are the Major Untoward Incidents That Have Happened with Aadhaar and What Was Actually Affected," Tech2, September 25, 2018, available at https://www.firstpost.com/tech/news-analysis/aadhaar-security-breaches-here-are-the-major-untoward-incidents-that-have-happened-with-aadhaar-and-what-was-actually-affected-4300349.html.

[10] Tech2 Staff, "UIDAI Blocks 5,000 Officials from Aadhaar Portal Following Reports of Unauthorised Usage," *Tech2*, September 1, 2018, available at https://www.firstpost.com/tech/news-analysis/uidai-blocks-5000-officials-from-aadhar-portal-following-reports-of-unauthorised-usage-4294143.html.

identity theft that have arisen in the case of Aadhaar biometrics data[11] could compromise any future FRT system that will rely on or integrate any pre-existing facial or biometric data that has been collected for Aadhaar.

It is thus important that FRT is developed, trained, and used within a clear technological and legal framework with strong mechanisms for oversight, accountability, and redress as well as clear metrics for indicating inaccuracy and misuse. Furthermore, it is important that principles are developed to guide appropriate and inappropriate applications of the technology and ensure that proper training and capacity building is provided to users of facial recognition technology. Towards informing such a framework - this paper seeks to document present uses of FRT in India, understand the applicability of existing legal frameworks to the use of FRT, and define key areas that need to be addressed when using the technology in India.

Use cases of FRT by the State

The development and use of facial recognition technology in India by the State has been growing over the years as a tool for security, solving crime, and tracking and identifying different categories of persons such as missing persons

Across these systems and applications there is a significant lack of publicly available information with respect to the grounds on which the system is implemented and the basis on which and how data is collected, stored, and used.

FRT systems are also being used by educational institutions such as schools and colleges. The Central Board of Secondary Education, (a national level board of education in India for public and private schools, controlled and managed by the Government of India) has started to use FRT to provide access to digital documents to students.

Some of the other applications and systems include:

A. Digi-Yatra

In India, FRT has been deployed at airports as part of the Government’s Digi-Yatra policy to give a “seamless, hassle-free and paperless journey experience to every air traveller in India.”[12] The Digi Yatra Policy was launched in 2018 by the Ministry of Civil Aviation and it is a facial biometric boarding system for automated processing at airports.

[11] Reetika Khera, “Aadhaar Failures: A Tragedy of Errors,” April 5, 2019, available at https://www.epw.in/engage/article/aadhaar-failures-food-services-welfare
[12]“Digi Yatra”- Reimagining Air Travel in India, August 9, 2018 available at http://civilaviation.gov.in/sites/default/files/Digi%20Yatra%20Policy%2009%20Aug%2018.pdf

The policy aims to utilise facial recognition technology to simplify passenger processes at various points of the airport from check in to boarding the flight. As per the policy, the creation and use of a digi-yatra ID for passengers is completely voluntary and consent is required for the sharing of facial data via the digi-yatra platform . The facial data cannot be stored for longer than the duration of the journey and should be purged within one hour of the departure of the flight. The policy also provides for periodic audits of the biometric system to ensure adherence with prescribed data protection standards.[13]

In 2018, the Bangalore International Airport entered into an agreement with Vision-Box[14] to provide "paperless self boarding technology." The technology aims to identify passengers as they move across the airport. Hyderabad International Airport[15] has also deployed the use of FRT on a trial basis and since July 2019, passengers have had the option of using their face as their boarding pass. FRT has also been rolled out on a pilot basis at the international terminal of the Delhi Airport.[16] There is also a plan to introduce FRT at train stations across the country- starting with Bangalore.[17]

B. Aadhaar and FRT

In 2018, the Unique Identification Authority of India (UIDAI) indicated that it will incorporate FRT into India's national identity system, known as Aadhaar. The technology will be integrated as part of the authentication process to create a multi-factor authentication process (the user will have the choice of combining a number of methods of authentication that have been approved by the central government).[18]. As per the circular issued by the UIDAI, the incorporation of FRT is to ensure inclusive authentication and the UIDAI will be working with biometric device providers to integrate needed features into certified registered devices. According to the circular, no further information needs to be captured as a photograph of the resident is captured at the time of enrolment.[19]

The UIDAI has since announced a pilot programme to test the functionality of FRT for financial services, which is being conducted along with the National Payments Corporation

[13] Ibid

[14] https://www.vision-box.com/pressroom/press-releases/vision-box-closes-major-deal-with-bangalore-international-airport-limited

[15] 'Facial recognition: As airports in India start using the technology, how will it be regulated?' available at https://scroll.in/article/929851/facial-recognition-as-airports-in-india-start-using-the-technology-how-will-it-be-regulated

[16] 'Delhi Airport begins facial recognition tech trials for domestic vistara flyers' available at https://inc42.com/buzz/delhi-airport-to-enable-facial-recognition-tech-under-digiyatra/

[17] 'Indian Railways is proposing to implement facial recognition to identify criminals' available at https://www.techradar.com/in/news/indian-railways-looking-to-implement-facial-recognition-to-identify-criminals

[18] "Authentication Ecosystem," Unique Identification Authority of India | Government of India, accessed November 30, 2020, https://uidai.gov.in/aadhaar-eco-system/authentication-ecosystem.html.

[19] https://uidai.gov.in/images/resource/Uidai_circular_Face_authentication_15012018.pdf

of India (NPCI).[20] The NPCI is responsible for operating the Aadhar enabled payment system, which allows individuals to complete transactions using their Aadhar number and biometric verification.[21] This new pilot programme would look to test the feasibility of using facial recognition as a means of verification for such services. It would first be tested on non financial transactions and then rolled out to all transactions depending on the success of the pilot. However, two important questions remain unanswered; Firstly, how was the dataset used to train the algorithm created, and did it constitute images collected from the Aadhar database? Secondly, will facial recognition be extended as a form of authentication for other services linked to Aadhar?

C. Identification of Missing Children

In April 2018, news items reported that the trial of a facial recognition system commissioned by the Delhi High Court helped correctly identify approximately 3000 missing children. The Delhi High Court had in *Sadhan Haldar v The State NCT of Delhi*[22] issued the use of Automated Facial Recognition System (AFRS) for the purpose of tracking and re-uniting children. The system had matched 10,617 children with missing cases from across the country - however, only 3202 of those children's identities have been verified.[23]

D. Identification at political protests

As per a newspaper report[24], the Delhi police used the AFRS software to screen crowds of people who had attended a rally held by the Prime Minister in December 2019. The newspaper report noted that the Delhi Police has so far created a photo dataset of 1,50,000 'history sheeters' (which has been defined as "such persons who figure on the CCTNS data base -- accused persons, prisoners, missing persons and unidentified found persons including children, and unidentified dead persons") for routine crime investigations, 2000 images of terror suspects and a third category of 'miscreants' (no formal definition has been provided for this category). According to the newspaper report, this was the first time FRT had been used at a political rally. The police used a set of facial images collected through filming protests at various spots in the capital through the years to identify law and order suspects.[25]

[20] Soumyarendra Barik, "UIDAI, NPCI Piloting Face Authentication for Aadhaar," *MediaNama* (blog), October 6, 2020, https://www.medianama.com/2020/10/223-aadhaar-facial-recognition/.

[21] "Aadhaar Enabled Payment System (AePS) – Aadhaar Pay | NPCI," accessed January 4, 2021, https://www.npci.org.in/what-we-do/aeps/product-overview.

[22] (W.P. (CRL) 1560/2017

[23] Richa Banka, "Delhi HC Seeks Ministry Officials' Reply on Plea Regarding Difficulty in Tracing Missing Kids," *Hindustan Times*, May 1, 2019, available at https://www.hindustantimes.com/delhi-news/delhi-hc-seeks-ministry-officials-reply-on-plea-regarding-difficulty-in-tracing-missing-kids/story-PAVLYqgD3YJSiqpzj99igM.html.

[24] Jay Mazoomdar, " Delhi Police film protest, run its images through face recognition software to screen crowd", Indian Express, December 28, 2019, available at https://indianexpress.com/article/india/police-film-protests-run-its-images-through-face-recognition-software-to-screen-crowd-6188246/

[25] Jay Mazoomdaar, "Delhi Police Film Protests, Run Its Images through Face Recognition Software to Screen Crowd," *The Indian Express* (blog), December 28, 2019, available at

The people attending the rally were required to pass through a metal detector gate where a camera captured the image of the person and sent a live feed to the control room. The live feed was then compared with an existing dataset. The Delhi police has refused to comment on specific actions taken as a result of their use of FRT at the rally.[26]

E. Deployment by different state law enforcement agencies

(i) Punjab Artificial Intelligence system

The Punjab Police has deployed the use of an AI based facial recognition system known as the Punjab Artificial Intelligence System (PAIS). When confronted with a suspect[27]officers can snap a photograph with their smartphone and search it against a database compiled by uploading pictures of convicted offenders housed in jails across Punjab. The system leverages FRT , natural language processing, gang analysis, and phonetic search technologies and contains name, alias, parents name, date of birth, crime type, FIR number, police acts, facial image and speech text data. The app is equipped with a two layer authentication and access for different users can be managed via a centralised dashboard. No administrative or department changes were made during implementation of the project beyond state level nodal agencies comprised of four - six officers being established. A ‘zone wise’ training is made available to law enforcement officials using the app on download.[28]

(ii) Pehchaan in Uttar Pradesh

Mirzapur in Uttar Pradesh has established the Pehchaan citizen app. The app has integrated Microsoft’s Advanced Facial Recognition Technology[29] and can be used by the public and law enforcement. The app provides users with a confidence score of the likelihood that two faces belong to the same person by running the face against the ‘All India Criminal Database’. As per documentation on the app - law enforcement can create a ‘criminal database’ using the app, hotel owners can upload the details of visitors, employers can use the app for background checks, and the public can use it to verify different people they come into contact with.[30]

https://indianexpress.com/article/india/police-film-protests-run-its-images-through-face-recognition-software-to-screen-crowd-6188246/.

[26] Alexandra Ulmer Siddiqui Zeba, “India’s Use of Facial Recognition Tech during Protests Causes Stir,” Reuters, February 17, 2020, https://www.reuters.com/article/us-india-citizenship-protests-technology-idUSKBN20B0ZQ.

[27] ‘Cops in India are using Artifcial Intelligence that can identify you in a crowd’ available at https://www.huffingtonpost.in/2018/08/15/facial-recognition-ai-is-shaking-up-criminals-in-punjab-but-should-you-worry-too_a_23502796/

[28] Ankit Gupta and Gaurav Gaur, “FICCI Smart Policing Awards 2018: Compendium of Best Practices in Smart Policing” (FICCI, 2018), available at http://ficci.in/spdocument/22984/FICCI-Compendium-of-Best-Practices-in-SMARt-Policing-2018.pdf.

[29] ibid

[30]Ibid

(iii) Face Tagr and Neoface

Similar technology as used in the pehchaan citizen app is also being used by the Chennai Police- the technology known as Face Tagr was first deployed in 2017 in select areas of Chennai.[31] It is used to match real time data emerging from CCTV cameras with the State's criminal database-if the technology identifies any person as a criminal, the police get an immediate notification. Meanwhile, the Surat Police relies upon NEC's Neoface proprietary facial recognition technology to keep a track on interested individuals.[32] The technology was first deployed in areas with high foot traffic and is focused on identifying individuals who have a prior history of pickpocketing. chain snatching and other such crimes.

(iv) e-beat book app

Delhi police is in the process of equipping its beat cops and Police Control Room (PCR) vehicles with remote facial recognition systems[33]. The e-beat book app used by the beat level police office is currently equipped with technology to scan fingerprints. The Delhi Police wants to build on that technology and arm it with FRT. The app is at the pilot stage and has not been rolled out as yet.

F. National Automated Facial Recognition System

Original Request For Proposal

In July 2019, the National Crime Records Bureau (**NCRB**) of the Ministry of Home Affairs published a Request for Proposal (**RFP)**[34] for the National Automated Facial Recognition System (**AFRS)**.

According to the RFP, the system is part of larger efforts to modernize the police force and enable recording, analysis, retrieval and sharing of information between organizations. To do this, the RFP requires the development of a centralized database with capabilities to identify or verify an individual from digital images, videos, and sketches based on features, contours and other prominent data points and should be able to account for changes such as change in facial expression, direction, angle, lighting, age, hairstyle, beard, glasses, scars, marks, and tattoos. The system would be available to police and should be able to perform one to many - including the full database - and one to one comparisons. The AFRS should be able to broadly match a suspect photograph with the database created using photographs available from a number of databases and services including passport services, Crime and Criminal

[31] Anand Murali, "The Big Eye: The Tech Is All Ready for Mass Surveillance in India," FactorDaily, August 13, 2018, available at https://archive.factordaily.com/face-recognition-mass-surveillance-in-india/.

[32] Ibid

[33] Aditi Agarwal, 'Delhi Police working on arming PCR vans with facial recognition software'; November 20, 2020, available at https://www.medianama.com/2020/11/223-exclusive-delhi-police-working-on-arming-pcr-vans-with-facial-recognition-software/

[34] 'Request for Proposal to procure National Automated Facial Recognition System' available at http://ncrb.gov.in/TENDERS/AFRS/RFP_NAFRS.pdf

Tracking Network System (**CCTNS)**[35], Interoperable Criminal Justice System (**ICJS**)[36], Immigration Visa Foreigner Registration Tracking (**IVFRT)**[37], Khoya Paya, Police IT Karnataka, Enterprise e-Cops Telangana, G-Cops, Cyprus Tamil Naidu, e-Gut Gujarat, and state and national automated fingerprint identification system, NAFIS and Crime Analytics solutions o**r any other image database available with police/other entity.**

It should also be capable of matching the suspect's face with pre-recorded feed obtained from pre-recorded video feeds of CCTV cameras deployed in critical identified locations **or with the video feeds received from private or other public organization's video feed.** In addition to carrying out authentication and verification based on images, the solution should be compatible with other biometric solutions in order to create comprehensive biometric authentication reports. The database will cater to two categories, namely criminal and non criminal (i.e, missing person, unidentified, dead persons). The NCRB in its response to a legal notice issued by the Internet Freedom Foundation has stated that the AFRS solution will not be integrated with the Aadhar database.[38] As per the Response, AFRS will run on the state and national level CCTNS/ICJS database. It does not shed further light on the use of the database - stating only "The AFRS will be a centralized web application hosted at the NCRB Data Centre and will be made available for access to only police in the country in a secure environment. Police stations will use the software only for the intended purpose as per a well laid down standard operating procedure (SOP)."[39]

The system would be hosted at the NCRB and is envisioned to store 10 million images and eventually scale to 50 million. The system would need to be compliant with a number of international standards including NIST Data Format for the Interchange of Fingerprint, Facial, Iris & other Biometric Information, JPEG 2000/PNG/BMP lossless compression for mug shots, Electronic Biometric Transmission Specification, a certified version of the Wavelet Scalar Quantization algorithm, ISO 1979405/ICAO compliant and the system should work with ONVIF Profile S and ONVIF Version X compliant camera makes. The RFP also notes that in order to ensure interoperability, e-governance initiatives should simultaneously be moving to adopting the ISO 19794 standard.

[35] The CCTNS is a mission mode project under the National e-governance plan and headed by the NCRB. The project establishes a national database that integrates data from across state level police departments. For more information see: http://ncrb.gov.in/BureauDivisions/cctnsnew/index.html

[36] The ICJS is a system to connect police, courts, prosecution, prisons, and forensic labs into a centralized database to facilitate data exchange. In 2015, the Cabinet Committee on Economic Affairs approved the revamping of the CCTNS to include the integration of the ICJS. For more information see: https://digitalpolice.gov.in/About.html and https://www.svpnpa.gov.in/images/npa/pdfs/SIITApp/PresentationforNPA05072016ver40.pdf

[37] Undertaken by the MHA under the National e-Governance Plan, the IVFRT creates a centralized database to verify travelers and includes identity details, biometrics, registration details, and entry/exit details. For more information see: https://meity.gov.in/content/immigration-visa-and-foreigner%E2%80%99s-registration-tracking-ivfrt

[38] NCRB response to the legal notice sent by the Internet Freedom Foundation seeking a recall of the RFP' available at https://internetfreedom.in/the-ncrb-responds/

[39] NCRB Response to the legal notice issued by Internet Freedom Foundation; November 5 2019, available at https://drive.google.com/file/d/0B3J0iAyRzCGxRXViUWcya3RXS0hXb3cxeDJYQU5DWnZKZnhj/view

It is important to note that CCTV cameras are a premise for the use of AFRS technology. The CCTV camera captures the video recording, the AFRS technology uses that digital information to isolate pictures of individual faces, extract information about facial features from those pictures, compare that information with the watchlist information, and indicate matches between faces captured through the CCTV recording and those held on the watchlist.[40]

From the RFP, the scope of the AFRS is unclear. Phrases such as ‘creation and maintenance of a database of photographs in digital form for sharing by all stakeholders in the system”[41] indicate an open ended mandate for the system to be able to integrate with other databases over time. As the AFRS envisions integration with other databases a key question that arises is to what extent will data be shared across databases? For example, databases like the CCTNS contain more information than just images. Will individuals searching an image in the AFRS also have access to other forms of data stored alongside profiles in the CCTNS? The scope, objective, and purpose of the AFRS needs to still be clearly defined to prevent function creep and ensure the database is limited to criminal purposes and does not extend to uses such as state welfare. What will be the relationship between the AFRS and Aadhaar or other biometric databases? Currently the RFP envisions the AFRS being used to create comprehensive biometric reports. For what purposes would these reports be created and based on what information?

Revised RFP

The aforementioned RFP for the AFRS was recalled and cancelled on 22nd June 2020, and has since been replaced with a new RFP.[42] The new RFP included a number of changes from the initial one. Most notably the revised RFP provided clarity as to the scope of the system[43] - noting that it will not include any integration with CCTV systems and will not mandate the installation of new CCTV cameras. However it is worth noting, that the new RFP expands the data in the AFRS database to include Scene of Crime images/videos - which could potentially contradict with its stance on CCTV cameras. On the technical side[44],the updated RFP removes the need to adhere to strict international standards. Furthermore, it included requirements for the system to be able to integrate with existing crime analytics solutions. Finally, it also does away with the list of databases that will constitute AFRS, thereby allowing the government to have carte blanche over the matter.

[40] R (Bridges) v. Chief Constable of South Wales Police and Ors (2019).

[41] Pg. 1 http://ncrb.gov.in/TENDERS/AFRS/RFP_NAFRS.pdf

[42] National Crime Records Bureau (NCRB), “Request For Proposal To Procure National Automated Facial Recognition System (AFRS)” (Ministry of Home Affairs, Government of India, 2020), available act https://drive.google.com/file/d/1KgnURYsFLBqOhLidW28nrbugI--SnKx5/view. “IFF’s Legal Notice to the NCRB on the Revised RFP for the National Automated Facial Recognition System,” Internet Freedom Foundation (blog), July 15, 2020, available at https://internetfreedom.in/iffs-legal-notice-to-the-ncrb-on-the-revised-rfp-for-the-national-automated-facial-recognition-system/.

[43] ibid

[44] Ibid

Legislative Discussions on the Implementation of FRT

As of July 2021, there has been no discussion in Parliament (at the Union level) on the Artificial Recognition System and only one question has been asked about it. However, questions have been raised in both houses about individual instances wherein Facial Recognition has, or is, to be implemented.

Lok Sabha

- 2nd February 2021: The Minister of State for Home Affairs was asked (a) about the total number of FRT systems being used by the state and central government; (b) whether any guidelines have been laid down for the police forces to prevent the technology from being used for unauthorised surveillance; and (c) whether any study has been conducted by the Central Government on the accuracy of FRT systems being deployed.[45] The Minister in his response stated that 'police' and 'law and order' come within the purview of the state governments and therefore it is the responsibility of the state governments to deal with offences under the existing laws. He also stated that no data in this regard is maintained at a central government level.
- 17th March 2020: The Minister of State for Home Affairs was asked[46] about (a) whether the central government has formulated any action plan for using facial recognition technology for law enforcement purposes and by the security forces; and (b) steps being taken by the government in light of the fact that facial recognition is not entirely accurate and could lead to punitive action against innocent individuals. The Minister did not directly respond to the question about the accuracy of facial recognition technology; he instead stated that the adoption of such technology is an ongoing exercise and that the central government has adopted and promoted emerging technologies for upgradation of police forces from time to time. State Governments also adopt the qualitative requirements and technology directives in such technologies including facial recognition.
- 12th December 2019: A question was posed towards the Minister of Civil Aviation on the implementation of facial recognition at Indira Gandhi International Airport[47]. To which the Minister responded by saying that as per the Digi-Yatra programme facial recognition has been implemented in the airport for a trial period of 3 months, with 2605 passengers having registered as of that point.

[45] Magunta Sreenivasulu Reddy and Vincent H Pala "UNSTARRED QUESTION NO. 191 - Facial Recognition Technology" (Government of India, February 2, 2021), available at http://164.100.47.194/Loksabha/Questions/QResult15.aspx?qref=18796&lsno=17

[46] Amar Singh, "UNSTARRED QUESTION NO. 3847 - Facial Recognition Technology" (Government of India, March 17, 2020), available at http://loksabhaph.nic.in/Questions/QResult15.aspx?qref=15230&lsno=17.

[47] T. R. Paarivendhar, "UNSTARRED QUESTION NO: 4024 Facial Biometric Identification for Air Travel" (Government of India- Lok Sabha, December 12, 2019), available at http://164.100.24.220/loksabhaquestions/annex/172/AU4024.pdf.

- 6th December 2019: The Minister of Woman and Child Development received a question on the implementation of a facial recognition or Aadhar based tracking system to locate missing children[48]. Accordingly it was revealed that the Delhi police was in fact using FRT to help track missing children as per an order from the Delhi High Court.
- 21st March 2018: The Minister of Electronics and Information Technology was asked whether Face Recognition has been introduced as a security feature for data authentication[49], to which the Minister answered that facial recognition will be used in conjunction with other modes of authentication.
- 7th February 2018: Numerous questions regarding the implementation of Facial Recognition in Aadhar authentication were posed to the Minister of Electronics and Information Technology[50]. The response covered the use of facial recognition as one of many means of authentication, the issue of camera quality in capturing pictures for FRT, and some of the safety protocols implemented for FRT in the context of Aadhar.

Rajya Sabha

- 11th February, 2021: The Education Minister was asked amongst other questions over FRT, about (i) the use of FRT by the Central Board of Secondary Education; (ii) the privacy concerns over student's biometric data; (iii) the reasons for the government to go ahead with FRT despite the concerns over the efficacy of the FRT; and (iv) the details of the entities having access to the personal data.[51] The Minister admitted to the use of FRT by CBSE as one of the authentication mechanisms in multi- factor authentication for providing digital marksheets to students. He also submitted that as there is no collection or storage of biometric facial data; the privacy concerns have been addressed. The facial data is not stored on the server and therefore facial image data is not available. The question about the need to go ahead with FRT despite concerns over its efficacy was not addressed.
- 5th March 2020: The Minister of Human Resource Development was asked whether the central government was aware of the use of FRT by certain state governments to take attendance in educational institutions, and whether the central government had plans to introduce such systems as well.[52] In its response the Minister said that the

[48] Kunwar Pushpendra Singh Chandel and Pinaki Misra, "UNSTARRED QUESTION NO: 3117 - Juvenile Homes" (Government of India- Lok Sabha, December 6, 2019), available at http://164.100.24.220/loksabhaquestions/annex/172/AU3117.pdf.

[49] Prabhakar Reddy Kotha, "UNSTARRED QUESTION NO. 4153 - Authentication of Data" (Government of India- Lok Sabha, March 21, 2018), available at http://164.100.24.220/loksabhaquestions/annex/14/AU4153.pdf.

[50] Dinesh Trivedi and Saugata Roy, "UNSTARRED QUESTION NO. 857 - Facial Recognition for Aadhar" (Government of India- Lok Sabha, February 7, 2018), available at http://164.100.24.220/loksabhaquestions/annex/14/AU857.pdf.

[51] Mallikarjun Kharge, "UNSTARRED QUESTION NO. 1173 - Facial Recognition for Digital Documents" (Government of India - Rajya Sabha, February 11, 2021), available at https://pqars.nic.in/annex/253/Au1173.pdf

[52] Mahesh Poddar, "UNSTARRED QUESTION NO. 1671 - AI for taking attendance," (Government of India - Rajya Sabha, March 5, 2020), available at https://rajyasabha.nic.in/rsnew/Questions/QResult.aspx

government did not have any specific information about the use of FRT for attendance in educational institutions and that it did not have any plans to introduce such systems.

- 4th March 2020: The Minister of State for Home Affairs stated that approval has been accorded for the implementation of AFRS by the NCRB. The Minister stated that the AFRS will use police records and will only be accessible to Law Enforcement Agencies[53].
- 6th February 2020: In response to a question on the use of FRT to track missing children[54], the Minister of Women and Child Development explained that the Delhi Police and the Ministry have been using FRT for the purpose of tracing missing children.
- 8th August 2018: The question was posed to the Home Ministry as to whether new technologies were being developed to investigate crime[55]. In his response, the Home Minister mentioned Facial Recognition technology as being one of the technologies developed by the government.

What these questions demonstrate is that discussions surrounding the development and use of FRT, in the legislature, have historically been reactionary as opposed to proactive - with the executive taking most of the initiative in the conceptualisation and implementation of FRT in India. Perhaps as a matter of concern, most of the questions raised in the Lok Sabha and Rajya Sabha did not focus on the privacy and security safeguards in place for the use of FRT or if the development and use was supported by legal backing, appropriate training, and oversight.

FRT through the lens of Right to Privacy

In 2017, the Supreme Court of India held the right to privacy to be a fundamental right under the Indian Constitution[56]. While this right is subject to reasonable restrictions, these restrictions have to comply with a three fold requirement, namely (i) existence of a law; (ii) legitimate state aim; and (iii) proportionality. Therefore, the legal sanction and validity of FRT will have to be viewed through the lens of the conditions prescribed by the Supreme Court. The requirement for the existence of a law emerges from the requirement of Article

[53] A.K Selvaraj, “UNSTARRED QUESTION NO. 1495 - Automated Facial Recognition System,” (Government of India - Rajya Sabha, March 4, 2020), available at https://rajyasabha.gov.in/rsnew/Questions/ShowQn.aspx?tk=b522f26d-2163-480b-9eb6-d3b5e234e438.

[54] Mahesh Poddar, “UNSTARRED QUESTION NO.629 - Tracking of Missing Children” (Government of India - Rajya Sabha, February 6, 2020), available at http://164.100.47.5/qsearch/QResult.aspx.

[55] Manoj Kumar Jha, “STARRED QUESTION NO.234 - New Technologies Used for Investigation of Crimes” (Government of India - Rajya Sabha, August 8, 2018), available at http://164.100.47.5/qsearch/QResult.aspx.

[56] K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1

21 of the Constitution which stipulates that “no person can be deprived of his life or personal liberty, except as per the procedure established by law’. The term ‘procedure established by law’ was elaborated upon the Supreme Court in the case of *Maneka Gandhi v Union of India*[57] where the Supreme Court had held that the law which deprived personal liberty had to be ‘fair, just and reasonable, not fanciful, oppressive or arbitrary. The Court in the case of *Mohd. Arif v Registrar, Supreme Court of India*[58] observed that Article 21 was to be read along with other fundamental rights, thus not only does the procedure established by law have to be just, fair and reasonable, but also the law itself has to be reasonable.

Absence of any legislative backing

The first requirement to be satisfied by the State when it intervenes to encroach on privacy is the existence of a law. There is currently no legislative sanction for the use of FRTs by either the State or any private entity. In July 2019[59] The Internet Freedom Foundation issued a legal notice to the NCRB and the Ministry of Home Affairs seeking a recall of the RFP. The legal notice highlighted the absence of any statutory sanction for the creation of such a system. The NCRB in the Response [60] relied upon a 2009 note of the cabinet which envisaged the creation of six agencies, namely (i) National Automated Fingerprint Identification System; (ii) Fingerprint Enrolment Devices; (iii) Automatic Facial Recognition System; (iv) Mobile Devices Terminals; (v) AVLS and CAD based traffic management system; and (vi) GIS based Crime Analytics.

As per the NCRB, FRT has cabinet approval and therefore there is no need for any legislative or executive order sanctioning the establishment of the AFRS. However, a cabinet approval is not a statutory enactment and it does not confer any legislative authority for the use of facial recognition technology. It cannot be taken in lieu of required legislative sanction. The Supreme Court while deciding upon the validity of Aadhar in K.S. Puttaswamy v Union of India[61] (Aadhar) noted that “an executive notification does not satisfy the requirement of a valid law contemplated under Puttaswamy. A valid law in this case would mean a law passed by Parliament, which is just, fair and reasonable. Any encroachment upon the fundamental right cannot be sustained by an executive notification. The Supreme Court struck down certain requirements of mandatory linkage of scholarships issued by the Central Board of Secondary Education and the University Grants Commission with Aadhar on the grounds that it did not have a legal basis.

[57] (1978) 1 SCC 248

[58] *Mohd. Arif v Registrar, Supreme Court of India* (2014) 9 SCC 737

[59] ‘Legal Notice to recall the Request for Proposal for Automated Facial Recognition System’, July 18, 2019, Internet Freedom Foundation, available at https://internetfreedom.in/maskon/

[60] ‘NCRB Response to the legal notice received from Internet Freedom Foundation’, November 5, 2019, available at https://internetfreedom.in/the-ncrb-responds/

[61] (2019) 1 SCC 1

Not in conformity with the principle of legitimate state aim and proportionality

In Puttaswamy, the Supreme Court had held that "the requirement of a need, in terms of a legitimate state aim, ensures that the nature and content of the law which imposes the restriction falls within the zone of reasonableness mandated by Article 14, which is a guarantee against arbitrary state action.[62]" In the absence of a legal basis for using FRT which clearly specifies the different grounds and rationale for the deployment of FRT, it becomes difficult to ascertain whether a legitimate or proportionate objective is being fulfilled. As has been highlighted earlier, FRT has been deployed for multiple purposes; in airports (to give a "seamless, hassle-free and paperless journey experience to every air traveller in India"[63]) by law enforcement agencies (to identify and capture criminals), by educational institutions (to track the attendance of students and teachers); and now the NCRB has released a RFP for creating the AFRS for a variety of purposes including for "identifying criminals, missing children/persons, unidentified dead bodies and unknown traced children/persons all over the country."[64]

As can be seen, there is no singular or specific purpose for the use of FRT, it varies from identifying criminals, locating missing children to ensuring hassle free air travel for passengers. It is pertinent to note that while the RFP for the creation of AFRS indicates multiple uses of such a system (including criminal investigations), the Response stipulates that while AFRS aims to identify individuals across various databases such as ICJS, CCTNS, Immigration Visa Foreigner Registration Tracking (IVFRT) and other databases available with State police, its primary use will be for identifying unidentified persons/dead persons.

The third test to be complied with is 'proportionality'- the means which are adopted by the legislature are proportional to the object and needs sought to be fulfilled by the law. The Supreme Court in Modern Dental College & Research Centre v State of Madhya Pradesh[65] specified the components of proportionality standards:

- A measure restricting a right must have a legitimate goal;
- It must be a suitable means of furthering this goal;
- There must not be any less restrictive, but equally effective alternative; and
- The measure must not have any disproportionate impact on the right holder.

[62] K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC

[63] "Digi Yatra"- Reimagining Air Travel in India, August 9, 2018 available at http://civilaviation.gov.in/sites/default/files/Digi%20Yatra%20Policy%2009%20Aug%2018.pdf

[64] The original RFP has since been taken down by the government but a copy can be found at: National Crime Records Bureau (NCRB), "Request For Proposal To Procure National Automated Facial Recognition System (AFRS):" (Ministry of Home Affairs, Government of India, n.d.), https://www.medianama.com/wp-content/uploads/RFP_NAFRS.pdf.

[65] *Modern Dental College & Research Centre v State of Madhya Pradesh,* (2016)7 SCC 353

The proportionality standard was approved by the Supreme Court in the 2018 Puttaswamy judgement (Aadhaar). The court while rejecting the requirement of mandatory linkage of bank accounts with Aadhaar noted that imposing such a restriction on the entire population, without any evidence of wrongdoing on their part, would constitute a disproportionate response.[66] The Court held that "under the garb of prevention of money laundering or black money there cannot be such a sweeping provision which targets every resident of the country as a suspicious person. Presumption of criminality is treated as disproportionate and arbitrary."[67]

Deployment of FRT over large segments of the population for varied reasons may be regarded as disproportionate to the objective sought to be achieved. Depending upon the objective sought to be achieved by the use of FRT, it is necessary to understand whether the government could adopt an alternative, less intrusive mechanism to achieve the said objective. With respect to analysing the proportionality of the AFRS, it is important to understand that the RFP does not stipulate any data minimisation or data retention measures to be adopted for establishing such a system. It is silent on the sources of images that can be legitimately used by the system, the gravity of offences that might qualify for its use, or checks against any further mission creep in the purposes for which the AFRS may be used[68]. At the same time the RFP envisions the AFRS to have the capacity to store 10 million images and eventually scale to 50 million.

Legal Frameworks and FRT in India

Legislation

(i) The draft Personal Data Protection Bill 2019 and FRT

In 2018, the Ministry of Electronics and Information Technology, Government of India had constituted a Committee of Experts to frame recommendations for a data protection framework in India. The Committee submitted its report[69] and a draft Personal Data Protection Bill in July 2018[70]. On December 11, 2019, the Central Government introduced

[66] Smriti Parsheera, "Adoption and Regulation of Facial Technologies in India: Why and Why not?", National Institute of Public Finance and Policy, November 2019, available at https://www.datagovernance.org/files/research/NIPFP_Smriti_FRT_-_Paper_5.pdf

[67] *K.S. Puttaswamy v. Union of India*, (2019) 1 SCC 1

[68] Smriti Parsheera, "Adoption and Regulation of Facial Technologies in India: Why and Why not?", National Institute of Public Finance and Policy, November 2019, available at https://www.datagovernance.org/files/research/NIPFP_Smriti_FRT_-_Paper_5.pdf

[69] Committee of Experts, "A Free and Fair Digital Economy Protecting Privacy, Empowering Indian" (Ministry of Electronics and Information Technology, n.d.), available at https://www.thehinducentre.com/resources/article24561547.ece/binary/Data_Protection_Committee_Report-com.

[70] Committee of Experts, "The draft personal data protection bill, 2018" (Ministry of Electronics and Information Technology, 2018), available at https://www.prsindia.org/sites/default/files/bill_files/Draft%20Personal%20Data%20Protection%20Bill%2C%202018%20Draft%20Text.pdf.

the Personal Data Protection Bill (PDP Bill) in Parliament[71]. The Bill has been referred to a Joint Parliamentary Committee and the Committee is expected to submit its report in December 2021.

Facial images, iris scans, fingerprints fall within the definition of biometric data under the Bill and they are further recognised as sensitive personal data in terms of clause 3(36). Under the PDP Bill, the proposed Data Protection Authority will notify any existing data fiduciary as a significant data fiduciary, if the said data fiduciary uses new technology for processing or on the basis of the sensitivity of the personal data processed.[72] If the significant data fiduciary intends to use any new technology or use any sensitive personal data such as genetic data or biometric data, it cannot commence processing such data until it has undertaken a Data Protection Impact Assessment.[73] Thus for use of facial recognition technology both public sector and private sector data fiduciaries will be required to conduct a data protection impact assessment prior to commencing with the deployment of facial recognition technology.

However, the PDP Bill also provides that the Central Government if it is satisfied that it is necessary or expedient[74] to do so, may by a written order exempt any agency of the Government from the application of all or any of the provisions of this Bill, subject to such procedure, safeguards and oversight mechanism as may be prescribed. A blanket exemption has been provided to the Central Government to exempt any agency of the Central Government from any or all of the provisions of the Bill. Therefore, it is possible for the Government to exempt law enforcement agencies from the requirements of the Bill, including the need to undertake a data protection impact assessment and to exempt law enforcement agencies from being notified as significant data fiduciaries under the Bill.

Further, clause 36 of the Bill also provides for exemption of certain provisions of the Bill in cases where the personal data is processed in the interests of prevention, detection,investigation and prosecution of any offence or any other contravention of any law. This includes exemption from classification as a significant data fiduciary and the need to undertake a data protection impact assessment.

The Bill establishes a Data Protection Authority (DPA) to ‘protect the interests of the data principal, prevent any misuse of personal data and ensure compliance with the provisions of the Bill’. Under the Bill, the DPA has the authority over the processing of personal data by private data fiduciaries as well as the State. The powers of the DPA range from advising the

[71] “The personal data protection bill, 2019,” Pub. L. No. 373 of 2019 (2019), available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

[72] Clause 26(1)(e)

[73] Clause 27(1)

[74] Clause 35: “Where the Central Government is satisfied that it is necessary or expedient, (i) in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign states, public order; or (ii) for preventing incitement to the commission of any cognisable offence relating to sovereignty and integrity of India, the security of the State, friendly relations with foreign states, public order, it may, by order, for reasons to be recorded in writing, direct that all or any of the provisions of this Act shall not apply to any agency of the Government in respect of processing of such personal data, as may be specified in the order subject to such procedure, safeguards and oversight mechanism to be followed by the agency as may be prescribed.”

Government and any other authority on measures to be taken to protect personal data[75] to ascertain the circumstances where a data protection impact assessment shall be mandatory. It also has the power to conduct an inquiry either suo moto or on the basis of a complaint received by it, if it has reasonable grounds to believe that the activities of the data fiduciary are being conducted in a manner which is detrimental to the data principal. But by virtue of clauses 35 and 36 of the Bill, the Central Government can exempt surveillance and law enforcement agencies from the jurisdiction of the DPA thereby preventing the DPA from conducting an investigation into the use of FRT by the State.

It is pertinent to note that clause 92 of the Bill states that no data fiduciary can process such biometric data as may be notified by the Central Government, unless such processing is permitted by law. Biometric data includes facial images, fingerprints and iris scans[76]; therefore, if the Bill is enacted with this provision in place, the Central Government will have to specifically permit the use of FRT by law enforcement and ensure that it is backed by a valid law.

There are also several statutes that permit and regulate state surveillance including interception, decryption of communications, monitoring of traffic data, and access to stored information. The use of FRT does not fit clearly into any of the surveillance capabilities that are legally backed in India. The use of the technology could be understood as a tool used by law enforcement to carry out their duties as articulated under State Police Acts and associated Police Manuals. As noted earlier, the use of such technology by different law enforcement agencies will have to satisfy the three fold requirement laid down by the Supreme Court in Puttaswamy; namely; (i) legality, i.e. there should be a valid law passed by either the central government or the state legislature; (ii) legitimate state aim; and (iii) it should satisfy the test of proportionality; i.e that it should be the least effective restrictive measure.

As per publicly available information[77], the Ministry of Home Affairs has prepared amendments to the Identification of Prisoners Act 1920 through the draft bill titled ‘The Identification of Prisoners and Arrested Persons Bill, 2020’ to provide legislative backing for the collection of fingerprints, palm prints, photos, iris and retina images, voice samples and vein patterns. It will allow police agencies to collect biometric samples of prisoners as well as individuals summoned for interrogation. This could be understood as a move to provide legal backing to the use of FRT in India for criminal purposes.

Key provisions that govern surveillance in India are the Telegraph Act, 1885, the Information Technology Act, 2000 and the Code of Criminal Procedure, 1973. The interception of posts/telegraphs is governed by the Telegraph Act, whereas the Information Technology Act enables the government to access information collected in computer

[75] Clause 49(2)(l)

[76] Clause 3(7): “biometric data means facial images, fingerprints, iris scans, or any others similar personal data resulting from measurements or technical processing operations carried out on physical, physiological, or behavioural characteristics of a data principal, which allow or confirm the unique identification of that natural person.”

[77] “New Bill could unleash facial recognition free-for-all”, the Ken, February 11, 2020, available at https://the-ken.com/story/new-bill-facial-recognition-free-for-all/?searchTerm=facial%20recognition

records. In addition to these laws, Sections 91 and 92 of the Code of Criminal Procedure can also be used for targeted surveillance. Section 91 empowers a Court or any officer in charge of a police station to summon "any document or any other thing" from a person,if it is "necessary or desirable" for the purposes of any investigation, inquiry,trial or other proceeding under the Code. This provision is often used by the police to seek information from intermediaries, or otherwise access stored data. Further, Section 92 regulates the interception of a document, parcel or thing in the custody of a postal or telegraph authority.

Information Technology (Amendment) Act, 2008

Section 69 and 69 B of the Information Technology (Amendment) Act, 2008, lay down provisions for the interception, monitoring and decryption of digital information and data by the State.

1. Section 69 and associated Rules[78] establish grounds and procedures for authorized agencies to intercept, decrypt, and monitor information generated, transmitted, received or stored in any computer resource.

2. Section 69 B and associated Rules[79] establish grounds and procedures for authorized agencies to monitor and collect traffic data or information generated, transmitted, received, or stored in any computer resource.

The following paragraphs provide a comparison of rules between the rules under Section 69 and Section 69 B of the IT Act.

a. Grounds

   - Section 69 - The ground under the rules are as follows: (i) sovereignty and integrity of India; (ii) defence of India; (iii) security of the State; (iv) friendly relation with foreign States; (v) public order; (vi) preventing incitement to the commission of any cognizable offence relating to above; or (vii) investigation of an offence.

   - Section 69(B) - To enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country.[80]

[78] The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009

[79] The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009

[80] As per Rule 3(2) of the the Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009, the purposes relating to cyber security include; (i) forecasting of imminent cyber incidents; (ii) monitoring network application with traffic data or information on computer resource; (iii) identification and determination of viruses or computer contaminant; (iv) tracking cyber security breaches or cyber security incidents; (v) tracking computer resource breaching cyber security or spreading virus or computer contaminants; (vi) identifying or tracking any person who has breached, or is suspected of having breached or likely to breach cyber security; (vii) undertaking forensic of the concerned computer resource as a part of investigation or internal audit of information security practices in the computer resources; (viii) accessing stored

b. Authorisation

- Section 69 - No person shall be able to carry out interception, decryption or monitoring of any information generated, transmitted, received or stored in any computer resource under Section 69 (2) without an order issued by a competent authority.
- Section 69(B) - No directions for monitoring and collection of traffic data or information under Section 69B(3) of the Act shall be issued, except by an order made by the competent authority.

c. Competent Authority

- Section 69 - The competent authorities include (i) Secretary in the Ministry of Home Affairs in cases relating to the central government; or (ii) the Secretary of the Home Department in the case of a state government or union territory. In case of unavoidable circumstances, an order may be issued by an officer not below the rank of joint secretary, duly authorised by the competent authority. In case of an emergency either i) in a remote area where getting prior directions is not feasible or ii) for operational reasons getting directions is not feasible - then any such activity can be carried out with " the prior approval of the Head or the second senior most officer of the security and law enforcement agency. In such cases, the competent authority must be informed within 3 working days and their consent must be sought.
- Section 69(B) - Secretary to the Government of India in the Department of Information Technology under the Ministry of Communications and Information Technology.

d. Standard of Necessity

- Section 69 - Before issuing the order, the competent authority must "consider the possibility of acquiring the necessary information by other means and the direction under Rule (3) shall be issued only when it is not possible to acquire the information by any other reasonable means.
- Section 69(B) - The rules do not outline any standard of necessity that must be taken into consideration by the competent authority before the issuing of an order.

e. Review Procedure

- Section 69 - Copy of the order has to be submitted before the review committee within a maximum period of 7 working days from the date of the issuance of the order. The committee has to meet at least once within a

information for enforcement of any provisions of the laws relating to cyber security for the time being in force; and (ix) any other matter relating to cyber security.

period of 2 months to determine whether the orders issued are in compliance with the prescribed procedure and law.

- Section 69(B) - A copy of the order has to be submitted before the review committee within a maximum period of 7 working days from the date of the issuance of the order. The committee has to meet at least once within a period of 2 months to determine whether the orders issued are in compliance with the prescribed procedure and law.

f. Review Committee Membership

- Section 69 - At the Union level, the review committee consists of the Cabinet Secretary as the Chairman, the Secretary to the Government of India Incharge, Legal Affairs and the Secretary to the Government of India, Department of Telecommunications. At the State level, it consists of the Chief Secretary as Chairman, the Secretary Law/Legal Remembrancer Incharge, Legal Affairs and Secretary to the State Government (other than the Home Secretary).

- Section 69(B) - At the Union level, the review committee consists of the Cabinet Secretary as the Chairman, the Secretary to the Government of India Incharge, Legal Affairs and the Secretary to the Government of India, Department of Telecommunications. At the State level, it consists of the Chief Secretary as Chairman, the Secretary Law/Legal Remembrancer Incharge, Legal Affairs and Secretary to the State Government (other than the Home Secretary).

g. Review Committee Powers

- Section 69 - Where the Review Committee is of the opinion that the directions are not in accordance with the specified provisions, it may set aside the directions and issue an order for destruction of the copies, including a corresponding electronic record of the intercepted or monitored or decrypted information.

- Section 69(B) - Where the Review Committee is of the opinion that the directions are not in accordance with the provisions referred to above, it may set aside the directions and issue an order for destruction of the copies, including a corresponding electronic record of the monitored or collected traffic data or information.

h. Duration of the Order

- Section 69 - Unless not revoked earlier, the order can be in force for 60 days from the date of issuance of the order. The order can be renewed from time to time for a period not exceeding a total of 180 days.

- Section 69(B) - All records to be destroyed within a period of 9 months from the receipt of direction or creation of a record, whichever is later, except in a case where the traffic data or information is, or is likely to be, required for functional requirements. The intermediary is required to destroy the order issued by the competent authority for the monitoring or collection of information within a period of 6 months of discontinuance of the monitoring or collection of traffic data, except if the order is required for any ongoing criminal proceedings.

i. Confidentiality

- Section 69 - The information shall not be disclosed or shared by the authorised agency for any purpose other than for investigation, sharing with a security agency for the purpose of an investigation or as part of judicial proceedings before the competent court. Other than this, no acquired information shall be disclosed to the public. This shall also extend to the details of the order and directions issued by the competent authority.
- Section 69(B) - The details of monitored or collected traffic data or information shall not be used or disclosed by any appointed intermediary. Any information collected shall not be used or disclosed by the authorised agency, except for forecasting imminent cyber threats or general trend of port-wise traffic on the internet, or general analysis of cyber incidents, or for investigation or in judicial proceedings before the competent court in India. Other than the instances mentioned above, strict confidentiality shall be maintained in respect of directions for monitoring or collection of traffic data or information issued by the competent authority under these rules.

Intelligence agencies that are authorized to carry out interception under the Act were notified in 2018 and include the intelligence bureau, narcotics control bureau, enforcement directorate, central board of direct taxes, directorate of revenue intelligence, central bureau of investigation, national investigation agency, cabinet secretariat, directorate of signal intelligence, Commissioner of Police Delhi.[81]

3. Section 79(2)(c) and its associated rules[82] also outline the requirements for cyber cafes in India to maintain records of details of users including type and details of identifying documents, name, address, gender, contact, date, computer terminal identification, log in time and log out time. These records are subject to check by an authorised officer of the registration agency.

Does the IT Act and its sections constitute a legal basis for FRT?

As mentioned in the prior section on the right to privacy there is no explicit law mandating the use of FRT - a requirement mandated by the Supreme Court under Puttaswamy. However, it is plausible to imagine that the State may, in the absence of such a law, rely on

[81] http://egazette.nic.in/WriteReadData/2018/194066.pdf
[82] Ministry of Communications and Information Technology, “Information Technology (Guidelines for Cyber Cafe) Rules, 2011,” April 11, 2011, available at wipo.int/edocs/lexdocs/laws/en/in/in100en.pdf.

the aforementioned sections of the IT act for a legal basis - by arguing that the usage of FRT is merely an extension of the powers of surveillance granted to the state by the act. To that end it is worth examining whether, despite not explicitly authorising it, the IT act can act as a legal basis for FRT.

The Act defines data as “a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network . and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.”[83] Furthermore it defines information as including “ data, message, text, images, sound, voice, codes, computer programmes, software and databases or microfilm or computer generated microfiche”.[84]

Applying the definitions of information and data under these clauses, it is apparent that the state possesses the ability to undertake surveillance of existing computer systems and develop a database of information (subject to this database being limited by Section 69B (8) which outlines the timelines for destruction of records).

However, what is not apparent is whether facial recognition would fall within the scope of ‘interception, decryption and monitoring’ - which are the activities that the sections mandate. This leads to questions as to how the data collected under the IT Act can be used by the state. If one is to view the application of FRT as being a separate activity beyond the scope of ‘interception, decryption or monitoring’, then it is clear that the IT Act does not explicitly allow for the implementation of facial recognition by the state.

FRT should not be considered simply as an extension of ‘interception, decryption and monitoring’; then it is feasible that the IT Act would in fact satisfy the legality test outlined in Puttaswamy, i.e any circumvention of the right to privacy can only occur in an instance wherein a law mandating it exists. In such a case, the legality of the use of FRT would then be contingent on the legitimate state aim and proportionality test outlined by Puttaswamy.

Ultimately, while the IT Act would allow for states to collect data and information from existing CCTV feeds, it is unclear whether this data or information could be used as part of a wider FRT infrastructure. What is clear however, is that the IT Act cannot be used as explicit legal validation for the setting up of such an FRT infrastructure, e.g. this act cannot be used to justify the setting up of dedicated FRT cameras.

Indian Telegraph Act, 1985

Section 5 and the associated 419A[85] rules establish grounds and procedure for the interception of communications by intelligence agencies.

[83] Information Technology (Amendment) Act, 2008
[84] Ibid
[85] Ministry of Communications and Information Technology, “Rule 419A of the Indian Telegraph Rules, 1951,” March 1, 2007, available at https://dot.gov.in/sites/default/files/march2007.pdf.

- The provisions of the associated 419A rules are similar to those of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, when dealing with authorization, standard of necessity, time frame and review procedure.

- While mostly similar, some key distinctions do exist between the laws[86]. The first, and most significant, of these relates to the standard of necessity that must be met by the competent authority in the issuing of any direction. In the case of the Telegraph act the competent authority must consider the acquisition of the necessary information by other means "while issuing directions[87]", whereas in the IT Act, this must be done "before issuing any direction.[88]" This change seems to enforce a stricter standard to be met by the competent authority to prove the necessity of any interception before the issuing of any order in the case of the IT Act, when compared to the Telegraph act.

- Secondly, changes have been made with respect to the punishment of a service provider. While the 419A rules explicitly lay down a punishment in saying "not only fine but also suspension or revocation of their licenses[89]", the rules under section 69 state the intermediary or person in charge's liability "for any action under the relevant provisions of the time being in force.[90]" In doing so it has broadened the scope of punishment for offences under the IT Act.

- Changes have also been made to the language of the IT Act so as to clarify provisions previously stated in the Telegraph Act. One such example is 419A rules prescribing that "the service providers shall designate two senior executives of the company[91]" whereas the 69 rules explicitly define the roles of these executives by stating that "every intermediary or person in-charge of computer resource shall designate an officer to receive requisition, and another officer to handle such requisition."[92]

- Beyond these changes, the 69 rules has had numerous clauses added to it that are missing in the 419A rules. These include a list of definitions[93], the explicit requirement for the competent authority to be informed by the issuing officer of the state of emergency[94], clauses relating to the authorisation of government agencies to perform interception, monitoring and decryption activities[95], procedure for states to obtain authorisation to issue orders for interception,

[86] Jadine Lannon, "Indian Telegraph Act, 1885, 419A Rules and IT (Amendment) Act, 2008, 69 Rules," *The Centre for Internet and Society* (blog), April 28, 2013, available at https://cis-india.org/internet-governance/blog/indian-telegraph-act-419-a-rules-and-it-amendment-act-69-rules.
[87] Supra 50, §3
[88] Supra 46, §8
[89] Supra 50, §15
[90] Supra 46, §21
[91] Supra 50, §10
[92] Supra 46, §14
[93] Ibid, §2
[94] Ibid, §3
[95] Ibid, §4

monitoring and decryption activities outside of their jurisdiction[96], rules regarding the non destruction of records of directions provided in instances wherein it is required for an ongoing investigation, criminal complaint or legal proceeding[97], prohibition of carrying out interception, monitoring and decryption activities without prior authorisation[98] and the prohibiting of disclosure of any intercepted, monitored or decrypted information.[99]

Section 7 enables the government to define and issue telecom licenses.

Any company looking to apply for a telecom license will be offered a Unified License (UL), with the terms and conditions of the various services that the company may look to offer.[100] The provisions stipulated under this unified license are as follows:[101]

- Provision for Interception: The UL requires that requisite monitoring and interception facilities for each type of service be provided by the Licensee at their own cost as per the government's requirements.[102]
- Encryption: The Licensee shall be barred from employing bulk encryption equipment in its network.[103]
- Privacy: The Licensee must take all necessary steps to ensure the confidentiality of client and customer data and information[104]. This includes the prevention of divulging of information by any person acting on behalf of the Licensee. The two exceptions to this are those situations wherein the party that is the subject of the information consents to the divulging of the information or wherein the information is already publicly available.[105]
- Lack of Remote Access: "Under no circumstances, should any Remote Access to the suppliers/manufacturers and affiliate(s) be enabled to access Lawful Interception System(LIS), Lawful Interception Monitoring(LIM), Call contents of the traffic and any such sensitive sector/data, which the

[96] Ibid, §5
[97] Ibid, §23(2)
[98] Ibid, §24

[99] Ibid, §25
[100] Vipul Kharbanda, "Policy Paper on Surveillance in India," *The Centre for Internet and Society* (blog), August 3, 2015, available at https://cis-india.org/internet-governance/blog/policy-paper-on-surveillance-in-india#_ftn14.
[101] Ministry of Communications and Information Technology, "License Agreement for Unified License" (Government of India, n.d.), available at https://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf.
[102] Chapter IV, Para 23.2 of the UL
[103] Chapter V, Para 37.1 of the UL
[104] Chapter V, Para 37.3 of the UL
[105] Chapter V, Para 37.2 of the UL

Licensor may notify from time to time.[106] The Licensee Company is not allowed to use remote access facility for monitoring of content.[107]

- Monitoring as per the Telegraph Act: All monitoring must be done in accordance with the provisions of the Telegraph Act, 1985.[108]
- Service Specific Provisions: While these are general provisions, the license stipulates provisions specific to each of the services under it:
    - ❖ Access Service - The designated person of the Central/ State Government shall have the right to monitor the telecommunication traffic in every MSC/ Exchange/ MGC/ MG/ Routers or any other technically feasible point in the network set up by the Licensee. The Interface requirements as well as features and facilities as defined by the Licensor should be implemented by the Licensee for both data and speech. Call records must be maintained along with records of other associated information such as time, date and location information. The Licensee is required to provide the call data records of all the specified calls handled by the system at specified periodicity, as and when required by the security agencies.[109]
    - ❖ Internet Service - The Licensee is required to maintain Call Data Records/IP Data Records for the internet including Internet Telephony Service for a minimum period of one year. The Licensee shall maintain log-in/log-out details of all subscribers for services provided such as internet access, e-mail, Internet Telephony, IPTV etc. These logs shall be maintained for a minimum period of one year[110]. Lawful Interception and Monitoring (LIM) systems of requisite capacities are to be set up by the Licensees for Internet traffic including Internet telephony traffic through their Internet gateways and /or Internet nodes at their own cost, as per the requirement of the security agencies or government.[111]
    - ❖ National Long Distance Service - The requisite monitoring facilities are required to be provided by the Licensee as per requirement of the Licensor.[112]
    - ❖ International Long Distance Service - The designated person of the Central/ State Government, in addition to the Licensor or its nominee, has the right to monitor the telecommunication traffic in every ILD Gateway / Routers or any other technically feasible point

[106] Chapter VI, Para 39.23(xii) of the UL
[107] Chapter VI, Para 39.23 (xiii) of the UL
[108] Chapter VI, Para 39.23 (xix) of the UL
[109] Chapter VIII, Para 8.3 of the UL
[110] Chapter IX, Para 7.1, 7.2, 7.3 of the UL

[111] Chapter IX, Para 8.1 of the UL
[112] Chapter X, Para 5.2 of the UL

in the network set up by the Licensee. The Licensee is required to make arrangements for monitoring simultaneous calls by Government security agencies.[113]

- Global Mobile Personal Communication by Satellite (GMPCS) Service - The designated Authority of the Central/State Government as conveyed by the Licensor from time to time shall have the right to monitor the telecommunication traffic in every Gateway set up in India.[114]
- Public Mobile Radio Trunking Service (PMRTS) - Suitable monitoring equipment as may be prescribed by the Government for each type of System used will be provided by the Licensee at his own cost for monitoring, as and when required.[115]
- Very Small Aperture Terminal (VSAT) Closed User Group (CUG) Service - Requisite monitoring facilities/ equipment for each type of system used, shall be provided by the Licensee at their own cost for monitoring as and when required by the Government.[116]
- Surveillance of MSS-R Service - The Licensee has to provide at its own cost technical facilities for accessing any port of the switching equipment at the HUB for interception of the messages by the designated authorities at a location as and when required.[117]
- Resale of International Private Leased Circuit (IPLC) Service- The Licensee has to take IPLC from the licensed ILDOs. The interception and monitoring of Resellers circuits will take place at the Gateway of the ILDO from whom the IPLC has been taken by the Licensee. The provisioning for Lawful Interception & Monitoring of the Resellers' IPLC shall be done by the ILD Operator and the concerned ILDO shall be responsible for Lawful Interception and Monitoring of the traffic passing through the IPLC.[118]

Does the telegraph act provide a legal basis for FRT?

Much like in the case of the IT Act, the extent to which the telegraph act authorizes the use of FRT is dependent on whether the use of FRT can be classified as being under the scope of 'monitoring.' As with the IT Act, it is unclear whether such an argument would satisfy the test of legality outlined in Puttaswamy. And should it satisfy such a test, it would still have to pass the tests of legitimate state aim and proportionality.

[113] Chapter XI, Para 6.6 of the UL
[114] Chapter XII, Para 7.4 of the UL
[115] Chapter XIII, Para 7.1 of the UL
[116] Chapter XIV, Para 8.1 of the UL
[117]Chapter XV, Para 8.1 of the UL
[118] Chapter XVI, Para 4.1 of the UL

The Code of Criminal Procedure

Section 91 and 92 of the Code of Criminal Procedure 1973,[119] are commonly used by law enforcement to request access to stored data. Section 91 enables any court in India or officer in charge of a police station to summon a person to produce a document or any other thing that is needed for the purposes of an investigation, inquiry, trial or other proceeding. Section 92 enables a District Magistrate or court to order the interception of a document or thing in the custody of the postal or telegraph authority. Furthermore, police authorities could make use of facial recognition technology in instances wherein individuals are in violation of orders passed under Section 144 of the CrPC; which empowers the district magistrate of a state to issue orders directing either a specific individual or a group of individuals to abstain from doing certain acts.[120]

Given the broad framing of sections 91 and 92, as well as the PDP bill's exemption in cases of state security, such a scenario could arise wherein the police could utilise image data gathered from a multitude of sources to conduct surveillance through FRT. Meanwhile, section 144 can be used to prohibit citizen's actions such as gathering for peaceful protest. This can be then used in conjunction with the exemption in the PDP bill to justify the use of FRT on protesters.[121]

State Police Acts and Model Police Manual

Given the lack of a dedicated FRT law, the manner of deployment and use of FRT systems is often left to individual police departments. Therefore, this can result in an immense variance as it pertains to scope, data use, and applicability of use of FRT systems across states and police departments.

In India, law enforcement is regulated via regulation and policy developed at the State level. Thus, each state in India has its own Police Act and associated Police Manual to govern the day to day functioning of its police forces. A Model Police Manual on which these can be based has been issued by the Bureau of Police Research and Development. The fact that each State has its own Police Act and Manual has resulted in unharmonized policies, practices, and standards with respect to police action and practice.

CCTV Policies

A number of cities have also installed city- wide CCTV systems. The regulation of these appears to be taking place at the city level and with different approaches and requirements:

[119] "Section 91 in The Code Of Criminal Procedure, 1973," accessed January 5, 2021, available at https://indiankanoon.org/doc/788840/.
"Section 92 in The Code Of Criminal Procedure, 1973," accessed January 5, 2021, available at https://indiankanoon.org/doc/1544088/.

[120] "Section 144 in The Code Of Criminal Procedure, 1973," accessed January 5, 2021, available at https://indiankanoon.org/doc/930621/.

[121] "Facial Recognition Technologies in India: Why We Should Be Concerned," accessed January 4, 2021, available at https://blog.theleapjournal.org/2020/01/facial-recognition-technologies-in.html.

No	City	Document	Issued by	Details
1	Delhi	Delhi Rules for Regulation of CCTV Systems in NCT of Delhi, 2018[122]	Lt. Governor of National Capital Territory of Delhi	● Legally required reporting to the Delhi Police on installation and use of CCTV systems in public spaces ● Notice of the presence of a CCTV system in Public Places ● Limitations on use of footage ● Encrypted storage of information ● Limitations on access to footage ● Pre-determined but undefined retention period
2	Mumbai	Voluntary Code of Practice for CCTV based Surveillance by Public and Private Establishments in Navi Mumbai, 2014[123]	Navi Mumbai Police	● Rules applicable to certain public and private establishments ● Use of CCTV for a specified reason or an identified need ● Video Feed to be stored for a minimum of 5 days, with video being at least 5FPS ● Sharing of CCTV data with Navi Mumbai Police

[122] Government of NCT of Delhi, "Delhi Rules for Regulation of CCTV Systems in NCT of Delhi, 2018," 2018, available at http://dceast.delhigovt.nic.in/wps/wcm/connect/b4db69004622dcdbb778b7c8da9eb17e/CCTV.pdf?MOD=AJPERES&lmod=1855201116&CACHEID=b4db69004622dcdbb778b7c8da9eb17e.

[123] Navi Mumbai Police, "Voluntary Code of Practice For CCTV Based Surveillance by Public and Private Establishments in Navi Mumbai," August 4, 2014, available at http://www.mahapolice.gov.in/files/code_practice/1.pdf.

3	Bangalore	Karnataka Public Safety (Measures) Enforcement Rules, 2018[124]	Karnataka Legislative Assembly	● Places legal requirements on certain commercial, industrial, infrastructure and residential establishments to have 24x7 CCTV coverage ● Establishes clear technical guidelines for CCTV cameras and mandates a 30 day backup with video in 1920x1080p or higher resolution ● The rules mandate the creation of a special wing of the police specialising in the field of functioning of electronic devices ● Routine checks of CCTV systems by local police
4	Surat	Request for Proposal for Selection of implementing agency for Suman eye[125] / Suraksha Setu: Safe City Project[126]	Surat Municipal Corporation	● Surveillance system run by the Surat Municipal Corporation for traffic control ● 24x7 feed, with 30 days retention capabilities at 1920x1080p resolution ● Centralized data and command center with a 'Video wall' capable of showing feeds from multiple

[124] Home Secretariat, "Karnataka Public Safety (Measures) Enforcement Rules, 2018 - Notification" (Government of Karnataka, June 28, 2018), available at http://www.gazette.kar.nic.in/26-7-2018/Part-4A-(Page-4891-4910).pdf.
"Karnataka Public Safety (Measures) Enforcement Act, 2017," Pub. L. No. L.A. Bill No 36 of 2017 (n.d.), available at http://dpal.kar.nic.in/ao2017/44%20of%202017%20(E).pdf.

[125] Smart City Development Limited, "Request for Proposal for Selection of Implementing Agency for Suman Eye (CCTV Network) Project," September 25, 2018, available at https://www.suratsmartcity.com/Documents/Tenders/SSCDL_SumanEye_RFP_01_2018.pdf.

[126] Department of Administrative Reforms and Public Grievances, "Suraksha Setu: Safe City Project," 2015, available at https://nceg.gov.in/sites/default/files/nceg2015/case-studies/Case%20Study%20-%20Suraksha%20Setu%20v2.0%20.pdf.

				cameras in real time ● Suman Eye shall be integrated with pre existing surveillance infrastructure in Surat ● Police forces have complete access to the feed from the system
5	Hyderabad	The Andhra Pradesh Public Safety (Measures) Enforcement Rules 2014[127]	Andhra Pradesh Legislative Assembly	● The laws operate almost identically to those laid down by the Karnataka Public Safety (Measures) Enforcement Rules - These rules were the framework on which the Karnataka rules were based.
6	Pune	Pune Municipal Corporation Website[128]	Pune Municipal Corporation	● Live 24x7 feed with live alerts automatic alerts sent to the police for “crowd gathering, suspicious objects, suspicious loitering, automatic number plate recognition”

Case Law

Modern Jurisprudence concerning surveillance by the state against individuals in India has been defined by three major cases:

- People’s Union for Civil Liberties (PUCL) v. Union of India, 1996
  The case centred around the issue of surveillance through illegal phone tapping of politicians by the union government.[129] Any form of surveillance undertaken on

[127] Andhra Pradesh Legislative Assembly, “The Andhra Pradesh Public Safety (Measures) Enforcement Rules 2014,” February 18, 2014, available at https://hyderabadpolice.gov.in/acts/Publicsafetyact.pdf.
Andhra Pradesh Legislative Assembly, “Andhra Pradesh Public Safety (Measures) Enforcement Act-2013,” July 6, 2013, https://hyderabadpolice.gov.in/acts/Publicsafetyact.pdf.

[128] Pune Municipal Corporation, “Closed Circuit Television System (CCTV),” accessed March 3, 2020, available at https://www.pmc.gov.in/en/closed-circuit-television-system-cctv.

[129] People’s Union for Civil Liberties v. Union of India, (1997) 1 SCC 301

telephone conversations must be done as per the appropriate legislation[130] and in a manner that is just, fair and reasonable.[131] In order to meet these standards, the court put forth a test consisting of pre-conditions in order for the executive's use of surveillance to be considered lawful. Of these preconditions , the most important included:[132]

- ➢ Orders for telephone tapping could only be provided by the Home Secretary of the union government or of a state government. However, in an emergency this power can be delegated to any officer of the Home Department of the union or the state. At no point is there a need for any judicial authorization (warrant).
- ➢ The authority must consider whether the information can reasonably be acquired by other means.

- Justice K.S. Puttaswamy (retired) v. Union of India, 2017

  As mentioned earlier, this landmark case explicitly established the constitutionality of the right to privacy as an inherent element of part III of the Indian constitution.[133] It expanded on the rationale of PUCL, and provided a more detailed explanation of the standards to be met by the state in order to carry out any surveillance activity that might be antithetical to the right to privacy including i) reasonableness[134], ii) the existence of legislation prescribing the surveillance[135], iii) existence of compelling state interest[136] and iv) proportionality and legitimacy.[137]

- Vinit Kumar v. Central Bureau of Investigation, 2019

  The Bombay High Court in this case held that any order relating to the interception of information as per article 5(2) of the Indian Telegraph act can only be issued in two instances – public emergency or public safety.[138] The Supreme Court of India had previously clarified the definitions of these phrases in the PUCL case, saying: "Public emergency would mean the prevailing of a sudden condition or state of affairs affecting the people at large calling for immediate action. The expression 'public safety' means the state or condition of freedom from danger or risk for the people at large."[139]

[130] Ibid, ¶30 (In this case as per Indian Telegraph Act, 1885, §5(2))
[131] Ibid, ¶30
[132] Ibid, ¶35

[133] K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC, ¶84
[134] Ibid, ¶310, 88
[135] Ibid, ¶87
[136] Ibid, ¶378
[137] Cyril Amarchand Mangaldas, "Right To Privacy: Surveillance In The Post-Puttaswamy Era," *BloombergQuint* (blog), December 11, 2019, available at https://www.bloombergquint.com/law-and-policy/right-to-privacy-surveillance-in-the-post-puttaswamy-era.
[138] Vinit Kumar v. Central Bureau of Intelligence, (2019), ALLMR (CRI), 5227
[139] Soumya Tiwari, "Bombay HC Finds Home Ministry's Interception Orders Illegal, Says Procedural Safeguards Mandatory," MediaNama (blog), October 30, 2019, available at https://www.medianama.com/2019/10/223-bombay-hc-interception/.

Government Initiatives

In addition to the above laws, the government of India has also undertaken a number of projects to facilitate state surveillance. For example, the government has been implementing the National Intelligence Grid (NATGRID)[140] - a project to create a comprehensive and searchable database - and the Centralized Monitoring System (CMS)[141] - a project to enable intelligence agencies to directly intercept communications on a service provider network without assistance from the provider. This, along with other similar projects such as the Lawful Intercept and Monitoring project (LIM)[142], Crime and Criminal Tracking Network & Systems (CCTNS)[143], Network Traffic Analysis System (NETRA)[144], have been criticized for facilitating mass surveillance, being opaque, and implemented without clear legal backing or oversight mechanisms.[145]

Limitations of the Existing Framework

Though aspects of the surveillance regime in India do contain safeguards[146] - such as an oversight committee for interception orders and clear grounds on which interception can take place - it has been criticized for lacking judicial authorization, placing heavy handed penalties on service providers for non-compliance, prohibiting transparency of interception orders, lacking key safeguards such as notice to the individual, and for being a set of patchwork provisions that establish varying grounds and conditions for surveillance that leave existing and emerging practices such as the use of CCTVs and the use of facial recognition technology unregulated.

It is worth noting that though the right to privacy has been guaranteed as a fundamental right, the jurisprudence regarding what this right encompasses is still at a relatively nascent stage. Courts in India are yet to recognise the effect of surveillance spread over a period of time

[140] Vijaita Singh, "NATGRID to Have Access to Database That Links around 14,000 Police Stations," *The Hindu*, July 12, 2020, available at https://www.thehindu.com/news/national/natgrid-to-have-access-to-database-that-links-around-14000-police-stations/article32058643.ece.

"Expression of Interest (EoI) for Selection of HR Recruitment Agency for Consultancy Services Required for Hiring of Technical (Contractual) Manpower in NATGRID" (Ministry of Home Affairs, Govt. of India, August 13, 2019), available at https://www.mha.gov.in/sites/default/files/EOI.pdf.

[141] Maria Xynou, "India's Central Monitoring System (CMS): Something to Worry About?," *The Centre for Internet and Society* (blog), January 30, 2014, available at https://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about.
Government order: https://dot.gov.in/sites/default/files/DOC231013.pdf?download=1

[142] Maria Xynou and Elonnai Hickok, "Security, Surveillance and Data Sharing Schemes and Bodies in India" (The Centre for Internet and Society, n.d.), available at https://cis-india.org/internet-governance/blog/security-surveillance-and-data-sharing.pdf.

[143] Ibid

[144] Ibid

[145] Udbhav Tiwari, "The Design & Technology behind India's Surveillance Programmes," *The Centre for Internet and Society* (blog), January 20, 2017, available at https://cis-india.org/internet-governance/blog/the-design-technology-behind-india2019s-surveillance-programmes.

[146] Elonnai Hickok, "Policy Brief: Oversight Mechanisms for Surveillance — The Centre for Internet and Society," November 24, 2015, available at https://cis-india.org/internet-governance/blog/policy-brief-oversight-mechanisms-for-surveillance.

from different points of observation is an invasion on the right to privacy of an individual. Known as the 'mosaic theory of privacy'[147], the United States Supreme Court introduced this concept in the seminal case of *United States v Jones*. The approach is based on the recognition that comprehensive aggregation of even seemingly innocuous data reveals greater insight than consideration of each piece of information in isolation. This theory has also found acceptance in the Taiwan courts[148], but to date it has only been argued by private individuals in primarily domestic dispute cases, and not against the state in surveillance cases.

Justice Chandrachud in the privacy judgement had alluded to this theory while stating that *"Individually, these information silos may seem inconsequential. In aggregation, they disclose the nature of the personality: food habits, language, health, hobbies, sexual preferences, friendships,ways of dress and political affiliation. In aggregation, information provides a picture of the being: of things which matter and those that do not, of things to be disclosed and those best hidden"*.[149] The petitioners in the Aadhaar case[150] had also argued that the aggregation of data and the linking of the data with Aadhar should be deemed to be impermissible as it is capable of being used to affect every aspect of an individual's personal, professional, religious and social life. Unfortunately, the Court did not delve into this argument as it accepted the State's contention that under the Aadhaar Act, the data remains in silos and there is no aggregation of data.

International Perspectives

The use of FRT, and the complications that arise from its use, are not problems that are solely limited to the Indian context. A number of states around the globe are in the midst of determining how to balance the potential security benefits of the technology with the dangers to personal liberties that it presents. Given, therefore, that debates around FRT are taking place the world over, it is worth analysing its deployment, use and regulation in a multitude of states.

United Kingdom

In June 2021, the UK Information Commissioner had given her opinion on the use of live facial recognition technology in public places. She observed that "central legal principles to consider before deploying LFR are lawfulness, fairness and transparency, including a robust evaluation of necessity and proportionality. This evaluation is particularly important because

[147] Orin Kerr, "The Mosaic Theory of the Fourth Amendment," Michigan Law Review 111, no. 3 (December 1, 2012): 311–54.

[148] Tony Tung-Yang Chang, "Recent Development Of Mosaic Theory In Taiwan's Privacy Law - Privacy - Taiwan," April 20, 2020, available at https://www.mondaq.com/privacy-protection/919812/recent-development-of-mosaic-theory-in-taiwan39s-privacy-law.

[149] K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1

[150] K.S. Puttaswamy (Retd) v Union of India (2019) 1 SCC 1

LFR involves the automatic collection of biometric data, potentially on a mass scale and without individuals' choice or control"[151]

In July 2019, the UK's Information Commissioner's Office had observed that there are significant data protection and privacy issues that need to be addressed prior to the rollout of live[152] facial recognition technology.

In September 2019, the UK High Court[153] initially upheld the use of Automated Facial Recognition Technology by the South Wales Police. It held that the use of the technology was in consonance with the Human Rights Act, 1998 and the Data Protection Act, 2018. In arriving at its conclusion, the court noted that (i) there was adequate legal protection under the existing legislation as well as in the statutory code of of practice and standard operating procedures published by the South Wales Police; (ii) the AFR technology was deployed in a fair and transparent manner and was not disproportionate; (iii) the technology was not deployed in a covert manner; when AFR is was deployed, the police were required to take steps to inform members of the public about AFR and as to its place and time of deployment. In January, the UK Government's Biometric Commissioner[154] expressed his disagreement with the High Court's decision. As per the Commissioner, the High Court decision should not be seen as a "blanket authorisation to use LFR in all circumstances." The Commissioner recommended a statutory binding code of conduct to be issued by the government which should address the concerns arising out of the use of live facial recognition technology by the police, and where possible, other biometrics. The Commissioner emphasised that such a code should provide greater clarity about proportionality considerations and that the law enforcement agencies should provide the legal basis for processing in a sufficiently clear manner, prior to the commencement of processing. This ruling has since been overturned by the Court of Appeal of England and Wales in August 2020. The court found that there were "fundamental deficiencies[155]" in the legal framework relating to who can be placed on the watchlist and the criteria that determines where such technology can be deployed. By leaving these questions to the police the court determines that "too much discretion is currently left to individual police officers."[156]

[151] Information Commissioner's Office, "Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places," June 18, 2021, available at https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf.

[152] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/blog-live-facial-recognition-technology-data-protection-law-applies/

[153] R (Bridges) v Chief Constable of South Wales Police and Secretary of State for the Home Department [2019] EWHC 2341

[154] Information Commissioner's Opinion: "The use of live facial recognition technology by law enforcement in public places.", October 31, 2019, available at https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf

[155] ¶91, [2020] EWCA Civ 1058

[156] Ibid

United States of America

In February 2020, a bill titled Ethical Use of Facial Recognition Act was introduced in the United States Congress[157]. The bill proposes a moratorium on the government use of facial recognition technology until a commission recommends the appropriate guidelines and limitations for the use of such technology. This follows the action taken by certain cities in the USA such as Oakland, San Francisco, Cambridge, Berkley and Sommerville in banning the use of FRT.[158]

As per the bill, facial recognition has been shown to disproportionately impact communities of colour, women, activists and immigrants. There is evidence that the technology has been used at protests and rallies which in turn has a chilling effect on free speech. It proposes to create a Congressional Commission which would consider and create guidelines for the use of facial recognition technology by government officials. According to the bill, any government official proposing to use facial recognition technology prior to a legislation implementing the guidelines issued by the commission will require a judicial warrant to do so. In June 2020, a bill titled Facial Recognition and Biometric Technology Moratorium Act was introduced in the Senate. The bill seeks to prohibit biometric surveillance by the Federal Government without explicit statutory authorization and to withhold certain Federal public safety grants from State and local governments that engage in biometric surveillance.

Illinois has also enacted a law to regulate biometric information. Known as the Biometric Information Privacy Act[159]It regulates the collection, use and handling of biometric information. It explicitly states that the full ramification of such technology is not fully known and therefore it is necessary to regulate such technology. However, this law is only applicable to private entities. Further, several U.S. states have also banned the use of FRT.[160]

European Union

In January 2020, an initial draft of the EU white paper on AI was released which stated that the European Union was considering a five year moratorium on the use of facial recognition technology in public spaces.[161] Though, as per newspaper reports the EU had initially backed away from from imposing a blanket ban on the use of such technology and had instead put

[157] "Ethical Use of Facial Recognition Act," February 12, 2020, available at https://www.merkley.senate.gov/imo/media/doc/20.02.12%20Facial%20Recognition.pdf.

[158] Rachel Metz, "Beyond San Francisco, More Cities Are Saying No to Facial Recognition," CNN, July 17, 2019, available at https://www.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html.

[159] "Biometric Information Privacy Act" (Illinois General Assembly, October 3, 2008).

[160] "Facial Recognition Laws in the United States #ProjectPanoptic," *Internet Freedom Foundation* (blog), available at May 3, 2021, https://internetfreedom.in/facial-recognition-laws-in-the-united-states-projectpanoptic/.

[161] Foo Yun Chee, "EU Mulls Five-Year Ban on Facial Recognition Tech in Public Areas," Reuters, January 16, 2020, available at https://in.reuters.com/article/uk-eu-ai-idINKBN1ZF2QN.

"Facial Recognition: EU Considers Ban of up to Five Years," BBC News, January 17, 2020, available at sec. Technology, https://www.bbc.com/news/technology-51148501.

the onus on the member states to regulate such technology, [162] It appears that the European Commission is still considering imposing a ban on it in public spaces within the EU. [163]

There has been a varied response of the member states to the use and regulation of FRTs. In Germany, the Hamburg Data Protection Commissioner found the use of facial recognition technology by the police during the G20 summit in 2017 to be incompatible with the data protection laws. It found it to be particularly problematic as the technology was deployed in the absence of any law.[164] On the other hand, the Swedish Data Protection Authority permitted the police to use facial recognition technology to identify criminals. As per the authority, the technology is more effective at identifying perpetrators than manual identification by the police.[165]

Observations and Conclusions

The use of facial recognition technology in India by law enforcement and the state is nascent but growing. Based on publicly available information about the use of FRT in India, the following observations can be made:

- Need for a legal and regulatory framework

  Presently there are no legal or regulatory frameworks governing the use of FRT in India and existing legal frameworks for surveillance in India do not clearly extend to the use of FRT technology.

  In the Puttaswamy judgement (2017), the Supreme Court held the right to privacy to be a fundamental right, and like other fundamental rights, held it to not be an absolute right. The right is subject to reasonable restrictions and the restrictions have to comply with a three fold test; (i) legality; (ii) legitimate state aim; and (iii) proportionality.

  The existing laws and regulations were formulated for regulating targeted surveillance and not bulk surveillance. When these laws and regulations were

[162] Christine Fisher, “EU Backs Away from Proposed Five-Year Facial Recognition Ban,” Engadget (blog), accessed November 30, 2020, available at https://www.engadget.com/2020-02-11-european-commission-facial-recognition-guidelines.html.

[163] Luana Pascu, “European Commission hasn’t completely ruled out biometric facial recognition ban in public spaces”, available at https://www.biometricupdate.com/202009/european-commission-hasnt-completely-ruled-out-biometric-facial-recognition-ban-in-public-spaces, September 4, 2020

[164] “Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement” (European Union Agency for Fundamental Rights, February 25, 2019), available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf.

[165] New Europe Online, “Sweden Authorises the Use of Facial Recognition Technology by the Police,” New Europe (blog), October 28, 2019, available at https://www.neweurope.eu/article/sweden-authorises-the-use-of-facial-recognition-technology-by-the-police/.

formulated, the technology for bulk surveillance was in its nascent stage and the discourse around privacy and surveillance was not as well developed as today.[166]

The existing laws governing surveillance in India do not incorporate the necessary privacy principles of purpose limitation, collection limitation, data quality, oversight and accountability and the rights of the persons who are under surveillance. In the absence of a data protection law, it is critical that surveillance laws incorporate these principles. Deployment of FRT is a means of bulk surveillance and it is not clear that it conforms with the principle of proportionality which subsequent to the Puttaswamy judgement has become one of the standards to test restrictions on the right to privacy.

Further, as noted earlier, the Home Ministry has in response to a legal notice sent by the Internet Freedom Foundation stated that the basis of the FRT system such as the AFRS is a 2009 cabinet note, however a cabinet note is not a statutory enactment and cannot be used as a legal basis for deploying facial recognition technology. In the Aadhar judgement, the Supreme Court had struck down the use of Aadhar as a means for mandatory verification of SIM cards as there was no legislative backing for the same and held that it was a disproportionate and unreasonable state compulsion.

It is also unclear what policies and procedures are being put in place when the technology is adopted at the state and city level. This raises serious concerns with respect to oversight, accountability, redress for the use of FRT and the consistent implementation of safeguards to protect against misuse. Given past surveillance projects and practices by the State and emerging uses of FRT by law enforcement - such as at protests - there is a need for a clear regulatory framework that defines the acceptable uses of FRT, the methods involved in its use, and safeguards to protect against the use of FRT for mass surveillance. Key safeguards for policymakers to consider include:

a. **Standards of Necessity and Proportionality:** While Puttaswamy has laid down standards of necessity and proportionality that must be applicable to any exception to the right of privacy, the unique characteristics of FRT are such that these standards must be explicitly integrated into any regulatory framework. Given the ability of FRT to undertake bulk surveillance on a scale previously unseen, it is imperative that standards of necessity be strict, and that standards of proportionality take into consideration factors such as the scale and scope of a threat, human rights, etc.

b. **Oversight, accountability, and redress:** Clear mechanisms and bodies for oversight and accountability need to be established including requirements for audits and transparency reports.

c. **Data Protection Impact Assessment**: As noted earlier, under the proposed PDP Bill, 2019, a data fiduciary (either private or government) shall be classified as a significant data fiduciary, based on the sensitivity of the data processed or the use of any new technology for processing of personal data. If a significant data fiduciary intends to use biometric or genetic data, then

[166] Rishabh Bailey, Vrinda Bhandar et al "Use of personal data by intelligence and law enforcement agencies", August 1, 2018, available at https://www.datagovernance.org/files/research/BBPR2018-Use-of-personal-data.pdf

no such processing shall commence until it has undertaken a data protection impact assessment. Such an assessment shall specify the measures to be adopted for managing and mitigating the risk of harm that could be caused to the data principal. The Data Protection Authority has also been empowered to specify the circumstances wherein such a data protection impact assessment shall be mandatory[167]. As the PDP Bill is finalized, data protection impact assessments should remain in the framework envisioned.

d. **Human Rights Impact Assessments**: As recommended by the Freedom Online Coalition, prior to procuring and deploying FRT systems, the government should undertake a human rights impact assessment to understand and mitigate potential harm to an individual's human rights.[168]

e. **Consent structures**: Meaningful structures for consent that take into consideration passive data collection need to be defined for the use of FRT in criminal and non-criminal cases.

f. **Notice structures:** Meaningful notice needs to be provided regarding the use of FRT. The content of such notices should provide information to users to understand if and when FRT is being used, how the technology works, how their data will be stored, and what rights they have.

g. **Purpose limitation:** To protect against function creep, limitations on what purposes FRT databases can be used for are important. This is particularly true if it is a criminal database. Similarly, limitations on how data stored in an FRT database can be used and shared need to be defined. Limitations on what databases can be interoperable with FRT databases also need to be defined.

h. **Retention and deletion standards:** Clearly defined and granular retention and deletion standards with respect to different scenarios need to be defined. For example, no match vs match - criminal vs. non criminal etc. The circumstances on which individuals will have the ability to request the deletion of their data should be defined.

i. **Opt-n out standards:** Except in specified and clearly defined instances, individuals should have the ability to opt out of the use of processes dependent on FRT.

j. **Access standards**: Individuals should have the ability to request access to information that is stored about them in a FRT related database including access to records of comparisons, how they have been categorised in the database, and what information is stored in association with their name.

k. **Evidentiary status and weight:** The evidentiary status and weight of decisions made via FRT needs to be clarified.

l. **Transparency in permitted action/use resulting from a match:** Transparency and established procedure is needed about the permitted action/use followed after a match has been confirmed as per the statistical significance of the match.

[167] Clause 27(2)

[168] https://freedomonlinecoalition.com/wp-content/uploads/2020/11/FOC-Joint-Statement-on-ArtificiaI-Intelligence-and-Human-Rights.pdf

m. **Statistical Standards for confirming a match:** The accepted standards for statistical probability for confirming a match need to be defined and harmonized across the use of FRT in India.

- Potential applicability of the PDP Bill
  If enacted, the PDP Bill would have implications for the use of FRT by law enforcement in India by requiring processing of facial images to be permitted by law as per clause 92 of the Bill. The applicability of this provision will depend on if the Central Government notifies facial images as a type of biometric data protected under clause 92 and whether or not the Central Government exempts law enforcement from section 92 or other provisions of the Act via clause 35.

- Need for comprehensive and harmonized regulation of CCTVs
  The fact that systems like the AFRS will draw heavily on images from public and private CCTVs is concerning as CCTVs are governed differently, if at all, across cities in India. This points to the need for clear regulation of CCTVs by public and private actors before a system like the AFRS is implemented.

- Need for clarity in scope, structure, and process of FRT systems There is little publicly available information about the actual scope, structure, and processes followed for FRT systems in use in India. Key areas that need to be addressed include:
  a. **Basis and process for creation of databases for FRT:** Clarity is needed with respect to the way in which databases for FRT are being created. This includes information about the baseline data that will comprise the database, on what basis information will be added to the database, and what information will be added to the database.
  b. **Organization and categories in a database**: Clarity is needed on what categories and partitions will exist in a database. For example, the RFP for the AFRS indicates that the database should have logical partitioning for criminals, unidentified dead bodies, missing persons, found persons, foreigners arrested etc. It will be important for the categories that will comprise to be clearly defined as it will inform what categories of images can be uploaded and stored on the database.
  c. **Scope of databases:** The scope and objective of databases created for FRT need to be clearly defined including if the database will be integrated or interoperable with other databases and if databases be limited to specific purposes such as criminal purposes, state welfare purposes etc.
  d. **Process and grounds for using FRT:** Further clarification is needed as to the grounds and process for using FRT. Specifically, on what grounds can FRT be used, what authorization process will be followed, and what process safeguards are in place to protect against misuse.
  e. **Process for comparison:** The process for comparison against different categories in a database will be important to further clarify ie. can law enforcement search a photo against the entire database each time or will

images of potentially missing persons only be run against the ‘missing persons’ partition.

f. **Technical Feasibility and Accuracy:** The standards to ensure technical feasibility and accuracy need to be clearly identified. For example, the technical feasibility of some of the requirements found in existing proposals such as the RFP for the AFRS need to be fully assessed - for example requirements for capabilities of the database include “add photographs obtained from newspapers, raids, sent by people, sketches to the criminal’s repository tagged for sex, age, tattoos etc.”[169]

g. **Role of algorithms**: Given the significant impact that decisions informed by FRT can have on the individual - it is important that when and how algorithms are used is clarified and that these have been audited for accuracy. For example, the RFP for the AFRS refers to the integration of algorithms in the system without specifying what functions would be automated or shaped by an algorithmic decision - stating: “The system shall offer logical algorithms and user-friendly, simple graphical user interface making it easy to perform the facial matching”.[170]

- Need for capacity building in end users

  From publicly available information, it is unclear what capacity building measures are in place for the use of FRT technology by law enforcement. It is not clear if law enforcement are mandated to undergo comprehensive training or receive certification prior to using the technology. To ensure that end users of the technology are fully trained in both the technical and ethical dimensions of FRT it is imperative that comprehensive training is provided to end users.

- Need for public discourse

  As systems like that being developed in Uttar Pradesh[171] indicate that use of FRT systems connected to criminal databases are not limited to law enforcement but also open to the public, there is a need for robust public discourse on the implications and appropriate use of FRT by different actors including: law enforcement, public sector entities, private entities, and the public. Such public discourse must focus on firstly, clearly articulating to the public the scope and dangers involved with implementing FRT. While this report may serve as a starting point, research organisations, public policy bodies and think tanks must take the onus to educate the public on the matter. On the government’s side, any regulatory framework that is proposed must be subject to input from the public as has been the case with other proposed regulatory frameworks for digital technology. Furthermore, given the potential the technology has with respect to targeting minorities, it is especially imperative that feedback and suggestions are sought from underrepresented communities.

[169] Pg. 3 http://ncrb.gov.in/TENDERS/AFRS/RFP_NAFRS.pdf

[170] Pg. 3 http://ncrb.gov.in/TENDERS/AFRS/RFP_NAFRS.pdf

[171] Ankit Gupta and Gaurav Gaur, “FICCI Smart Policing Awards 2018: Compendium of Best Practices in Smart Policing” (FICCI, 2018), available at http://ficci.in/spdocument/22984/FICCI-Compendium-of-Best-Practices-in-SMARt-Policing-2018.pdf.

- Need for research into impact

  There is a need for research into the impact of FRT in India and the potential harms that can emerge. Specific areas that require further research include:

  a. **Bias and Discrimination**: Concerns of bias, and discrimination via the use of FRT are acute in India. Factors which could influence the efficacy, accuracy and potential biases of FRT in India include skin colour, geography, religion, caste, etc. This could lead to new forms of discrimination or reinforce existing forms. There is thus a need to research to what extent bias and discrimination is present in the use of FRT by the Indian state, how such bias can be minimized and ultimately removed, and what safeguards are needed to enable individuals to effectivleyeffectively protect themselves from being discriminated against
  b. **Accuracy:** Requirements for inclusion of images like 'sketches' in tenders also raises concerns about the accuracy of data that might be in databases collated for the use of FRT. There must be significant resources dedicated to researching the accuracy of the data that is being used to undertake facial recognition, and whether such systems and sources of data can be considered reliable in the Indian context.
  c. **Impact on rights:** The misuse of FRT could result in harm against fundamental rights including privacy, freedom of expression, and the right to assembly. Having already seen the use of FRT in the case of public protests, further research into how FRT can be implemented within the legal and constitutional framework without inhibiting these rights, is essential.
  d. **Impact of use on social behaviour and norms:** The presence and pervasive use of FRT in public spaces has the potential of shifting understandings of acceptable behaviour in public and can also be used to push subjects towards specific forms of behaviour. More research is needed into how FRT is being used and the direct and indirect impact it has on social norms and behaviour.