TAKSHASHILA INSTITUTION

AI-Based FRT in Policing

Madhukumar S, Parthasarathy S R

Takshashila Discussion Document 2025-25
Version 1.0, October 2025

This policy brief was produced by the authors as part of the Law Enforcement and Policing Fellowship 2024--2025. It is an outcome of the second hackathon conducted under the fellowship, which focused on Artificial Intelligence in Policing.

Recommended Citation:
Madhukumar S, Parthasarathy S R, ``AI-Based FRT in Policing'', Takshashila Discussion Document 2025-25, Version 1.0, October 2025, The Takshashila Institution

©The Takshashila Institution, 2025

Contents

1 Executive Summary

Madhukumar is a Control Systems Engineer with four years of experience in the locomotive domain. His areas of interest include electric vehicles, space exploration, geopolitics, and public policy. He was part of Takshashila's GCPP Tech & Policy cohort 39.

Parthasarathy is a policy enthusiast with experience across information technology, microfinance, and renewable energy. He completed Takshashila's GCPP course in the 40th cohort and currently works with a renewable energy social enterprise, leading grassroots projects in rural communities and collaborating with diverse stakeholders.

AI-based Facial Recognition Technology (FRT) is being increasingly used in law enforcement worldwide. The technology behind it has been significantly improved in terms of speed and accuracy of prediction, as a result of increased research by academia and industry.[1] New AI models, such as Yolov10, have emerged in the past decade, with results meeting expectations of law enforcement agencies around the world. However, concerns regarding privacy, accountability, transparency, racial discrimination in prediction, biased training/test data, and false positives have increased as well.[2] In order to harness the technology for the betterment of society and improve the efficiency of law enforcement, it is vital that there be government intervention to regulate and moderate the development and usage of AI-based facial recognition systems.

This policy brief discusses two areas wherein the Government may play the role of an umpire to achieve the below goals:

1. Building public confidence about the use of FRT to enhance public safety and making law enforcement timely by reducing the information asymmetry between the law enforcement agencies (LEAs), technology providers, and the public regarding how FRT is used, the data it processes, its accuracy, and its implications; and
2. Creating favourable and competitive market conditions and ensure participation from diverse market players.

The first policy area suggests building upon the existing regulations for CCTV and surveillance equipment in the country and developing broader regulatory standards for facial recognition systems using AI for deployment by law enforcement. It recommends establishing clear equipment standards for Original Equipment Manufacturers (OEMs) and examines potential unintended consequences of such standardisation,offering strategies to mitigate them.

The second policy area looks at the regulations covering AI-based FRT in the European Union, and proposes setting up a similar central regulatory agency as the EU, in India, which will regulate AI models, as well as training and testing data sets to be used in FRT. The aim of the regulatory agency would be to ensure the development of safe, high-quality technology built on diverse and representative data that reflects India's demographic diversity, thereby reducing bias and supporting the overall objectives of law enforcement.

Both the policy ideas aim to create favorable market conditions in the country, so that there is participation by several private entities to develop standard and safe FRT equipment, and AI models trained on large, high-quality, and relevant datasets. These policies also seek to ensure compliance with ethical, privacy and safety standards to build public trust and support law

enforcement agencies to use FRT effectively and responsibly for public safety.

2 Introduction

Use of artificial intelligence based facial recognition technology (FRT) for the purposes of general law enforcement and public safety is set to be one of the most widely used applications of AI. Recent cases suggest that law enforcement agencies around the world have used facial recognition technology to identify rioters, spot potential disruptors at public events, access control applications at airports and track down criminals based on prior records, among other things. Studies have found that smart technologies such as AI enabled FRT could help cities reduce crime by 30-40 per cent and reduce response times for emergency services by 20-35 per cent.[3]

However, the use of such technologies can raise public concerns about the sharing and misuse of personal data, potential violations of individual rights, unlawful surveillance, and the risk of false identification. If these issues are not adequately addressed, they may lead to serious consequences and erode public trust, ultimately undermining the potential benefits of the technology.

The graphic below provides details of the extent of usage and regulation of the AI based facial recognition and surveillance in policing across various countries.

Usage and Regulation of the AI based Facial Recognition and Surveillance in Various Countries

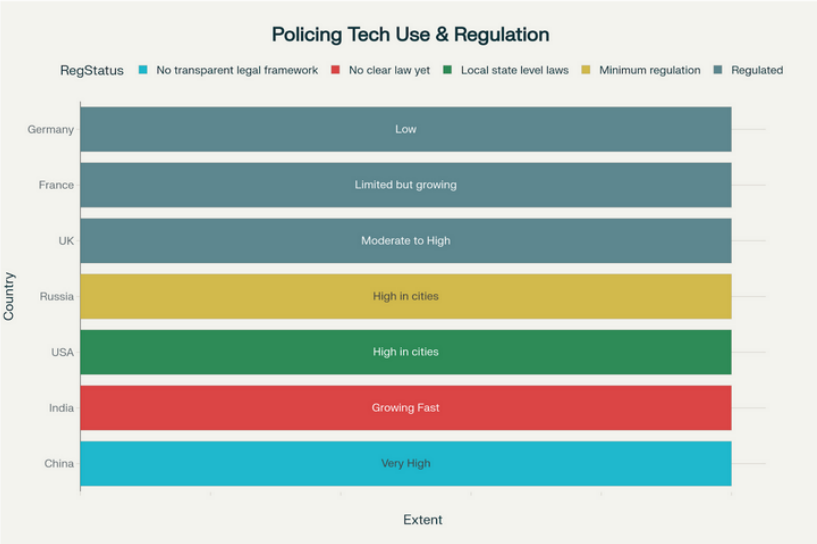

Figure 1: Image generated by the authors using GenAI

The State and its various arms, having both the power to coerce

citizens (to provide personal data) and also the responsibility to keep them safe, must play a significant role in enabling the adoption of the AI-based technologies in law enforcement. It becomes imperative for the state to ensure that data collected for specific purpose of policing is also transparent so that the scope of unchecked surveillance at the level of an individual is reduced.

The behaviour of the Government in this regard can either ensure the creation of a suitable ecosystem or can create an environment of fear.

Thus, a strategy to implement the technology with the backing of suitable transparent regulations becomes necessary. The aim of the strategy should be to ensure the active participation of the society and the markets for the successful adoption of the technology.

3 AI Based Facial Recognition Technology in Operational Policing

AI Based FRT has various use cases in operational policing, which are being employed by police departments across the world and have seen increased efficiency in resource allocation, reduced investigation time, increased detention of the accused, and increased prevention of crime.

The following are a few popular use cases:

1. Wanted Criminal Identification in Public Spaces An AI model is trained with the national criminal data base to detect a wanted criminal. The CCTV videos from various public installations are fed to the AI model in real time, which detects human faces, extracts features, and predicts whether the person is a wanted criminal or not.[4] When a person of interest is recognized by an AI model, it warns the police personnel to take action.

CNN Based Facial Feature Extractor and Image Classifier Training

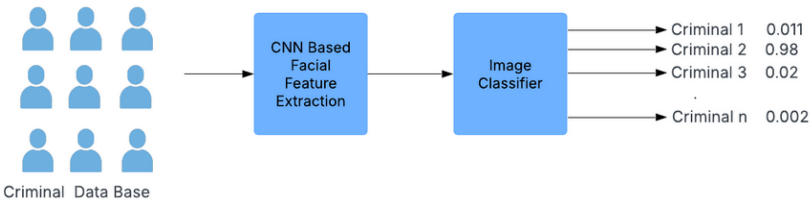

Figure 2: Authors'Visualisation

AI Based FRT Steps in Criminal Identification Application

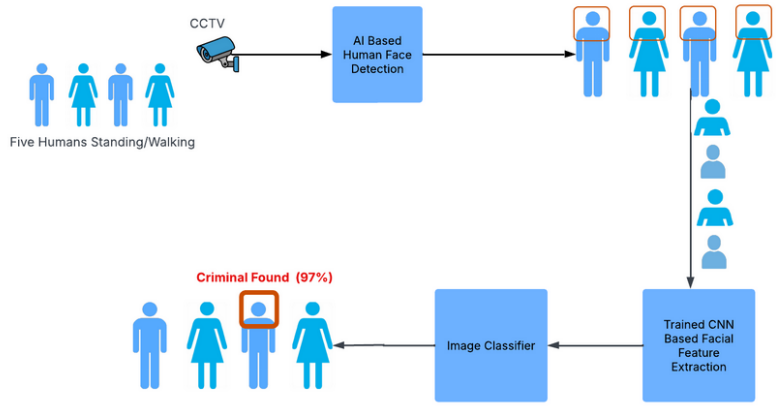

Figure 3. Authors' Visualisation

2. Suspect Identification or a Missing Person Identification in Public Spaces. Here, the CCTV videos are fed to an AI model, which is trained to detect the human faces. Further the faces of humans in the video and the face of the suspect or a missing person are fed to the AI model that has been trained to extract facial features, The widely used technology here is a Convolutional Neural Network (CNN).[5] The facial features of a target person are compared against the others to match the identity with a certain degree of confidence.

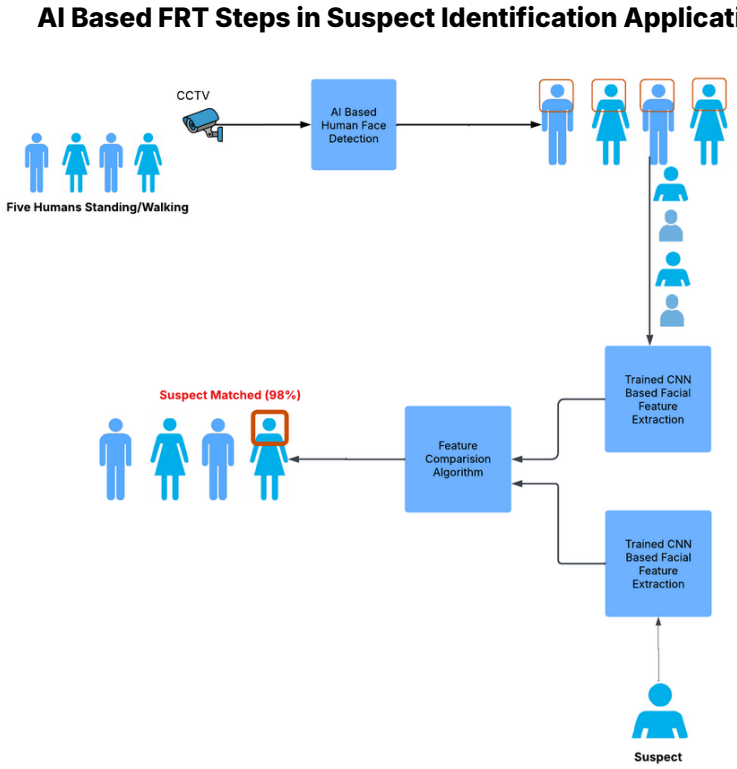

Figure 4. Authors' Visualisation

4 Current Issues in the Usage of FRT System in Operational Policing

1. FRT System Accuracy.
2. FRT System Black Box.
3. FRT System Safety
4. Lack of A Localised FRT System.

4.1 FRT System Accuracy

FRT system accuracy depends on various factors, broadly looked from two angles – Hardware and Software.

Hardware: The CCTV camera feeds are the major source of data input for the FRT system used for policing applications. The image quality plays a major role in the accuracy of prediction by the FRT system. Currently, there is no standard with respect to CCTV camera image resolution, which leads to increased inaccuracies in the predictions.

Software: The AI model used in the FRT system, and the data that the model has been trained on, largely influences the accuracy of predictions. Currently, there are no standards or regulations around the type of AI model to be used, and the data to be used for training and testing the model.

4.2 FRT System Black Box

Law enforcement agencies and private companies often possess substantially more technical, operational, and proprietary information than the general public subject to surveillance. This includes knowledge of algorithmic accuracy, system limitations, data sources, and access to specialised databases. Explanations and disclosures about how facial data is collected, processed, stored, and deployed are often insufficient, limiting oversight and accountability. As a result, errors arising from biased or inaccurate data inputs remain difficult for affected individuals to detect or challenge. This can lead to misidentification, surveillance overreach, and erosion of civil rights. This asymmetry further undermines public scrutiny and weakens institutional checks, while also diminishing public trust in the technology's use for law enforcement purposes.

4.3 FRT System Safety

This has to be again looked at from two angles broadly- Hardware and Software.

Hardware: There are mainly two types of CCTV cameras available in the market. They are: a) Smart camera that gets connected to the internet and stores data on the cloud, and b) A camera that doesn't get connected to the internet and stores the data on an offline database. Both the types are prone to be hacked. As a consequence,video feed can be modified electronically, and used for unintended purposes.

Software: The firmware of the CCTV cameras can be tampered and can be modified to make the camera non-functional or hacked to divert the video feed.

4.4 Lack of Localised FRT System

Today, most of the CCTV cameras are not AI-enabled. The images from CCTV cameras all around the city need to be either collected manually by individual law enforcement agencies, or accessed via cloud and run facial recognition algorithms over the data, which is a time and resource-intensive task. If the CCTV cameras are AI enabled, facial recognition can be carried out on local data and the law enforcement agencies can access the prediction results via secured online channels.

This policy brief discusses two such policy ideas which need to be taken up by the Government to build trusted relationships between law enforcement and the communities, leading to the introduction of artificial intelligence in facial recognition and surveillance technology to transform how police services and citizens collaborate to improve public safety.

5 Policy Ideas

5.1 Policy Idea 1: Govt. mandating video capturing device OEMs to have standardised specifications and protocols to allow for two-way interface

Ministry of Electronics and Information Technology (MeitY) has recently amended the Public Procurement (Preference to Make in India) Order, 2017 and the "Electronics and Information Technology Goods (Requirement of Compulsory Registration) Order, 2021 for closed-circuit television (CCTV) cameras manufactured, imported or sold in India to standardise their quality and system security.[6] As per these amendments, all CCTV systems mandatorily require Standardisation Testing and Quality Certification (STQC) from Government-authorised bodies. The STQC tests focus on critical security parameters such as physical tamper resistance, role-based access controls for firmware updates, encrypted data transmission, strong software safeguards, and resilience against penetration attacks. The notification also mandates preference for locally manufactured CCTV and outlines a framework for calculating domestic content. The reasons for the STQC guidelines revolve around national security concerns, prevention of sub-standard cameras whose performance are questionable, and the need to support local CCTV and surveillance equipment manufacturers.

FRT is different from the usual surveillance done using CCTVs and other surveillance devices. FRT mainly uses AI for carrying out two activities: identification and verification.[7] Identification is done on a one-to-many match basis, and verification is done on a one-to-one match. The use of AI in this technology makes it a handy tool for law enforcement, but also gives rise to other challenges emanating from a lack of transparency, privacy infringement and false positives, among others. To ensure the safe, ethical, and locally-anchored deployment of facial recognition and surveillance technologies in law enforcement, it is imperative for the Government to formulate comprehensive technical standards for original equipment manufacturers (OEMs).

The current regulations by MeitY for CCTV and surveillance equipment can act as a foundation upon which broader regulatory standards for facial recognition systems using AI can be developed and enforced. The regulations for AI based FRT should also focus on defining standard AI models, inbuilt AI computing power, API based access and local storage whose access can only be controlled through the permission of the local owners.

The current STQC requirement mandates have led to an unintended consequence in the surveillance equipment manufacturing market. The push for mandatory certification and essential requirement (ER) guidelines has caused concerns among

several local MSMEs as they have found it challenging to get these certifications and meet these requirements. This has also led to a market that is increasingly concentrated. Similar unintended consequences can be expected when standardised specifications are rolled out for FRT-based equipment. MeitY should take the lead in addressing these consequences by supporting the medium and small manufacturers through mechanisms such as subsidised access to testing labs, phased implementation of mandatory STQC requirements, and providing technical handholding.

Defining standard specifications that include user-controlled access to stored data, mandatory STQC certification, and ensuring favourable market conditions for broad industry participation, can significantly boost public trust in surveillance technologies. This, in turn, would facilitate wider adoption of such systems and enhance the effectiveness of law enforcement.

5.2 Policy Idea 2: Govt. to regulate creation of training data, AI models, testing data, evaluation and implementation of AI based facial recognition models

India currently doesn't have a comprehensive AI act/law that governs the development of AI models, which includes training data to be used to train AI models, the type of AI models to be employed, who develops the AI model i.e Public sector undertaking, private MNC, or private-Indian firm, testing data set to be used to evaluate the performance of the AI models, evaluation criterions to determine the fit to use for law enforcement application.

The European Union is at the forefront in regulating AI with the world's first comprehensive AI Act –'The European AI Act of 2024'.[8] Adopted by the European Parliament, the Act aims to regulate AI systems based on the level of risk they pose.

Article 10(1)(2)(3) of EU AI Act mandates that AI model shall be developed on the basis of training, validation, and testing data sets that meet certain quality criteria such as;

1. Training, Validation, and Testing data sets shall be relevant, sufficiently, representative, and to the best extent possible, free of errors.[9]
2. Data sets shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, contextual, behavioral or functional setting within which the high-risk AI system is intended to be used.[10]
3. AI system provider must detect the biases in the AI model and correct it, for which, the providers of AI systems may exceptionally process special categories of personal data, subject to appropriate safeguards.[11]

The government of India should establish an independent,

statutory AI regulatory body under the Ministry of Home Affairs to set standards for training ,validation, and test dataset, and critical to quality (CTQ) criteria to be met by the AI system provider for the law enforcement Policing application.

5.2.1 Mandate of the AI Regulatory Body

The AI regulatory body shall be responsible to enforce the rules regarding Data governance, AI model certification, AI based FRT usage guidelines, Performance review, and Transparency.

Data Governance

1. The training, validation, and test data used in the development of AI based FRT systems shall be checked for diversity, unbiasedness, and privacy.
2. Maintain and update the repository of the training, validation, and test data set.
3. The third party AI based FRT system provider should use the training, validation, and test data approved by the AI regulatory body.

Training Dataset

For an AI-based facial recognition system to detect a target person among many people in public spaces, it must be trained with a labelled image dataset. AI models extract features from training images and learn from them. The performance of an AI model depends on various factors, one of which is the training dataset. The training data should not be skewed, in terms of ethnicity, skin tone, gender, age, and cultural attire (Beards, Turbans, Cap, Hijabs etc) of a person. For example, if a criminal database used to train the AI model has more males of a certain skin tone and with a beard, the AI models would incorrectly match an image of an innocent male with a beard and similar skin tone to a criminal in the database with high probability.

The technical team of the AI regulatory body shall study the biases in the training data base and reduce them by balancing the training images for demography, age, gender, cultural attire etc.

Validation Dataset

Images in the validation dataset are used during the AI model training process. A neural network-based image classifier is trained in multiple passes of the entire training image dataset to the neural network. In each pass, called an epoch in AI/ML parlance, of the training dataset, the neural network learns to extract features and classify the same. After each epoch, validation images are passed through a neural network to monitor the model performance and help in tuning hyperparameters and prevent overfitting. A validation dataset which is not truly representative of the real-world scenarios, like CCTV footage with different lighting, camera angles, occlusions etc. would lead to underperformance of the model.

The technical team of the AI regulatory body shall create a validation data set that is truly representative of real-world CCTV footage.

Test Dataset

Test dataset is a completely unseen data by the AI model, which is used to evaluate the final model performance to estimate real-world accuracy after the model training is done. The test data should consist of images that represent the real world CCTV footage, including blurry images, different lighting conditions, various angles, and images from different weather conditions i.e Sunny, Dark, Raining, Dusty etc.

In a policing application, it is also important to have images of real people or artificially generated images in the test dataset who look similar to a person in the criminal database. This helps evaluate the AI model's false positive rate.

The technical team of the AI regulatory body shall create a test data set that is truly representative of real-world CCTV footage.

5.2.2 AI Model Certification

The AI regulatory body shall define minimum performance requirements for the usage of AI based FRT model in operational policing application, and certify the same. The AI based FRT system performance is measured on several parameters, which are as follows:

Accuracy: The percentage of predictions that are correct, both in terms of matches and non-matches of a target person. Precision: The correct prediction of a target match among all predicted target matches.

Recall: Ratio of number of accurately predicted target person match to total number target person in the test dataset.

F1 Score: Harmonic mean of precision and recall.

False Positive Rate: Percentage of innocents wrongly predicted as a target person.

False Negative Rate: Percentage of target people that the system failed to predict as a match.

The third-party AI-based FRT system developer shall meet the performance criteria defined by the regulatory board to get their AI model certified for the application of policing. The certified FRT system shall be allowed for the police departments at local, state and national level to buy and install.

5.2.3 AI Based FRT Usage Guidelines

The AI regulatory body shall develop Standard Operating Procedures (SOPs) for AI tool usage in operational policing, which should clearly state the requirement for human verification

of AI-predicted results before actions are being taken by the police.

5.2.4 Performance Review

The AI regulatory body shall periodically evaluate the usage and performance of deployed AI-based FRT systems by the police authorities and subject the FRT system to re-certification every 2-3 years.

To ensure the AI models are up to date with the latest technology and training data, the performance criteria shall be revised, and the already deployed AI based FRT system shall be subjected to an upgrade.

5.2.5 Transparency

The police departments at local, state and national levels, that are using AI based FRT system, shall publish a yearly report that reveals the type of AI model being employed, developer of the AI model, training, validation, and test data used, performance of the AI model over an year and usage of the technology in solving various cases with detailed case studies emphasizing the involvement of human in the decision making process. This would increase public trust in using AI-based FRT in the policing application.

6 Conclusion

AI-based facial recognition systems are cornerstone technologies that have the potential to help the police to significantly improve the investigation process, efficiently allocate resources, detain accused, and prevent crimes from occurring. The technology has been developing at a fast rate, and there is increased adoption with minimum guardrails. It is imperative to regulate the nuances of the AI-based FRT application in operational policing.

The two policy practices suggested address the concerns and risks posed by the usage of AI-based FRT on the video feeds from public and private CCTV installations. Implementation of the first policy approach, which pertains to standardising the hardwares and softwares for AI-based FRT, increases public trust in terms of installation of CCTV cameras and accuracy of AI-based predictions, by setting standards for CCTV hardware quality, cybersecurity resilience, and AI integration, as CCTVs are the main source of video feed for policing purposes.

The second policy suggestion pertaining to the establishment of an independent and statutory AI regulatory body, helps set the standards to be followed on development of AI based FRT system, certification for policing application, usage by the police departments, auditing and compliance.

Endnotes

1. Simmler, Monika, and Giulia Canova. 2025. "Facial Recognition Technology in Law Enforcement: Regulating Data Analysis of Another Kind." Computer Law & Security Review 56 (April):106092.

2. "Approach Document for India Part 1 -Principles for Responsible AI FEBRUARY 2021 RESPONSIBLE AI AIFORALL." n.d

3. Teale, Chris. "Report: Smart City Technology Could Dramatically Improve Quality-of-life Indicators." Smart Cities Dive, June 12,2018.

4. Reddy, P. Vinay, Srinija Sanku, Trivedula Akhilsai, and Advala Gayatri. 2025. "CNN Based Criminal Face Identification System Using Video Surveillance." SSRN Electronic Journal.

5. Rani, Ruchi, Kiran Napte, Sumit Kumar, Sanjeev Kumar Pippal, and Megha Dalsaniya. 2025. "Face Recognition System for Criminal Identification in CCTV Footage Using Keras and OpenCV ." Ingénierie Des Systèmes D Information 30-3.

6. Ministry of Home Affairs, Office Memorandum, Government of India,2024.

7. Registration Department. Guidelines for Implementation of 'Essential Requirement(S) for Security of CCTV, September 22, 2024.

8. "Article 10: Data and Data Governance EU Artificial Intelligence Act." n.d.

9. "Article 10: Data and Data Governance, EU Artificial Intelligence Act."n.d.

10. "Article 10: Data and Data Governance, EU Artificial Intelligence Act." n.d.

11. "Article 10: Data and Data Governance EU Artificial Intelligence Act." n.d.

The Takshashila Institution is an independent centre for research and education in public policy. It is a non-partisan, non-profit organisation that advocates the values of freedom, openness, tolerance, pluralism, and responsible citizenship. It seeks to transform India through better public policies, bridging the governance gap by developing better public servants, civil society leaders, professionals, and informed citizens.

Takshashila creates change by connecting good people, to good ideas and good networks. It produces independent policy research in a number of areas of governance, it grooms civic leaders through its online education programmes and engages in public discourse through its publications and digital media.

©The Takshashila Institution, 2025