DRISHTI–NAYAN POLICY DRAFT: REGULATING FACIAL RECOGNITION TECHNOLOGY (FRT) IN INDIAN POLICING

1.Executive Summary

Facial Recognition Technology (FRT) is rapidly transforming law enforcement globally. By using AI to identify individuals based on facial features, FRT supports crime detection, prevention, and public safety enhancement.

However, in India, its fast deployment without adequate regulation raises critical concerns — privacy invasion, bias, misuse, lack of redressal, and surveillance overreach.

Hence, we propose a unified policy framework combining **DRISHTI (Draft Regulation for the Identification and Surveillance through Human-Targeted Imaging) and NAYAN (National Accountability for Your Automated Nagrik-Identification Network)**. This aims to govern FRT ethically, legally, and transparently in policing.

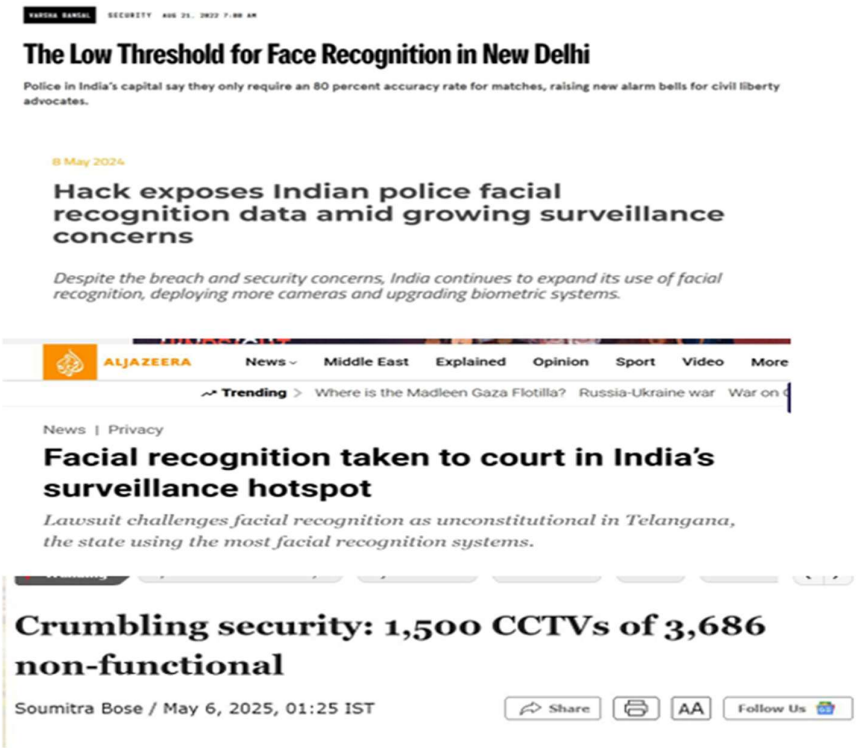
2.Introduction

2.1. Background

FRT leverages AI to identify or verify individuals from images or video feeds. Its adoption by police forces worldwide has accelerated, including in India, where several state agencies have piloted or deployed FRT for crime control and surveillance. The absence of a dedicated regulatory framework, however, has led to public concern over privacy violations, wrongful arrests due to misidentification, and the chilling effect on civil liberties.

2.2. Key Challenges

- **Privacy Erosion**: FRT enables mass, often covert, surveillance, threatening the right to privacy.
- **Algorithmic Bias**: Studies show FRT systems are less accurate for women, darker-skinned individuals, and minority groups, risking discriminatory outcomes.
- **Lack of Accountability**: Without clear rules, FRT can be misused, and wrongful identification may go unaddressed.
- **Civil Liberties**: Routine FRT use in public spaces can suppress free expression and assembly, undermining democracy.



SECURITY

The Low Threshold for Face Recognition in New Delhi

Police in India's capital say they only require an 80 percent accuracy rate for matches, raising new alarm bells for civil liberty advocates.

8 May 2024

Hack exposes Indian police facial recognition data amid growing surveillance concerns

Despite the breach and security concerns, India continues to expand its use of facial recognition, deploying more cameras and upgrading biometric systems.

ALJAZEERA News Middle East Explained Opinion Sport Video More

Trending Where is the Madleen Gaza Flotilla? Russia-Ukraine war War on

News | Privacy

Facial recognition taken to court in India's surveillance hotspot

Lawsuit challenges facial recognition as unconstitutional in Telangana, the state using the most facial recognition systems.

Crumbling security: 1,500 CCTVs of 3,686 non-functional

Soumitra Bose / May 6, 2025, 01:25 IST

Share AA Follow Us

3.Scope of the Policy

This policy applies to:

- **Law Enforcement Agencies**: State Police, CAPFs, Intelligence Units
- **FRT Use Cases**:
    - Public-space surveillance
    - Protest/event crowd monitoring
    - Integration with CCTNS/NCRB databases
    - CCTV, drones, and live face matching

Excluded: Private/commercial FRT systems, which fall under separate data protection regulations.

4.Why India Needs This Policy

India is one of the top adopters of FRT, with projects like **AFRS**, **Digi Yatra**, and **Smart City Surveillance**. Yet, key questions remain unanswered:

- Who can collect/store facial data?
- What is the retention period?
- Who ensures ethical use?
- What redressal do citizens have?

Key Risks**:**

- False positives & wrongful arrests
- Profiling of minorities, activists
- Unchecked surveillance without warrants

Key Needs:

- Legal safeguards and institutional review
- Bias audits and algorithmic transparency
- Citizen consent and grievance redressal

5.Benefits and Future Potential

Current Benefits:

- Missing persons and child trafficking resolution
- Airport/train station security
- Smart city FRT alert systems

Future Potential:

- India-trained bias-free AI models
- Decentralized, citizen-owned FRT
- Integrated drone surveillance and cyber policing

6.Budget & Resource Allocation

Estimated Budget: ₹750 Cr

Component	Allocation
FRT Testing & Validation Labs	₹500 Cr
Training Law Enforcement in Ethical AI	₹100 Cr
Citizen Awareness + Public Portal	₹50 Cr/year
FRT Ethics Board Setup (FEBI)	₹100 Cr

Funding Channels: Digital India, Smart Policing Mission, MeitY Grants

---

7. Institutional Oversight

- Nodal Ministry: Ministry of Home Affairs (MHA)
- Tech Vetting: Ministry of Electronics & IT (MeitY)
- Rights Oversight: National Human Rights Commission (NHRC)
- New Body: FRT Ethics Board of India (FEBI) – Evaluates, audits, and certifies all government FRT use

Mandatory for Each FRT Deployment:

- Privacy Impact Assessment (PIA)
- Bias & Discrimination Testing
- Legal Vetting by FEBI

8. Conclusion

India stands at a crossroads — between embracing digital policing and protecting democratic freedoms. With **DRISHTI–NAYAN**, we propose a forward-looking framework that:

- Balances law enforcement with civil liberties
- Ensures public trust through transparency
- Embeds accountability at every level

This policy is not anti-technology — it is pro-democracy, pro-safety, and pro-justice. The future of FRT in India must be human-centric, lawful, and inclusive.