International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 08 Augustl-2026 | Impact Factor: 3.5

A First Look into Users' Perceptions of Facial Recognition in the Physical World in India

Dr. Pankaj Kumar[1] and Dr. Kirna Rani[2]
[1]Assistant Professor, Akal Group of Technical & Management Institutions, Mastuana Sahib,
[2]PGT Teacher (Commerce), Saheed Bhai Diala Ji Public School, Longowal
(Email: pankajgoyal.sliet@gmail.com)

How to Cite this Article:

Kumar, P. & Rani, K. (2026). A First Look into Users' Perceptions of Facial Recognition in the Physical World in India. International Journal of Creative and Open Research in Engineering and Management, 02(8), 1-9. https://doi.org/10.55041/ijcope.v2i8.081

https://doi.org/10.55041/ijcope.v2i8.081

Abstract Facial recognition technology (FRT) has expanded rapidly across public and semi-public spaces in India, including airports, railway stations, police surveillance systems, gated communities, and commercial establishments. Drawing on available survey data, civil society reports, legal analysis, and secondary literature, this paper offers a first systematic examination of Indian users' perceptions of FRT deployed in physical environments. Findings indicate a complex, context-dependent picture: substantial public support exists for government and police use of FRT for security and crime control, yet significant concerns persist regarding privacy, accuracy biases (especially affecting women and certain communities), lack of consent and transparency, and the absence of a dedicated regulatory framework. Perceptions are shaped by trust in institutions, perceived utility, demographic factors, and lived experiences of surveillance. The paper highlights tensions between security benefits and rights-based risks, and outlines implications for policy, design, and future empirical research.

Keywords: facial recognition technology, privacy, surveillance, user perceptions, India, physical world, Digital Personal Data Protection Act

1. Introduction

Facial recognition technology has moved from controlled digital environments into the physical world, where cameras in public and semi-public spaces capture and match faces in real time. In India, deployments include DigiYatra at airports, CCTV-linked systems at railway stations and urban centres, police use for identifying suspects and protesters, biometric attendance systems, and private applications in gated communities and commercial spaces (Internet Freedom Foundation [IFF], n.d.; Outlook India, 2026).

While global research has examined user perceptions of FRT (Seng et al., 2021; Zhang et al., 2021), India-specific empirical work remains limited. Most available evidence comes from large-scale surveys on policing and surveillance (Common Cause & Lokniti-CSDS, 2023), small studies of younger cohorts, media reports of deployments, and legal critiques. This paper synthesises these sources to provide a first structured look at how Indian users perceive FRT in physical settings—its usefulness, risks, comfort levels, and the contextual factors that shape acceptance or resistance.

The analysis is guided by three questions: (1) How do Indian users evaluate the benefits and risks of FRT across different physical contexts? (2) What factors (trust, control, accuracy, demographics, location) influence these perceptions? (3) What are the implications for regulation and responsible deployment under India's emerging data protection regime?

2. Background: FRT in the Indian Physical World

India has become one of the more active adopters of FRT. The Internet Freedom Foundation's Panoptic Tracker documented over 170 FRT systems at various stages of procurement or deployment, with significant public investment (Hindu Business Line, 2024). Notable applications include:

- **Airports**: DigiYatra enables voluntary facial verification for contactless travel; proposals exist to expand real-time FRT cameras linked to central databases and NATGRID (Biometric Update, 2026; IFF, 2026).
- **Policing and public order**: Delhi Police and other forces have used FRT for missing persons, crime investigation, and monitoring of protests (The Wire, 2025; Indian Express, 2026).
- **Transport and urban spaces**: Railway stations and city CCTV networks incorporate or plan FRT.
- **Private and semi-private spaces**: Gated communities, offices, and some commercial venues use FRT for access control (Times of India, 2023).

Unlike passwords, facial biometrics are immutable. Error rates and demographic biases have been documented: commercial systems have shown higher misidentification rates for Indian women than men (Scroll.in, 2021). The Supreme Court's recognition of privacy as a fundamental right in *K.S. Puttaswamy v. Union of India* (2017) requires any intrusion to satisfy legality, necessity, proportionality, and procedural safeguards. The Digital Personal Data Protection (DPDP) Act, 2023, regulates personal data processing but contains broad exemptions for state functions related to security, public order, and law enforcement, and does not specifically address real-time biometric surveillance (Outlook India, 2026; The Wire, 2026).

3. Existing Evidence on User Perceptions in India

3.1 Support for Security-Oriented Uses

The most comprehensive public opinion data comes from the Status of Policing in India Report (SPIR) 2023, based on face-to-face interviews with nearly 10,000 respondents across 12 states and union territories (Common Cause & Lokniti-CSDS, 2023). Key findings include:

- Approximately half of respondents supported government (50%) and police (46%) use of FRT.
- Support was substantially higher for government than private-sector use.
- 61% supported FRT to identify people protesting against the government or its laws/policies.
- Support was even higher for identifying participants in communal riots or disturbances of public order (around 75%).
- Nearly 80% supported maintaining FRT databases of people convicted of minor or serious offences; support dropped for those merely charged but not convicted.

These figures suggest many citizens prioritise security and order over absolute privacy when the technology is framed as a tool of the state against crime or disorder. Regional variation was notable: higher support in states such as Gujarat and Andhra Pradesh, lower in Punjab, West Bengal, and among certain communities.

3.2 Concerns and Critiques

Support coexists with unease. SPIR data showed that many respondents still feared mass surveillance, and only a minority believed police were adequately trained to use advanced tools. Adivasi and Muslim respondents expressed greater criticism of biometric collection of suspects (Common Cause & Lokniti-CSDS, 2023).

A small quantitative study of Generation Z respondents (ages 18–24) found high familiarity with FRT and recognition of convenience benefits, alongside strong concerns about surveillance, loss of control over biometric data, potential

misuse, and inadequate legal protection (IJRASET study). Participants often felt they had limited agency over how facial data were collected, stored, or shared.

Media reporting and civil-society documentation reveal further practical concerns: lack of notice or meaningful consent in many deployments, opacity around databases and retention periods, risk of function creep (from missing persons to protest monitoring), and accuracy issues that can lead to wrongful identification (The Wire, 2025; Scroll.in, 2021). Protesters at sites such as Jantar Mantar have reportedly covered their faces or avoided certain areas out of fear of being profiled (Indian Express, 2026).

3.3 Contextual and Comparative Insights

International research shows that perceptions of FRT are highly context-dependent rather than binary (Seng et al., 2021). Users weigh utility, organisational trustworthiness, degree of control, and physical surroundings. Indian evidence aligns with this pattern: higher acceptance for security and convenience applications (airports, crime databases) and greater scepticism toward open-ended public surveillance or private commercial uses. Cultural and institutional factors—dense public spaces, pragmatic attitudes toward privacy in daily life, and relatively high institutional trust in some security contexts—also shape responses (Economic Times commentary, 2026).

4. Factors Shaping Perceptions

Several interrelated factors emerge from the available evidence:

- **Perceived utility and context**: FRT is more acceptable when framed as improving safety, reducing queues, or catching serious offenders than when associated with monitoring peaceful assembly or commercial profiling.
- **Trust in the deploying organisation**: Greater willingness to accept government/police use than private-sector use.
- **Control and consent**: Lack of notice, inability to opt out, and uncertainty about data flows reduce comfort.
- **Accuracy and fairness**: Documented higher error rates for women and potential disparate impact on minorities raise equity concerns.
- **Demographic and regional differences**: Support varies by state, community, and socioeconomic position; minority and marginalised groups often express stronger reservations.
- **Awareness and knowledge gaps**: A non-trivial portion of the population reports limited awareness of FRT or of privacy rights, which can produce passive acceptance.

5. Discussion: Tensions and Implications

Indian users do not reject FRT outright. Many appear willing to trade some privacy for perceived security and convenience, especially when the technology is associated with the state. At the same time, significant minorities—and particularly members of certain communities—express discomfort with mass biometric capture, potential misuse, and the chilling effect on expression and assembly.

This tension is sharpened by the regulatory gap. The DPDP Act provides a baseline for private-sector processing but leaves large exemptions for law-enforcement and security uses. No dedicated statute currently governs real-time FRT in public spaces, retention limits, accuracy thresholds, independent audits, or redress mechanisms. Deployments frequently rest on administrative decisions or procurement rather than clear legislative authorisation, raising questions under the *Puttaswamy* proportionality test.

For technology designers and deployers, the findings underscore the importance of transparency (clear notice), purpose limitation, human oversight of matches, and mechanisms for challenge and correction. For policymakers, the

evidence points toward the need for sector-specific rules that distinguish verification (one-to-one) from identification (one-to-many) in open spaces, mandate judicial or independent oversight for sensitive uses, and require public reporting on accuracy and impact.

6. Limitations and Future Research

This paper is a synthesis of secondary sources rather than a new primary study. Existing surveys provide valuable breadth but limited depth on everyday physical encounters with FRT or on qualitative rationales. Small-sample work on younger users offers richer insight but lacks generalisability. Future research should include:

- Vignette-based or experience-sampling studies adapted to Indian urban and rural contexts;
- Qualitative interviews exploring trade-offs people actually make;
- Disaggregated analysis by gender, caste, religion, class, and region;
- Longitudinal tracking as deployments expand and the DPDP regime is implemented.

7. Conclusion

Users' perceptions of facial recognition in the physical world in India are neither uniformly enthusiastic nor uniformly hostile. They are pragmatic, context-sensitive, and shaped by trust, utility, and lived experience of institutions. Substantial support for security-oriented applications coexists with legitimate worries about privacy, bias, opacity, and democratic chill. Addressing these concerns requires not only better technical design but also clearer legal boundaries, meaningful transparency, and opportunities for public deliberation. As FRT becomes more embedded in everyday Indian spaces, understanding and responding to users' perceptions will be essential for building systems that are both effective and rights-respecting.

References

Common Cause & Lokniti Programme, Centre for the Study of Developing Societies. (2023). *Status of policing in India report 2023: Surveillance and the question of privacy*. https://commoncause.in/

Hindu Business Line. (2024, June 14). Widespread use of facial recognition tech across India. *The Hindu Business Line*.

Internet Freedom Foundation. (2026, July 6). IFF raises concerns over proposed plan to further integrate facial recognition cameras in major Indian airports. https://internetfreedom.in/

Outlook India. (2026, July 15). Facial recognition in India: Privacy, surveillance and the missing legal framework. *Outlook India*.

Scroll.in. (2021, August 5). Indian faces were run through facial recognition tech tools. Here's why you should be concerned. https://scroll.in/

Seng, S., Al-Ameen, M. N., & Wright, M. (2021). A first look into users' perceptions of facial recognition in the physical world. *Computers & Security, 105*, 102227. https://doi.org/10.1016/j.cose.2021.102227

The Wire. (2025, July 1). Special | As AI took over policing in Delhi, who bore the brunt? *The Wire*.

Times of India. (2023, March 1). Facial recognition technology at Hyderabad gated areas: Experts flag privacy concerns. *The Times of India*.