



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

CHALLENGES, ISSUES, AND SOLUTIONS IN PREDICTIVE POLICING AND FACIAL RECOGNITION TECHNOLOGY

~Shruti Chourasiya

ABSTRACT

*Modern law enforcement is shifting from reactive tracking to pre-emptive surveillance through **Predictive Policing and Facial Recognition Technology (FRT)**. This paper explores the deep operational, ethical, and legal challenges these technologies pose within the Indian digital landscape. While promoted as tools for efficiency, their actual deployment—such as during the 2020 Delhi riots—reveals severe threats to civil liberties, automated bias against marginalized communities, and a lack of legislative oversight.*

*By analyzing Indian constitutional benchmarks like Puttaswamy (2017) alongside global precedents like Loomis (USA) and Bridges (UK), this study evaluates how unchecked biometric data collection violates **Articles 14, 19, and 21** of the Constitution. The paper exposes the "black box" nature of these algorithms, which hide systemic biases under proprietary secrets. Ultimately, it argues that India must abandon unregulated surveillance under general police powers and establish a strict, statutory framework that enforces transparency, algorithmic auditing, and human rights safeguards.*

1. INTRODUCTION

The concept of predictive policing began with place-based criminology in the 1800s, studying patterns of crime in specific areas. It evolved from traditional crime mapping in the early 2000s, with major U.S. police departments experimenting with hotspot identification. Advancements in big data and AI have transformed it into sophisticated algorithms that forecast crime

locations and times based on historical patterns, with facial recognition technology (FRT) emerging around the same time, though its use by law enforcement became highly controversial in the 2020s due to issues of privacy and potential discrimination. FRT became a powerful technology in the private sector with companies developing massive databases of internet images. Gradually the public became aware of law enforcement's use of FRT, often through private companies, like Clearview AI, that scraped images from the internet and social media for their databases. Though with its clearcut benefits there were some challenges using the same. Predictive policing and FRT in India entered into serious controversy around 2019-2020, when their deployment began to intersect with civil liberties, privacy concerns, and allegations of discriminatory enforcement. In 2019, the Indian Government announced plans to build the world's largest facial recognition system for policing. Civil society groups raised alarms over the lack of legal safeguards, transparency, and public consultation. During the Delhi riots in February 2020, police used FRT to identify and arrest individuals, including protestors against the Citizenship Amendment Act (CAA). Investigations revealed that arrests were made solely on the basis of facial recognition, without corroborating evidence or public witness testimony. This led to accusations of biased policing, especially against marginalized communities like Muslims and Dalits. This paper aims to highlight the grave issues and challenges associated with Predictive Policing and FRT which can possess serious threats in future. We will explore the judgments associated with it in the common legal system which will help us to frame a comparative analysis on the legality of the usage of predictive policing and FRT.

2. ISSUE

There is no doubt that Predictive policing and FRT provides us with several benefits. While they offer significant benefits, they also raise serious operational, ethical, legal, and civil rights challenges, particularly concerning bias, accuracy, transparency, privacy, and community trust. Predictive policing often reinforces systemic biases by relying on flawed historical data, disproportionately targeting marginalized communities. The use of opaque algorithms limits transparency and accountability, making oversight difficult. These practices erode public trust,

especially in communities already wary of law enforcement. Additionally, mass data collection without consent poses serious privacy risks. Talking about FRT raises serious concerns due to its lower accuracy for women and people of colour, often resulting in misidentification and civil rights violations. Its deployment without consent fosters mass surveillance, disproportionately.

affecting marginalized communities. The absence of clear policies and oversight further complicates accountability.

3. LEGALITY OF PREDICTIVE POLICING AND FRT

While predictive policy and FRT are increasingly used by Indian law enforcement, their legality is not clearly established. As there is no specific law regulating both. Deployments are often carried out under general police powers or as a part of city initiatives, without parliamentary oversight. In the Putaswamy case of 2017 where the Supreme Court recognized privacy as a fundamental right u/a 21. It also held that any use of Predictive policing and FRT must meet the three-part test: legality, necessity, and proportionality. The Information Technology Act, 2000 classifies biometric data (including facial images) as sensitive personal data, but applies mainly to private entities. The Digital Personal Data Protection Act, 2023 adds some safeguards, but doesn't directly regulate surveillance or predictive policing. Predictive Policing relies on historical crime data, which may embed caste, class and communal biases. It risks violating Article 14 (equality) and Article 21 (due process) due to profiling and pre-emptive targeting. FRT is often deployed without consent, transparency or oversight, raising concerns u/a 19 (Freedom of Movement and expression) and Article 21 (privacy). Projects like the National Automated Facial Recognition System (NAFRS) have been criticized for lacking legal safeguards and public consultation. Courts have not yet ruled directly on the constitutionality of Predictive policing or FRT. However, judgments like *Shreya Singhal v. UOI* (2015) and *Anuradha Basin v. UOI* (2020) emphasizes the need for clear legal basis and proportionality in restricting fundamental rights.

4. ANALYSIS

using Supreme Courts Judgments Privacy and Surveillance – Justice K.S. Puttaswamy v. Union of India (2017) In this case it was held that RIGHT TO PRIVACY is a fundamental right under article 21. Predictive policing and FRT involve mass data collection and surveillance. Any such use must meet the three-part test: (i) legality (backed by law), (ii) necessity (for a legitimate aim), (iii) proportionality (least intrusive means). Free Speech and Arbitrary Policing – Shreya Singhal v. Union of India (2015) It was held in the above case that vague laws are unconstitutional. Predictive policing may lead to profiling based on vague data patterns, chilling free speech and dissent. Algorithms must be transparent and narrowly tailored to avoid arbitrary enforcement. Equality and Non-Discrimination – Amish Devgan v. Union of India (2020) Hate speech must be judged contextually; intent and impact matter. Predictive models trained on biased data may disproportionately target marginalized groups, violating Article 14. In the U.S. the case of State v. Loomis (Wisconsin) 2016, it upheld the use of COMPAS, a predictive risk assessment tool, but flagged concerns about transparency and due process. The court allowed its use with caution. In Clearview AI Litigation: multiple lawsuits challenge the scraping and use of facial data without consent raising 4th Amendment and Privacy law concerns. In the U.K. FRT is governed by a mix of common law policing

powers, the Data Protection Act, 2018, the Human Rights Act 1998 and GDPR. The position of predictive policing in the U.K. is legally ambiguous as they are used under general police powers but lack statutory regulation. In *Bridges v. South Wales Police* (Court Of Appeal, 2020) it was held that the use of Live Facial Recognition was lawful in principle but SWP failed to comply with data protection, privacy and equality laws.

5. Rationale behind the use of Predictive Policing and FRT

Predictive Policing is designed to enhance law enforcement efficiency by using historical crime data and algorithms to forecast potential criminal activity. It helps to identify crime hotspots, allocate resources strategically, and intervene proactively to prevent offences. The goal is to shift policing from reactive to preventive, improving public safety and operational effectiveness. FRT enables rapid identification and verification of individuals using biometric data. It supports law enforcement in locating suspects, verifying identities and monitoring public spaces. It is valued for its speed, automation and potential to strengthen security infrastructure, especially in high risk or densely populated areas.

6. Challenges posed by Predictive Policy and FRT

- a. Challenges posed by predictive policing:
 - Bias and discrimination- Predictive models often rely on historical crime data, which may reflect systemic biases. This can lead to disproportionate targeting of marginalized communities, reinforcing over-policing and social inequities.
 - Lack of Transparency- Algorithms used in predictive policing are typically proprietary and opaque, making it difficult to assess how decisions are made. This undermines accountability and public trust.
 - Due Process Concerns- Pre-emptive policing based on algorithmic forecasts may violate the presumption of innocence and lead to interventions without concrete evidence.
 - Privacy Intrusions- Predictive systems often require mass data collection, raising concerns about surveillance and the erosion of individual privacy rights.
- b. Challenges posed by FRT

- Demographic Bias and Accuracy Issues FRT systems have shown lower accuracy for women and people of colour, increasing the risk of misidentification and wrongful detentions.
- Mass Surveillance and Consent FRT is frequently deployed without public consent, creating environments of constant surveillance and infringing on civil liberties.
- Regulatory Gaps Many jurisdictions lack clear policies on FRT use, including data retention, watchlist criteria, and oversight mechanisms.
- Ethical and Legal Complexity Balancing public safety with rights to privacy, expression, and equality remains a major challenge, especially in the absence of standardized legal frameworks.

7. PROPOSED SOLUTIONS

1. Establish a Comprehensive Legal Framework- Enact dedicated legislation that clearly defines the scope, limitations, and permissible use of both predictive policing and FRT and ensuring alignment with constitutional protections under Articles 14 (equality), 19 (freedom of expression), and 21 (privacy and due process).
2. Ensure Transparency and Accountability- Mandate algorithmic transparency through public audits, explainability standards, and disclosure of data sources. Require law enforcement agencies to publish annual reports on the use, outcomes, and oversight of these technologies.
3. Implement Bias Mitigation and Accuracy Standards- Use diverse and representative datasets to train predictive models and FRT systems. Conduct regular bias testing and accuracy evaluations, especially across gender, caste, and ethnic lines.
4. Strengthen Oversight and Human Review- Create an independent regulatory body to monitor deployment, investigate misuse, and enforce compliance. Ensure that algorithmic outputs are advisory, not determinative—final decisions must involve human judgment and be subject to review.
5. Safeguard Privacy and Consent- Require explicit consent for FRT use in non-criminal contexts and ensure individuals are informed when under surveillance. Limit data retention periods and prohibit secondary use of biometric or predictive data without legal authorization.

6. Promote Public Engagement and Digital Literacy- Involve civil society and local communities in policy consultations and oversight boards and launch awareness campaigns to educate citizens on their rights and the implications of surveillance technologies.

8. Conclusion and Personal Opinion

While predictive policing and facial recognition technologies hold promise to increase law enforcement effectiveness and public safety, the significant risks of bias, privacy violations, and erosion of public trust cannot be overlooked. Responsible governance requires a multifaceted approach: adopting strong legal and ethical frameworks, increasing transparency, mandating independent oversight, engaging communities, and applying cautionary limits or bans where necessary. I personally believe that use of Predictive policing and FRT is essential. Instead of looking for methods to remove it, we should adapt it. We live in a country with overburdened courts, limited police personnel, and millions of pending cases. Technologies like Predictive Policing and Facial Recognition Technology (FRT) can offer much-needed efficiency and precision. "In the future, privacy will be a thing of the past." — Scott McNealy, former CEO of Sun Microsystems. So maybe privacy isn't a myth—it's a battlefield. And the question isn't whether it exists, but how fiercely we're willing to defend it.

