JUDICIAL RESPONSE TO FACIAL RECOGNITION UNDER RIGHT TO PRIVACY IN INDIA

Shatakshi Singh, BA LLB (Hons.), Amity University

Dr. Reshma Umair, Associate Professor, Amity University

ABSTRACT

The rapid proliferation of Facial Recognition Technology (FRT) in India, exemplified by initiatives such as the Automated Facial Recognition System (AFRS) and DigiYatra, marks a paradigm shift in state surveillance and governance.

While these technologies promise enhanced security, efficiency in criminal identification, and seamless public service delivery, they simultaneously pose an unprecedented threat to the fundamental Right to Privacy. This research paper explores the constitutional validity of FRT in India, specifically analyzing the vacuum of legislative oversight and the consequent reliance on judicial interpretation.

The paper scrutinizes the technology through the lens of the landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India, which established privacy as a fundamental right under Article 21 of the Constitution.[1] It argues that the current deployment of FRT lacks the requisite "procedure established by law," fails the test of proportionality, and creates a "chilling effect" on civil liberties. By examining the limited judicial responses in India—ranging from high court observations on CCTV surveillance to pending litigations—and comparing them with global jurisprudential trends like the Bridges case in the UK, the paper attempts to construct a judicial standard for biometric surveillance. The study concludes that in the absence of a dedicated data protection framework regulating government surveillance, the unchecked expansion of FRT risks transforming the Indian democracy into a digital panopticon.

[1] *K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1 (India).

1. INTRODUCTION

1.1 Background of the Study In the digital age, the human face has transformed from a mere biological identifier into a digital key capable of unlocking vast troves of personal data. Facial Recognition Technology (FRT) utilizes biometric software to map facial features from a photograph or video, comparing the information with a database of known faces to find a match. In India, the adoption of FRT has been aggressive and widespread. From the National Crime Records Bureau's (NCRB) ambitious Automated Facial Recognition System (AFRS) aimed at modernizing policing[2], to the DigiYatra initiative for contactless airport entry, the technology is becoming ubiquitous.

However, this technological leap has occurred largely in a legal vacuum. Unlike traditional surveillance methods, FRT allows for mass surveillance without physical proximity, enabling the state to track individuals in real-time across public spaces. This capability fundamentally alters the relationship between the citizen and the state, shifting the balance of power heavily in favor of the latter.

1.2 Statement of the Problem The core legal problem lies in the tension between state security imperatives and individual privacy rights. India currently lacks a specific statute governing the use of FRT. The Personal Data Protection framework (specifically the DPDP Act, 2023) contains broad exemptions for government agencies in the interest of national security[3] and public order. Consequently, the deployment of FRT is largely an executive action, devoid of legislative scrutiny or judicial oversight.

This absence of a regulatory framework raises critical constitutional questions: Does the use of FRT satisfy the "legality" and "proportionality" tests laid down by the Supreme Court in *Puttaswamy*? Without a specific law, can the state infringe upon the biometric privacy of citizens? The judiciary, therefore, becomes the sole bulwark against potential state overreach.

1.3 Research Objectives The primary objectives of this research paper are:

[2] NAT'L CRIME RECS. BUREAU, REQUEST FOR PROPOSAL FOR AUTOMATED FACIAL RECOGNITION SYSTEM
(2019).

[3] The Digital Personal Data Protection Act, 2023, § 17, No. 22 of 2023, Acts of Parliament, 2023 (India).

1. To analyze the operational mechanism and extent of FRT deployment in India.
2. To examine the Right to Privacy as a fundamental right and its specific application to biometric data.
3. To critique the existing judicial response to surveillance technologies in India.
4. To determine whether current FRT practices withstand the constitutional test of proportionality.

1.4 Research Methodology This paper employs a **doctrinal research methodology**. It relies on primary legal sources, including the Constitution of India, Supreme Court judgments (specifically privacy jurisprudence), and relevant statutes such as the Information Technology Act, 2000. Secondary sources, including legal journals, reports by the Internet Freedom Foundation (IFF), and comparative case laws from the United Kingdom and the United States, are utilized to provide a critical perspective on the subject.

2. FACIAL RECOGNITION TECHNOLOGY: CONCEPT AND CONTEXT

2.1 Understanding the Technology To appreciate the legal implications, one must understand the functionality of FRT. The technology operates on three primary steps:

1. **Detection:** The system locates a face within an image or video feed.
2. **Analysis:** It maps the geometry of the face (distance between eyes, nose width, jawline) to create a unique "faceprint."
3. **Recognition:** The faceprint is compared against a pre-existing database.

Legally, the distinction between **1:1 verification** (is this person who they claim to be? e.g., unlocking a phone or DigiYatra) and **1: Many identification** (who is this person in this crowd? e.g., police surveillance) is crucial. The latter, "**1: Many**," poses the most significant threat to civil liberties as it presumes everyone in a public space is a suspect until identified, effectively reversing the presumption of innocence.

2.2 The Indian Landscape of Deployment India creates a unique ecosystem for FRT due to the massive scale of its population and the centralization of biometric data (Aadhaar).

- **The NCRB and AFRS:** The National Crime Records Bureau issued a Request for Proposal (RFP) for a centralized AFRS that would integrate facial data[4] from CCTV feeds with existing criminal databases (CCTNS). The objective is to identify criminals, missing children, and unidentified bodies. However, legal scholars argue that without a statutory basis, creating such a centralized database violates the rule of law.

- **DigiYatra:** Under the Ministry of Civil Aviation, this initiative uses FRT for airport entry. While technically "voluntary," there have been numerous reports of coercive enrollment and lack of informed consent, raising issues regarding the "informational self-determination" aspect of privacy.

- **Policing and Operation Chabutra:** In Telangana, law enforcement officers have been equipped with handheld devices to scan pedestrians' faces to check for criminal history. This practice, often conducted without a warrant or reasonable suspicion, represents the most visceral conflict between FRT and Article 21[5].

- **Educational Institutions:** Several universities and schools in India have implemented FRT for attendance, normalizing surveillance in educational environments and raising questions about the privacy of minors and young adults.

2.3 The "Function Creep" Phenomenon A critical aspect of the Indian FRT context is "function creep"—where data collected for one purpose is used for another. For instance, data collected for traffic violations (via ANPR and traffic cameras) being utilized for criminal investigations or monitoring peaceful protests. This fluidity of data usage, unchecked by rigid silos or legal firewalls, makes the judicial response vital. If the executive branch can repurpose biometric data at will, the concept of "purpose limitation"—a key tenet of data privacy—is rendered obsolete.

3. THE CONSTITUTIONAL FRAMEWORK: TESTING PRIVACY

3.1 The Post-Puttaswamy Era Before 2017, the legal status of privacy in

[4] NAT'L CRIME RECS. BUREAU, *supra* note 2.

[5] INDIA CONST. art. 21.

India was nebulous[6]. However, the nine-judge bench in *Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)* fundamentally altered the constitutional landscape. The Supreme Court held that the Right to Privacy is an intrinsic part of the Right to Life and Personal Liberty under **Article 21**[7].

Crucially for Facial Recognition Technology (FRT), the Court recognized **"Informational Privacy"**—the right of an individual to control the dissemination of their personal data. The face, being a biological attribute that allows for identification, falls squarely within this protective ambit.

3.2 The Three-Fold Test The Supreme Court laid down a strict three-fold test that any state intervention (like FRT surveillance) must pass to be constitutional. This test forms the backbone of any legal challenge against FRT:

1. **Legality (Existence of a Law):** The action must be sanctioned by a legislative act (a statute passed by Parliament), not just an executive order.

2. **Necessity (Legitimate State Aim):** The law must serve a valid purpose, such as national security or crime prevention.

3. **Proportionality (Rational Nexus):** The means used (FRT) must be proportionate to the aim. The state cannot use a "sledgehammer to crack a nut." Mass surveillance of innocent citizens to catch a few criminals fails this test.

4. REAL-TIME CASE STUDIES AND DEPLOYMENT

This chapter analyzes specific, real-time instances of FRT deployment in India, highlighting the legal controversies and the judicial response (or lack thereof) in each scenario.

4.1 Case Study I: S.Q. Masood vs. State of Telangana (Policing & Surveillance)

- **The Incident:** In May 2021, during the COVID-19 lockdown, S.Q. Masood, a social activist in Hyderabad, was stopped by police officers. They ordered him to

[6] *See M.P. Sharma v. Satish Chandra*, A.I.R. 1954 S.C. 300 (India); *Kharak Singh v. State of Uttar Pradesh*, A.I.R. 1963 S.C. 1295 (India).

[7] *K.S. Puttaswamy*, (2017) 10 S.C.C. 1 at ¶ 3 (India).

remove his mask and photographed him using a handheld tablet. When he objected, citing privacy, the police dismissed his concerns. The photo was allegedly processed through the **TSCOP** app, which links to criminal databases.

- **The Litigation:** Masood filed a Public Interest Litigation (PIL) in the **Telangana High Court** (*W.P. PIL No. 10 of 2022*).[8]

- **Legal Arguments:** The petitioner argued that the use of FRT by Telangana Police lacks any statutory backing (violating the "Legality" prong of *Puttaswamy*). Furthermore, treating every citizen as a potential suspect without "reasonable suspicion" violates the presumption of innocence.

- **Judicial Status:** The High Court issued notices to the State Government. The case is currently sub-judice and represents the most direct judicial challenge to **"predictive policing"** and stop-and-search biometric profiling in India. It tests whether executive discretion can override constitutional privacy rights in the name of "law and order."

4.2 Case Study II: The DigiYatra Controversy (Consent & Exclusion)

- **The Context:** DigiYatra uses FRT to facilitate "paperless" entry at airports. While the Ministry of Civil Aviation claims it is "voluntary," on-ground realities differ.

- **The Incident (2024-2025):** There were widespread reports and complaints of airport security personnel coercing passengers into signing up for DigiYatra or capturing their facial biometrics without informed consent.

- **Legal Issue:** This violates the principle of **"Informed Consent"** under the Digital Personal Data Protection (DPDP) Act, 2023. Additionally, a dispute regarding data ownership arose between the Digi Yatra Foundation (a private non-profit) and its technology partners, raising concerns about third-party access to biometric data of millions of flyers.

- **Judicial/Legal Response:** While specific PILs are pending, the legal consensus is

[8] *S.Q. Masood v. State of Telangana*, W.P. (PIL) No. 10 of 2022 (Telangana H.C., filed Dec. 2021).

that "coercive voluntariness" renders consent void ab initio. The lack of a clear exit mechanism (right to be forgotten) further complicates its legality.

4.3 Case Study III: Patna High Court Ruling (January 2026)

- **The Context:** The Bihar government mandated an Aadhaar-linked GPS-enabled facial recognition system for marking the attendance of doctors and faculty in medical colleges.

- **The Case:** Doctors challenged this move, arguing it violated their privacy and dignity by placing them under constant surveillance.

- **The Judgment (Jan 2026):** In a significant recent ruling, the **Patna High Court** upheld the validity of the FRT system.[9]

- **Judicial Reasoning:** The Court distinguished "surveillance" from "administrative monitoring." It held that:

    1. Public servants (doctors) have a lower expectation of privacy during duty hours.

    2. The aim (ensuring doctors are present for patient care) is a **legitimate state aim**.

    3. The measure is **proportionate** to the goal of "Good Governance."

- **Significance:** This case is a crucial precedent. It suggests that Indian courts may *permit* FRT when it is targeted, limited to public employees, and serves a clear public utility, distinguishing it from the mass surveillance in the *Masood* case.

4.4 Case Study IV: Delhi Police & The "Function Creep" (Protests)

- **The Incident:** During the 2019-2020 anti-CAA protests and subsequent Farmers' Protests, Delhi Police used FRT to screen crowds.

- **The Legal Violation (Function Creep):** An RTI filed by the **Internet Freedom**

[9] *In re: Mandatory Biometric Attendance v. State of Bihar*, C.W.J.C. No. 105 of 2026 (Patna H.C. Jan. 12, 2026).

Foundation (IFF) revealed that the FRT software used by Delhi Police was originally authorized by the Delhi High Court *solely for the purpose of finding missing children* (*Sadhan Haldar v. NCT of Delhi*).[10]

- **Analysis:** The police repurposed a tool meant for child protection to identify political protesters. This is a classic example of **"Function Creep"**—using data/tech for a purpose other than what it was legally authorized for. This violates the **"Purpose Limitation"** principle of data protection.

5. LEGAL ANALYSIS AND JUDICIAL TRENDS

5.1 The "Legality" Vacuum The common thread across all case studies (except the Patna HC case which relies on service rules) is the **absence of a primary statute**. The Personal Data Protection Act (DPDP Act 2023) has broad exemptions for the state (Section 17).

- *Analysis:* Without a "Facial Recognition Act," agencies like the NCRB operate FRT systems based on Requests for Proposals (RFPs) and executive memos. The Supreme Court in *Puttaswamy* clearly stated that an executive notification does not constitute "law" for infringing privacy. Therefore, systems like AFRS are currently operating in a zone of unconstitutionality.

5.2 Algorithmic Bias and Article 14 FRT systems are not neutral. Studies have shown they have higher error rates for darker skin tones and women.

- *Legal Implication:* If an FRT system falsely identifies an innocent person due to algorithmic bias (False Positive), it results in wrongful confinement or harassment. This violates **Article 14 (Right to Equality)** because the technology disproportionately prejudices specific demographics. The Indian judiciary has yet to adjudicate on "algorithmic discrimination," making this a fertile ground for future constitutional jurisprudence.

5.3 The "Chilling Effect" The mere existence of mass surveillance cameras with FRT capabilities creates a "chilling effect" on **Article 19(1)(a)** (Freedom of Speech). If citizens know they are being face-mapped at a protest (as seen in Case Study IV), they may refrain

[10] *Sadhan Haldar v. NCT of Delhi*, W.P. (Crl.) No. 1560 of 2017 (Del. H.C. 2018).

from exercising their democratic right to dissent. The courts must recognize that privacy is a prerequisite for the exercise of other fundamental liberties.

6. COMPARATIVE JUDICIAL TRENDS (GLOBAL STANDARDS)

To critique the Indian judicial response effectively, it is essential to compare it with established global jurisprudence. Other democracies have grappled with the same tension between FRT and privacy, often resulting in stricter judicial outcomes.

6.1 The United Kingdom: The *Bridges* Case Precedent The most significant global ruling on FRT is arguably *R (Bridges) v Chief Constable of South Wales Police (2020)*.[11]

- **Facts:** The South Wales Police used AFR (Automated Facial Recognition) in public spaces. Ed Bridges, a civil liberties campaigner, challenged this.
- **The Ruling:** The Court of Appeal held the police use of FRT was **unlawful**.
- **Key Takeaways for India:**
    1. **"Too Much Discretion":** The Court ruled that the police had too much discretion in deciding *who* to put on the "Watchlist" and *where* to deploy cameras. This mirrors the Indian situation with the NCRB and local police.
    2. **Equality Act Violation:** The Court found the police had not done enough to verify if the software had racial or gender bias. This sets a precedent for challenging Indian FRT under **Article 14** (Equality) due to known biases against darker skin tones.

6.2 The United States: A Patchwork of Bans and Regulation Unlike India’s centralized approach, the US response has been fragmented but aggressive in parts.

- **San Francisco Ordinance (2019):** became the first major city to **ban** the use of FRT by police and other government agencies, citing the threat to civil liberties.[12]
- **Illinois Biometric Information Privacy Act (BIPA):** A robust law that requires

[11] *R (Bridges) v. Chief Constable of South Wales Police* [2020] EWCA (Civ) 1058 (Eng.).

[12] S.F., CAL., ADMIN. CODE ch. 19B (2019).

written consent before private companies can collect biometric data. This stands in stark contrast to the DigiYatra model where consent is often assumed or coerced.

6.3 The European Union: The GDPR Standard Under the General Data Protection Regulation (GDPR), biometric data is classified as "Special Category Data" (Article 9). Processing it is generally **prohibited** unless explicit consent is given or it is strictly necessary for substantial public interest. The burden of proof is heavily on the state, unlike in India where the burden often falls on the citizen to prove privacy violation.

7. CRITICAL CHALLENGES AND CONCERNS

Beyond the legal vacuum, several practical and ethical challenges make the unrestricted use of FRT in India dangerous.

7.1 The "Black Box" Problem and Algorithmic Bias Indian faces are diverse. Most global FRT algorithms are trained on datasets dominated by Caucasian male faces.

- **The Error Rate:** Research indicates that FRT systems have significantly higher "False Positive" rates for women and people with darker skin tones.
- **The Consequence:** In a criminal justice system, a False Positive isn't just a glitch; it means an innocent person could be detained or interrogated. Without an **"Algorithmic Audit"** law, the Indian judiciary has no way to verify the accuracy of the tools the police are using.

7.2 Security Risks: "You Cannot Reset Your Face" Unlike a password or a credit card number, biometric data cannot be changed. If the AFRS database or DigiYatra servers are breached (a realistic concern given massive data leaks in India like the CoWIN breach), a citizen's facial identity is compromised forever. The current legal framework in India lacks specific provisions for **"Biometric Data Breach Notification"** or compensation for such irreversible loss.

7.3 Absence of Grievance Redressal If a citizen is wrongfully stopped by the police because of an FRT error (as feared in the *Masood* case), there is no clear administrative mechanism for redressal. The only option is a Writ Petition in the High Court, which is expensive and inaccessible for the common man.

8. CONCLUSION AND SUGGESTIONS

8.1 Conclusion

The deployment of Facial Recognition Technology in India is currently running faster than the law. While the *Puttaswamy* judgment established a fortress of privacy rights, the executive branch has found ways to tunnel underneath it using technology. The current use of FRT fails the **"Legality"** test because there is no specific statute authorizing it. It struggles with the **"Proportionality"** test because mass surveillance treats the entire population as suspects. As seen in the *Patna High Court* ruling versus the *Telangana* challenge, the judiciary is still finding its footing—permitting administrative monitoring while being wary of police surveillance. Ultimately, without legislative guardrails, FRT risks turning the promise of "Digital India" into the peril of a "Surveillance State."

8.2 Suggestions (The Blueprint for Reform) To balance security with privacy, this paper proposes the following legal reforms:

1. **Enactment of a "Facial Recognition Technology Act":** Parliament must pass a specific law regulating FRT, defining:
   - **Authorized Uses:** Strictly limited to serious felonies (murder, terrorism, kidnapping).
   - **Prohibited Uses:** Bans on using FRT for peaceful protests, misdemeanor tracking, or moral policing.
2. **Judicial Warrants for Surveillance:** Police should not be able to deploy FRT at their own discretion. Like wiretapping, the use of FRT in public spaces should require a judicial warrant based on probable cause.
3. **Mandatory Algorithmic Auditing:** Before any government agency deploys an FRT system, the algorithm must undergo an independent audit for racial and gender bias.
4. **Sunset Clauses for Data Retention:** Legislation must mandate that facial data collected from non-suspects (innocent bystanders) must be automatically deleted

within 24 hours.

5. **Strict "Purpose Limitation":** Data collected for public services (DigiYatra) must be legally firewall-ed from law enforcement databases (NCRB) to prevent function creep.

BIBLIOGRAPHY

Statutes & Bills:

- The Constitution of India, 1950.
- The Digital Personal Data Protection Act, 2023.
- The Information Technology Act, 2000.

Case Laws:

- *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1.
- *S.Q. Masood vs. State of Telangana*, W.P. (PIL) No. 10 of 2022 (Telangana HC).
- *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058 (UK).
- *Kharak Singh v. State of U.P.* (1963) AIR 1295.

Reports & Articles:

- Internet Freedom Foundation (IFF), "Project Panoptic".
- National Crime Records Bureau (NCRB), "Request for Proposal for Automated Facial Recognition System (AFRS)".