POLICE SURVEILLANCE TECHNOLOGIES AND PRIVACY PROTECTION IN INDIA: A CONSTITUTIONAL AND INSTITUTIONAL ANALYSIS OF FACIAL RECOGNITION SYSTEMS POST-PUTTASWAMY JUDGEMENT

Prananjeya B Gujjala, LLM (Criminal and Security Laws), Symbiosis Law School, Pune

ABSTRACT

Surveillance technologies have been gradually integrated into India policing that have radically changed the connection between the State and the individual. Facial recognition systems are one of the invasive types of surveillance among them, and they allow biometric identification at the population level and on a continual basis. This paper discusses the constitutional and institutional outlooks of the National Automated Facial Recognition System (NAFRS), which is a centralized facial recognition system used by law enforcement agencies in India.

Locating NAFRS in the aftermath of Justice K.S. Puttaswamy (Retd.). v. Union of India, the paper relies on the proportionality test of legality, necessity and proportionality to determine whether the system is compliant with Articles 14 and 21 of the Constitution. It concludes that NAFRS is not legally authorized, has no significant protection, and minimal supervision, making it a unconstitutional grey zone. The paper additionally reveals that the claims of necessity lack empirical evidence and that the magnitude and structure of facial recognition policing leads to imbalanced invasion in privacy and equality, especially since risks of algorithmic bias is recorded.

Besides the analysis of the doctrine, the paper points to structural deficits in police accountability and institutional capacity, which intensify the uncontrolled risks of surveillance. Based on comparative regulation strategies of the other constitutional democracies, the paper will end by either promoting a temporary police use of facial recognition moratorium or the passage of a rights-based legislative framework to guarantee constitutional adherence.

I. INTRODUCTION

Surveillance technologies are becoming more and more influential in modern policing in India.[1] Within the recent ten years, law enforcement agencies have increased the applications of CCTV networks, call data record analysis, Internet surveillance as well as database-driven investigative applications as a measure of standard policing, and this represents a trend in law enforcement that is endorsed across the world, as a measure of efficiency and crime prevention. Face recognition systems are one of such tools, and one of the most invasive types of state surveillance tools,[2] which significantly changes the relations between the individual and the State.

This institutionalisation has been put into place by the National Automated Facial Recognition System[3] (NAFRS), a centralized biometric system that is employed by the law enforcement agencies to compare the facial image of the photographs, videos, or live feed against the databases maintained at the State level. The scale and structure of NAFRS suggest that, even though it is advertised as an investigative tool to help identify suspects and locate missing persons, the shift towards population-scale biometric surveillance is underway.

In this paper, the author claims that NAFRS reveals an urgent deficiency in the alignment between privacy jurisprudence and policing in India. Usually through the Puttaswamy proportionality framework, the paper illustrates that NAFRS does not satisfy the constitutional provisions in Articles 14 and 21. These weaknesses are not just the doctrinaire, but the institutional weaknesses of police accountability and the constitutional ability to use new technologies.

II. CONSTITUTIONAL FOUNDATIONS OF SURVEILLANCE REGULATION IN INDIA

A. Privacy as a Fundamental right and Surveillance as a Rights-Violating State Action.

Regulation of state surveillance in India is constitutional because it is based on the acknowledgment of privacy as one of the fundamental rights in the Article 21 of the Constitution. Colonial Law, 1892: Justice K.S. Puttaswamy (Retd.). v. Union of India,[4] the

[1] Shubhojit Chattopadhyay & Anupam Chander, *Surveillance, Privacy and the Indian Constitution*, 15 Indian J. L. & Tech. 1, 4–6 (2019).
[2] A. Michael Froomkin, *The Death of Privacy?*, 52 Stan. L. Rev. 1461, 1474–76 (2000).
[3] Nat'l Crime Records Bureau, Request for Proposal for National Automated Facial Recognition System (NAFRS) (2019).
[4] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

Supreme Court dismissed previous doctrinal scruples and ruled that privacy is inseparable with life and personal liberty. The Court conceptualised privacy not as a unitary or fixed right, but as a group of interests that are mutually relevant such as the bodily integrity, decision autonomy, informational self-determination, and protection against arbitrary intrusion by the state. Privacy, in this meaning, is a structural guarantee that ensures the conditions that are needed in the effective exercise of other fundamental rights.[5]

Such interpretation of constitutions has far reached consequences on state surveillance. Surveillance is no longer a mere act of watching, it is an aggressive, assertive way of claiming the power of the State that changes the relation between the individual and the State.[6] Surveillance technologies reform the movement, communication, and expression of opposition by facilitating the gathering, accumulation, and processing of personal information. Facial recognition technology (FRT), specifically, is an intellectual extension of the surveillance abilities: it transforms the human face into a ubiquitous biometric signature, which enables constant tracking of the subject in both the public and private areas, without his/her knowledge of it.

B. The Puttaswamy Test of Constitutional Control of Surveillance.

In order to punish the state surveillance, Puttaswamy expressed a systematic proportionality framework that any privacy-invading action has to meet. First, it needs to be sanctioned by the law, that is, it should have a legal basis on the basis of a transparent, accessible and democratically established legal provision. Second, it has to be pursuing a lawful state objective, and the tools used have to be requisite in pursuing the objective. Third, the measure should fulfil the requirement of proportionality that implies a reasonable relationship between means and ends, minimum loss of rights, and availability of procedural protection against abuse.

This model is especially quite challenging when used in the context of biometric surveillance. In contrast to the traditional policing techniques, biometric systems do not simply accumulate evidence to particular suspects, they establish long term systems of surveillance that are capable of gathering information about whole groups of people. The risks of such systems as the Court itself recognized in Puttaswamy are not just in a possible individual abuse, but in their aggregative possibilities, their ability to be reused and their ability to creep over time.

[5] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, 297–298 (Chandrachud, J.).
[6] Vidhi Centre for Legal Policy, Privacy and Surveillance in the Digital Age 22–24 (2022).

This, therefore, implies that the bar of constitutional justification in instances of biometric surveillance should be extremely high.

More importantly, the Puttaswamy test is not a form of a checklist that needs to be applied automatically. It is a substantive question which calls the State to prove the existence as well as the design of a surveillance system. This would involve showing why the less intrusive options are insufficient, the ways the risks of abuse are addressed and what the institutional processes are in place to promote continued compliance. When applied to policing, it implies that assertions of necessity by the executives cannot replace evidence-based justification or authorisation by legislation.

C. Surveillance Jurisprudence Pre Puttaswamy.

Before Puttaswamy, Indian surveillance jurisprudence was less than entirely coherent and mostly submissive to executive discretion. People in the Union of Civil Liberties v. Union of India[7] that dealt with telephone tapping, the Supreme Court identified the obtrusive quality of interception but limited its answer to a procedural protection that exists in an executive structure. Although the Court emphasized the mechanisms of review and documentation of rationales, it also refrained on the issue of how surveillance powers of interrogation was in wider perspective unlawful or disproportionate.

The post-Puttaswamy jurisprudence is an indication of gradual yet intermittent change. The Court in the Aadhaar litigation used the proportionality analysis to the large-scale data collection and stressed on the limitation of purpose, data minimisation, and the risks of profiling. Though Aadhaar was supported, in some sense, the rulings noted that technological systems that can identify a large number of people have special constitutional risks. Notably, the Court acknowledged that this lack of sufficient precautions can make such systems to be unconstitutional even in cases where their goals were facially valid.

In spite of these developments the judicial involvement in surveillance is mostly reactive and sectoral. Biometric surveillance by police officers has avoided specific constitutional scrutiny and courts have reviewed welfare databases and communication interception, but not police-operated biometric surveillance. This chasm is especially jarring considering that surveillance by the law enforcers is one of the most powerful types of data gathering, and its effects can be felt instantly in the areas of liberty, equality, and the right to one's own body.

[7] People's Union for Civil Liberties v. Union of India, (1997) 1 S.C.C. 301 (India).

D. Statutory Framework and the issue of Regulatory Silence.

The legal environment of police surveillance in India demonstrates a drastic disparity between the constitutional doctrine and the design of legislation. The Police Act, 1861,[8] and its state-level equivalents grant the police all-inclusive investigative authority, but the former was created at a time when no one could imagine an algorithmic or biometric surveillance. These laws do not offer any clear permission, restriction, or regulation structure to facial recognition or such a technique. General provisions referring to inquiry or upholding of civic harmony cannot conceivably fulfil the Puttaswamy requirement of legality of profoundly intrusive surveillance.

The Information Technology Act, 2000, is not very relevant as it only covers interception and the processing of data in particular situations but it does not regulate the biometric identification by the enforcement. More recently, Digital Personal Data Protection Act, 2023, has provided a general structure of data processing, but greatly watered it down when it comes to state agencies in its wide exemption of law enforcement and order.[9] These exemptions instead of restricting surveillance may legitimise it with no real protection.

The lack of a police-specific surveillance law is not a legislative oversight hence no, but a structural deficiency in constitutionalising policing in the digital age. Executive directions or tenders or internal procedures like the ones on the foundation of the National Automated Facial Recognition System cannot replace a parliamentary enactment. In making this point, Puttaswamy emphasizes that, in order to be legal, there must be a norm, but it must be a law that regulates the scope, purpose, oversight, meaningfully.

III. NAFRS AND THE ARCHITECTURE OF FACIAL RECOGNITION POLICING IN INDIA

A. Conceptualisation NAFRS: Investigative Aid to Surveillance Infrastructure.

The National Automated Facial Recognition System (NAFRS) is a drastic change in the structure of policing in India. NaFRS, which can be conceptualised as a centralised facial recognition system used by law enforcement, is intended to facilitate an automated process of matching facial images taken on photographs, video, or live surveillance feed to large-scale databases hosted by the State. In contrast to conventional identifying devices, e.g., fingerprints

[8] Police Act, No. 5 of 1861,
[9] Digital Personal Data Protection Act, No. 22 of 2023, Sec 7 (India).

or eyewitness testimony, the facial recognition is not only invisible but also active, making the normal everyday movement of people an output of information, which can be analysed with the help of algorithms.[1011]

NAFRS is described as an investigative resource that is supposed to enhance efficiency in locating the suspects, tracing missing individuals as well as to facilitate criminal investigations. Nonetheless, the technical design and logic of the functioning of the system imply a significantly greater capacity. Enabling the interoperability of various databases, as well as the integration with the CCTV networks, NAFRS is not just a case-specific investigative tool but a generalised surveillance infrastructure. Its possible uses do not just stop at post-crime investigation, but also in real-time crowd, protests, and public places tracking, which obscures the distinction between targeted policing and surveillance of population on a scale.

This difference is of constitutional importance. Specific tools used in a particular investigation may be evaluated in a fairly limited rights context. Conversely, infrastructures that are able to monitor continuously without being discriminatory creates systemic issues of autonomy, dissent, and democratic participation. The fact that facial recognition has been turned into a policing structure as opposed to forensic assistance thus changes the constitutional interests of its use.

B. Legal Thoroughfare and NAFRS Executive foundations.

The dependence on the executive action prompts an immediate constitutional issue according to the legality prong which is formulated in Puttaswamy. Such large-scale surveillance systems not only involve but are involved in the structural violation of fundamental rights. However, NAFRS has never been debated in parliament, defined in statute, or law regarding their protection.[12] Rather, its normative basis lies in some mix of administrative discretion and general, pre-digital policing laws that are inappropriate to govern biometric technologies.

This executive-based approach to surveillance governance demonstrates a more institutionalized version of the tendency in Indian policing: the process of increasing the coercive capacity not by democracy, but in an administrative way. Although this can be a fast method of adopting the technology, it also destroys accountability in the constitution. The non-legislative anchoring means an openness in which key questions, such as to whom can be

[10] Frank Pasquale, *The Black Box Society* 19–21 (Harvard Univ. Press 2015).
[11] Woodrow Hartzog & Evan Selinger, *The Invisibility of Facial Recognition*, 73 Md. L. Rev. 1, 8–12 (2013).
[12] Ministry of Home Affairs, NAFRS Concept Note & Tender Documents (2019).

surveilled, why, why, and with what remedies can be resolved internally within the police force.

C. Deployment and Expansion: Developments In 2025.

Since its original conceptualisation, NAFRS has proceeded through pilot experimentation to general deployments. It is reported that several State police departments have installed facial recognition equipment that can be incorporated or used with the NAFRS framework. The proliferation of urban CCTV systems and the growing computerisation of police databases has been coupled with these deployments to form an environment that is friendly to the automated identification and tracking of individuals.

As the coming 2025 tells us, facial recognition is already reported to be applied in various policing situations, such as outnumbered crowds, detection of criminal activities, and daily management of law-and-order. Of special interest is the normalisation of such use which is a gradual process.[13] Facial recognition is ceased to be an extraordinary device that can be applied in extraordinary situations and is instead seen as an ordinary aspect of daily policing. This change has taken place without simultaneous consultation of people, duties of transparency, and any independent checking and balancing systems.

The development of NAFRS also should be viewed in the context of bigger trends in data-based governance. Facial recognition is a gate-way technology that makes state surveillance more extensive and enduring as policing becomes more and more dependent on databases, predictive analytics, and automated decisions. The fact there are no explicit limits on the scale of deployment, the duration of retention, or even the subsequent secondary use, makes the risk of function creep, where systems designed with limited purposes slowly take on extended and more invasive uses, even more problematic.

D. Techno-Legal Operating Risk and Academic Concerns.

An increasing amount of legal and policy literature has recognized serious dangers related to police operations involving the use of facial recognition technologies. Misidentification is one of the issues that keep occurring, especially the rate of greater mistakes reported in women, racial minorities and marginalised population. Such mistakes have grave consequences in a policing setting, such as false stops, arrests and stigmatic damage.[14] These risks are compounded but not minimized when entrenched in a system that is non-transparent and

[13] Software Freedom Law Center, India, Facial Recognition Technology and State Surveillance 31–34 (2024).
[14] Nat'l Inst. of Standards & Tech., Face Recognition Vendor Test (FRVT) 5–8 (2019).

accountable.

The other main issue is the chilling effect created by extensive surveillance. The awareness or the intuition that one may be constantly under surveillance as well as the affiliation they have with peers adds to the discouragement of the exercise of basic rights, such as the right to gather, demonstrate, and protest. This is enhanced by the presence of facial recognition, which eliminates anonymity in the public, which has traditionally been viewed as a critical element in the process of democracy.[15]

Another risk that scholars have taken care to warn against is the threats of functional creep and institutional obscurity. Facial recognition systems can be used to a wider set of purposes, including minor crimes and even political surveillance without any legal restrictions on the purpose of use. The fact that publicly available information on the standards of accuracy, audit processes, and redressal is not available also negatively affects the trust and accountability.

IV. APPLYING THE PUTTASWAMY TEST TO NAFRS

A. Legality: Does NAFRS Have a Legal Foundation?

The first and the most basic of the requirements in Puttaswamy is that law must authorize any state action that violates privacy. The Court made it very clear that the executive convenience, administrative practice, or internal guidelines do not qualify to replace a clear and democratically enacted legal framework where the basic rights are at stake. The law, in this regard, requires specificity, accessibility, and normative constraint the law has to establish the boundaries of power, stipulate boundaries, and issue some form of protection against abuse.

Comparing it to this standard, the legal basis of NAFRS is weak in the constitution. The system is not based on any explicit parliamentary legislation granting the application of the facial recognition technology by the police. The Police Act, 1861, or any of the State Police Acts, does not contain the means of consideration of biometric identification using an automated analysis of the face. These laws grant very wide investigative powers, yet Puttaswamy clarifies that general police authority is not adequate to support very intrusive technologies of surveillance. The more obtrusive the action the more precise legislation is needed.[16]

B. Legitimate Aim and Necessity: Convenience Is Not Constitutionality.

The justification of facial recognition technology is a routine affair in the State, which appeals

[15] Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934, 1950–52 (2013).
[16] Justice K.S. Puttaswamy (Retd.), (2017) 10 S.C.C. 1, 325.

to the purposes of crime prevention, national security, and public safety. In the abstract, these objectives are certainly valid. Puttaswamy does not restrain the State to such pursuits. Nevertheless, the constitutional question does not conclude with legitimacy. The State should also show that the selected means are needed to attain the stated aim.

One standard required is necessity. It demands of the State to establish not only that a measure is efficient or useful, but that it is necessary that there are no other alternatives equally efficient or useful which are less obtrusive.[17] This has not been relieved in the case of NAFRS. No publicly available information has shown that facial recognition is a major game changer in terms of the rise in conviction rates, better investigations, and the functions it cannot execute through less intrusion processes, like directed surveillance, warrants, fingerprints, or the old methods of investigation.

It is constitutionally important that there are no published impact assessments, accuracy audits, or cost-benefit analyses. Devoid of such evidence, facial recognition stands to be adopted due to fact that it is the technology that is attractive and not necessary, constitutionally Puttaswamy specifically warns against this type of technological determinism by reminding that the State should not be allowed to infringe rights simply because it is innovative or more economical in its administration.

C. Proportionality and Minimal Impairment.

Although there is a legitimate aim, Puttaswamy necessitates that the means used should be proportionate. This involves a balancing act where the extent of violation of rights is compensated with the gains that the State states, and whether the action minimally affects the fundamental rights or not.

The facial recognition technology presents an exceptionally intense intrusion. In contrast to episodic surveillance, NAFRS can provide uninterrupted surveillance of people within the open areas, most of the time without suspicion, notice, or consent. The magnitude of possible data gathering is huge as it involves not only suspects but regular citizens as well as the citizens who are involved in lawful activities. This dragnet-like structure is in stark contrast to the targeted surveillance designs that have always been related to constitutional policing.[18]

There are a number of reasons that make NAFRS disproportional. First, there is no well-defined

[17] Takshashila Institution, AI-Based Facial Recognition in Policing 18–20 (2025).
[18] S. & Marper v. United Kingdom, 2008 Eur. Ct. H.R. 1581.

boundary of data storage, and biometric data can be stored indefinitely. Second, the secondary use is not prohibited by any statute, which leads to the risk of the possibility of data being used in other purposes. Third, the lack of a previous judicial approval implies that the decisions regarding deployment are put at the discretion of the police, which negatively affects the principle of independent control.

D. Article 14, Equality, Algorithmic Bias.

Privacy cannot be limited to the proportionality analysis. Facial recognition technologies pose a grave concern as well regarding Article 14 that provides equality before the law as well as the absence of arbitrary action of the state. Facial recognition systems have been recorded to had increased rates of errors when it comes to women, darker skinned and other marginalised people with empirical studies made across the world.[19] These prejudices have very serious consequences in a society where social stratification is strong.

Errors do not exist in the abstract form when police implement biased technologies. These become wrongful suspicion, more police interactions, and disproportionate policing of already vulnerable populations. These results constitute indirect discrimination as a facially neutral technology would have disproportionate and unfair results. This increases the privacy violativeness as it consolidates exclusion and marginalisation trends.

The constitutional issue then is two-fold: NAFRS does not just invade privacy, but the way it does so is potentially dangerous, in strengthening structural inequality. Even Puttaswamy, acknowledged the fact that, privacy is bound up with dignity and equality. Any surveillance system that unfairly puts a strain on a group of people goes against all three values at the same time.

V. INSTITUTIONAL CAPACITY, ACCOUNTABILITY DEFICITS, AND COMPARATIVE PERSPECTIVES

A. Lack of Accountability when using Facial Recognition by Police.

The constitutional drawbacks that have been found in the use of NAFRS are not just the doctrinal flaws; these weaknesses are entrenched in the institutional flaws in the administration of policing in India. Surveillance technologies enhance power inequalities between the police and the citizen. In the context of a weak institutional accountability system, these technologies

[19] Joy Buolamwini & Timnit Gebru, *Gender Shades*, 81 Proc. Mach. Learning Res. 1 (2018).

are prone to deepening arbitrary and in transparent modes of state power. With NAFRS, the lack of accountability is structural and systemic.

Currently, police use of facial recognition systems, in terms of real-time or retrospective searches, does not have any prerequisite of a prior judicial authorisation.[20] The choices on deployments, inclusion of the database and search parameters are all left at the mercy of internal discretion of the police. This is a sharp contrast to constitutional guidelines on other proactive investigative methods, including search and seizure, monitoring of communications or intercepting communications, or detention in custody, all of which are not only open to judicial control but at least formally so. Facial recognition surveillance lacks ex ante control, which eliminates a crucial constitutional protection against abuse.

As problematic, is the absence of ex post transparency and review. No publicly enforced system of recording facial recognition searches, no requirement to publicly release aggregate use, and no mechanism of independent audit to determine accuracy, bias, or adherence to intended purpose exists. Those who are victims to facial recognition surveillance are not notified and given any significant chance to dispute their presence in databases or challenge false matches. The remedies, when they exist, on the issue of wrongful identification are only indirect and cumbersome, based on general constitutional litigation as opposed to specific statutory rights.

B. Police Institutional Capacity and Survey Surveillance and Role Risk.

The threats of NAFRS are combined with ongoing problems of institutional capacity of police. The issue of lack of training, resources and internal accountability has been a long time problem of the Indian policing. Examples of problems that have been recorded in reports of policing practices include overuse of discretion, political influence, custodial violence, and poor levels of public trust. The emergence of the potent surveillance technologies, in which strong protection measures are not provided, is particularly disturbing in such an environment.

Not only technical competence is necessary with facial recognition systems, but also normative training, an awareness of the constitutional restraint, the requirements of data protection, and the morality of surveillance. It is scarcely evident that police officers who use NAFRS are systematically trained on these fronts. In its place, the dependence on both vendors and technical personnel is putting the processes at risk of outsourcing significant constitutional decisions to non-transparent algorithms and proprietary systems.

[20] R (Bridges) v. Chief Constable of South Wales Police, [2020] EWCA Civ 1058 (U.K.).

Additionally, the political economy of policing increases risks of abuse. The surveillance technologies may serve as desirable means of monitoring dissent, dealing with protests, or carrying out informal social control especially in politically sensitive situations. Facial recognition systems are a system of governance and not law enforcement where institutional incentives hinge on adherence to the executive priorities at the expense of constitutional restraint. It is also a dynamic that is reinforced by the absence of external checks, and constitutional compliance relies on an internal admonition, and not a binding law.

C. Comparative Facial Recognition Policing Regulation.

The experience of other countries should be used to understand how constitutional democracies have addressed the problems of facial recognition in law enforcement. Though none of the jurisdictions has resolved the problems with flawlessness, there are several that noted the unusual dangers presented by biometric surveillance and reacted by implementing stricter regulatory measures than those that exist currently in India.

The biometric data is considered a special category of sensitive personal data that is given increased protection in the European Union.[21] Facial recognition by the police is strictly regulated and must be authorised by the law, restricted in purpose, and strongly controlled. Recent regulatory efforts point out that even where real-time biometric identification in the open areas is allowed, it should be done in a very limited set of situations where the crime is serious and even in that case it must be pre-authorised and heavily guarded.

This case of United Kingdom is another one to learn. Police live facial recognition has been subject to judicial review by courts and has been stressing the necessity, proportionality and operational safeguards on the real deployments. Data protection authorities provide regulatory guidance, that the police forces must carry out the impact assessment, use the deployment in reference to the particular objectives, and be transparent about the precision and bias. The judicial intervention has been a key factor in the formation of these restrictions.

In the US, the situation is more disjointed, though a number of states and cities have implemented a ban or a moratorium on police facial recognition, with many fearing inaccuracy, discrimination, and civil liberties.[22] Biometric privacy laws have also restricted unregulated use through litigation against biometric privacy laws, which has expressed judicial discomfort

[21] Regulation (EU) 2016/679, arts. 9–10 (General Data Protection Regulation).
[22] Jennifer Lynch, *Face Recognition Moratoria*, Elec. Frontier Found. (2020).

in the naturalisation of biometric surveillance.

D. Lessons for India

The comparative chart highlights a mutual constitutional hunch: facial recognition policing is not similar to regular methods of investigation and, thus, requires extraordinary treatment through regulation. There are a number of principles that come out. To start with, the law should be clear; executive discretion should not replace democratically promoted constraints. Second, tailoring needs to be such that facial recognition is only applied to major crimes and particular situations and not as a general surveillance tool. Third, one must have an independent control either in the form of courts or in the form of regulators or both to ensure misuse is avoided and people have trust. Lastly, there need to be transparency and accountability systems such as audits and remedies to convert constitutional promises into reality.

VI. CONCLUSION AND RECOMMENDATIONS

The paper has analysed the application of facial recognition technology in Indian policing within the context of the constitutional doctrine, institutional capacity and comparative practice. This analysis shows that the National Automated Facial Recognition System works in a constitutional grey zone, which is characterised by a wide range of surveillance potential and a low legal limit. Although the judgment made in the Justice K.S. Puttaswamy (Retd.) was transformative Police-operated facial recognition has never had any significant constitutional examination, even though the constitution was created to provide a strict infrastructure of restraining state action infringements on privacy.

Using Puttaswamy test shows structural and consistent gaps. NAFRS does not have a clear statutory underlying as enacted by Parliament and hence cannot pass the test of legality. Arguments of necessity are not substantiated, but are based on assumptions of efficiency instead of being based on the data of indispensability. The extent, continuity and density of facial recognition policing bring about disproportionate encroachment upon privacy and the risks of algorithmic bias recorded present a problem on their own in the context of Article 14. Poor accountability of institutions, insufficient training, and lack of independent control cause these failures to be amplified.

More importantly, the constitutional problem of NAFRS is neither accidental nor transitional. It represents a larger trend where policing capability grows on an executive level, and the legal and institutional restrictions are falling behind. Facial recognition so is symbolic of an even

larger governance failure:[23] the failure of current legal structures to place technologically empowered state power into some form of discipline.

B. Normative Position

On the constitutional level, the fact that NAFRS remains in its current form is hard to rationalize. In cases where a surveillance system is found to have failed all tests of the proportionality test and to have systemic dangers to privacy, equality and democratic freedom, constitutional fidelity requires restraint. The paper will take a stand in favour of the India side, i.e. India is in a normative dilemma of either imposing a temporary police use of facial recognition moratorium until an amendable constitutional framework is established, or to radically reform the surveillance governance system based on rights-centred governance.

Constitutional supremacy cannot be forced out by technological inevitability. Police legitimacy in a constitutional democracy is not based on efficiency itself, but instead on legality to legal boundaries that ensure individual dignity and autonomy.

C. Recommendations

Legislative Measures

- Give clear statutory permission concerning the use of facial recognition with clear purposes.
- Limit implementation to limited and well defined situations e.g. serious offence investigation or missing persons.
- Requirement of prior judicial permission of real-time or massive deployments.
- Bring about rigorous data minimisation, retention and purpose-limitation policies.
- Insist on the accuracy, bias and system performance to be independently audited.
- Instead, create individual rights that are enforceable such as the right to access, right to correct, right to delete, and right to compensation in case of wrong identification.

Judicial Intervention

- Considering facial recognition systems as the subject of Puttaswamy proportionality in future and upcoming litigation.
- Formulating regulations that would regulate the admissibility and reliability of evidence created by facial recognition.

[23] David Lyon, *Surveillance, Snowden, and Big Data*, 30 Big Data & Soc'y 1, 6–7 (2015).

- Making the State prove need and proportionality using empirical evidence, but not abstract claims.

Administrative Reform and Institutional Reform.

- At the level of the policing institution, there is a need to take immediate measures to bring the practice in line with the constitutional norms:
- Introduction of comprehensive standard operating procedures of the use of facial recognition.
- Compulsory education on police rights and data protection as well as surveillance ethics.
- Similar to the release of reports on transparency, the extent and frequency of facial recognition implementations should be published.
- Establishment of internal compliance departments with the responsibility of tracking effects and addressing complaints.