FACIAL RECOGNITION AND THE RIGHT TO PRIVACY: LEGAL AND ETHICAL CONCERNS IN INDIA

K. Reddemma Choudary, Mahindra University

ABSTRACT

Facial Recognition Technology (FRT) is significantly evolving and is being used across various sectors in India, but there is an absence of a legal framework and it is largely unregulated by specific legislation. This Article examines the legal grey area surrounding Facial Recognition Technology in India's current legal framework and also examines ethical and legal risks associated with FRT and its severe misuse in India, including a case study of Digi Yatra. Using Puttaswamy Judgement, this article critiques FRT's Failure to meet the threshold requirement given by the Supreme Court and this article highlights the design and rights-based risk of FRT, including Purpose creep, bias and misuse of data.

Introduction

'Facial Recognition Technology' has become more and more predominant in our culture as technology developed over time. We have transitioned from a period where we require a high quality and expensive camera with an experienced photographer to take a single photo to a point where any layperson can take a photo such was the development we have witnessed. As Albert Einstein once said ***'It has become appallingly obvious that our technology has exceeded our humanity'***[1]

Technology has evolved from using a camera for the purpose of capturing a memory to utilizing it as a massive surveillance tool and Facial Recognition Technology (or) FRT is the offshoot of this and one of the most influential surveillance tools ever made in the history of mankind. As with all inventions one has to analyze its positive and negative aspects and its effect on society as a whole.

In the Current Technological Era FRT has embedded itself in every aspect of a person's life from using it to unlock smartphones, identify criminals and suspected persons who are involved in criminal activities and law enforcement widely across the world use this software to combat and prevent criminal activity and these are the few practical applications of Facial Recognition Technology.[2]

C.P Snow in a New York Times Essay(1985) has characterised Technology as ***'Technology... is a queer thing. It brings you great gifts with one hand, and it stabs you in the back with the other.***[3]***'***

On December 22 ,2019 Delhi Police have used The 'Automated Facial Recognition' computer software which was fitted for the specific purpose of identifying missing children was used to screen masses during Prime Minister Narendra Modi's rally giving rise to severe concerns

[1] Albert Einstein, Letter to Heinrich Zangger (Dec. 1917), *in* 8 Albert Einstein: The Collected Papers of Albert Einstein 412 (John Stachel & Martin J. Klein eds., 1998).
[2] 'Nat'l Acad. of Scis., Eng'g & Med., Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance, Ch. 3, at 67 (2024), https://nap.nationalacademies.org/read/27397/chapter/5#67
[3] C.P. Snow, *Technology… Is a Queer Thing*, N.Y. Times, Mar. 15, 1971, https://www.physics.udel.edu/~watson/scen103/quotes.html.

about privacy and mass surveillance[4].

How Facial Recognition Technology Works

'Facial Recognition' is a expertise which is proficient of corresponding a human face from photos or videos against a database which has access to such digital information to confirm an individual's identity. It singles out distinguishing features of a person's face and runs it against the faces already logged in a database and with the advent of technological development of 21st century and growing use of sharing images and videos in social media and internet[5]. FRT is becoming the primary tool for law enforcement to identify people of interest and its use is not limited to law implementation. The use of 'FRT' is used in everyday aspects of a person's life from speeding up identity checks in airports and border crossings to being used in high traffic areas during music festivals and political rallies[6].

The FRT Operates with three specific functional goals in mind i.e Face detection , Feature extraction and Face Recognition[7] FRT functions through identifying a person by extracting their image and running it against a facial database this type of operational function requires an environment where FRT programs are trained using various large datasets often using AI as an intermediary[8].

While FRT has made life easier and provides various range of benefits in all aspects of society one has to understand that it is a double edge sword with such biometric information in the

[4] Al Jazeera, *Privacy Fears as India Police Use Facial Recognition at Rally*, Dec. 30, 2019, https://www.aljazeera.com/news/2019/12/30/privacy-fears-as-india-police-use-facial-recognition-at-rally (last visited June 13, 2025).

[5] Innovatrics, *Facial Recognition Technology: Face Recognition is a Technology Because of Its Contactless Nature*, Innovatrics (last visited June 14, 2025), https://www.innovatrics.com/facial-recognition-technology/#:~:text=Facial%20recognition%20is%20a%20technology,because%20of%20its%20contactless%20nature.

[6] Nat'l Acad. of Scis., Eng'g & Med., Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance, ch. 3, at 66 (2024), https://nap.nationalacademies.org/read/27397/chapter/5#66'

[7] 'Anwarul, Shahina & Susheela Dahiya, *A Comprehensive Review on Face Recognition Methods and Factors Affecting Facial Recognition Accuracy, in Proceedings of ICRIC 2019*, in 597 Lecture Notes in Electrical Engineering 495, 495–514 (P.K. Singh et al. eds., Springer Cham 2020), https://doi.org/10.1007/978-3-030-29407-6_36

[8] P. Vedavalli et al., Facial Recognition Technology in Law Enforcement in India: Concerns and Solutions, Data Governance Network, Working Paper No. 16 (2021), https://www.datagovernance.org/report/facial-recognition-technology-in-law-enforcement-in-india-concerns-and-solutions.'

hands of the law enforcement, government and private corporations and entities will always give rise to concerns of surveillance ,privacy concerns and also risk of data security.

Facial Recognition Technology and the Need for Legal Regulation in India

Currently as of 2025 there is no precise law leading usage of the 'Facial Recognition Technology' and absence of such legal framework has the potential for the technology to be misused and this can lead to devastating consequences as FRT can be used for collective observation, racial outlining, data misuse and such powerful technology needs to regulated by a legal framework in order to address the privacy and data protection concerns.

According to the Supreme Court Judgement in '**Justice K.S.Puttaswamy(Retd) vs Union Of India 2019 (1) SCC 1'** the supreme court has stated that to justify encroachment by state into people's 'right to privacy' which is safeguarded under 'article 21' of the indian constitution the state must fulfil certain threshold and they are as follows:

(i) The primary prerequisite that there must be a law in being to defend an infringement on privacy is an fast obligation of 'Article 21.'

No one may be destituted of life or individual freedom excepting via the method prescribed by law. The presence of law is a fundamental need.

(ii) The Second Requirement necessitates a legitimate State objective to ensure that the form and substance of the statute imposing the limitation align with the reasonableness standard demanded by Article 14, which serves as a safeguard against uninformed State act. The chase of a authentic state focus guarantees that the legislation is free from evident capriciousness.

(iii) The third criteria mandates that the methods used by the legislature be commensurate with the objectives and necessities intended to be addressed by the legislation. Proportion is a crucial element of the safeguard against uninformed State action, as it assures that the kind and extent of the infringement on the right is commensurate with the objective of the legislation.[9]

As we can observe from the three threshold requirements put forth by the supreme court in the 'puttaswamy judgement' the use of FRT does not satisfy the three requirements. Firstly there

[9] 'Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1, ¶ 310 (India).

is no legal framework surrounding FRT and executive discretion is not enough there must be a proper statute to defend such infringement of privacy. Furthermore FRT must be used for a specific purpose such as preventing terrorism and locating missing children and such tool should not be used based on the invocation of broad and vague contention that it is used for **'National Security' and 'Public Safety'** the use of such powerful tools must be with a clear and specified purpose. In the case of 'Sadhan Haldar Vs NCT of Delhi'[10] the delhi high court authorised the use of 'Facial Recognition Technology' only for the specific purpose of locating missing children however later it was found that the delhi police used such software during Prime Minister Narendra Modi Ramlila Maidan Rally to screen the crowd raising privacy related concerns[11]. Thirdly the methods adopted must be relative to object and requirements wanted to be contented by law which means that the use of FRT should not be more intrusive than necessary and should not be disproportionate to the purpose of the law.

Risks Associated With Facial Recognition Technology

Facial Recognition Technology has various associated risks ranging from Design based risk to Rights based challenges.

The Practical use of FRT especially by public authorities gives rise to ethical concerns in regards to use of FRT.

The Design Based Risk includes the concept of inaccuracies of FRT due to intrinsic factors such as 'facial expression, aging, plastic surgery' and disfigurement and extrinsic features such as quality of image, illumination and pose variation these factors gives rise to inaccuracies in the usage of facial recognition. 'Facial Recognition Technology' has often resulted the risk of displaying biases due to its lack of training data particularly it has proven to show error in color based error based on skin tone Similarly, studies have shown that 'FRT systems' in India have indicated mistake rate based on its proof of identity of Indian men and women and such biases are becoming more prevalent when FRT Systems are imported as such imported system rely on categories that are suitable in the context and with India being a diversified country with various different communities having diverse physical and facial features in such cases there

[10] Sadhan Haldar v. State (NCT of Delhi), W.P. (Crl.) 1560/2017, ¶ 12 (Del. HC Jan. 22, 2019).

[11] Al Jazeera*, Privacy Fears as India Police Use Facial Recognition at Rally*, Dec. 30, 2019, https://www.aljazeera.com/news/2019/12/30/privacy-fears-as-india-police-use-facial-recognition-at-rally (visited June 14, 2025).'

is a need for possessing pan india database of 'facial information and biometrics' which is essential to create a robust FRT system. There exists a security risk of hacking due to the companies that develop or deploy FRT systems as they possess a significant amount of facial data. One of the significant Rights based challenges in the realm of FRT is that often facial images and data composed for one aim are often used for another drive and the individual having assented to giving his facial data for the initial purpose in most of the cases is not aware of its subsequent use and this raises the concern often known as Purpose creep[12].

The Use of FRT requires training using AI and usually it is proficient on data circles of pictures and these data sets are obtained by rasping the internet to gather pictures of faces without the consent of the possessor such practice technically not considered violative of any statute or law however gives rise to ethical concerns of such practice[13].

Case Study - Digi Yatra

Digi Yatra is an ingenuity by the 'Government of India', under the 'Ministry of Civil Aviation', aimed at facilitating a seamless journey for air passengers through the use of a single token of facial biometrics to digitally authenticate uniqueness and any other necessary data for air travel. Digi Yatra asserts that data is safeguarded using a dispersed ledger, establishing a decentralised coating of trust among the ecosystem's numerous members.**[14]**

The New Indian Express in its article have claimed that the data of air passengers using digi yatra has been shared with the income tax department and such data is being used to identify tax evaders and those who under report their taxes[15] even though CEO of Digi Yatra and Income tax have denied such claims as baseless and false allegations this controversy however has reignited the concerns regarding data protection and data governance in India

[12]'NITI Aayog, Responsible AI for All: Adopting the Framework – A Use Case Approach on Facial Recognition Technology, Discussion Paper 3, at 19–22 (Nov. 2022), https://www.niti.gov.in/sites/default/files/2022-11/Ai_for_All_2022_02112022_0.pdf.'

[13] 'William Crumpler & Ainikki Riikonen, *Facial Recognition Technology: Responsible Use Principles and the Legislative Landscape*, Ctr. for Strategic & Int'l Stud. (Apr. 7, 2021), https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscae.

[14] DigiYatra Foundation*, Re-imagining Airport Experiences, DigiYatra Foundation* (last visited June 14, 2025), https://digiyatrafoundation.com/

[15] Dipak Mondal, *Tax Department to Tap Digi Yatra Data to Go After Evaders*, New Indian Express (Dec. 30, 2024), https://www.newindianexpress.com/nation/2024/Dec/30/tax-department-to-tap-digi-yatra-data-to-go-after-evaders (last visited June 14, 2025).'

The Data related concerns with the use of Digi Yatra has been addressed in 'Niti Ayog Discussion Paper: Responsible AI for All | Adopting the Framework: A Use Case Approach on Facial Recognition Technology':

The Digi Yatra must clearly state in their policy that facial biometrics are deleted from airport's database 24 hours after the departure of passenger.

The Digi Yatra with the consent of the user may share the data with cab operatives and added marketable objects however steps must be taken to safeguard that such accord is evocatively providing and is not hurried by defaulting.

The Digi Yatra Central Ecosystem must be secured with robust and state of the art security system as they possess sensitive personal data such as facial biometrics as such security practices are clearly mentioned under Rule 7 of the SDPI Rules.

With Such Sensitive Data there arises a need for frequent cybersecurity audits and vulnerability testing to ensure information security[16].

Conclusion

Facial Recognition Technology (FRT) is evolving with every passing day and the lack of legal framework and safeguards in India where due to such absence has given rise to the misuse of such massive surveillance tool like in Delhi where the police using it for Screening People in a Political Rally despite the order of the high court authorising its use however limited to locating missing children such blatant violation poses significant risk to privacy and civil liberties which was upheld in Puttaswamy Judgement where it has given thresholds which need to be fulfilled when encroaching privacy[17]. Without a legal framework FRT risks becoming a massive surveillance tool and India is currently in need of a legislation which ensures FRT is used ethically and transparently.

[16] 'NITI Aayog, Responsible AI for All: Adopting the Framework – A Use Case Approach on Facial Recognition Technology, Discussion Paper 3, at 32–33 (Nov. 2022), https://www.niti.gov.in/sites/default/files/2022-11/Ai_for_All_2022_02112022_0.pdf.
[17] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1, ¶ 310 (India).'