VOLUME 4 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

# PRIVACY VS SECURITY: BALANCING NATIONAL SECURITY CONCERNS WITH AI-POWERED FACIAL RECOGNITION IN COURT

- Janet Treesa P.G. & Krishnanunni J[1]

## Abstract

The burgeoning advancements in Artificial Intelligence (AI) have fueled the widespread adoption of facial recognition technology (FRT) within law enforcement and national security domains. In the justice system, AI-powered FRT has been used in various ways, such as identifying suspects in criminal investigations, enhancing security in courtrooms, and even as evidence in court. This research paper delves into the intricate balance between individual privacy rights and the security concerns surrounding the utilisation of AI-powered FRT within the justice system. The analysis extends to explore public perception and trust in FRT. Data, analysis, and information are meticulously drawn from a wide range of credible sources, including academic journals, research papers, and relevant statistics, ensuring the thoroughness and validity of the findings. The paper critically examines existing FRT systems, employing a discourse analysis that acknowledges their complexity. It pinpoints shortcomings and obstacles that hinder public acceptance. The study further explores the potential risks of discrimination and bias within facial recognition algorithms, emphasising the need to mitigate these flaws to guarantee just and equal outcomes in legal settings. Public opinion of and trust in FRT are also considered, highlighting the long-term social ramifications of its extensive use in courtrooms. Subsequently, the paper proposes formulating ethical and legal frameworks to navigate the complex interplay between security concerns and individual privacy rights in AI-powered FRT. It presents conclusions about usingFRT as evidence in court, promoting openness, accountability, and the defence of individual

[1] Students at Christ University Bangalore

rights. This research aspires to comprehensively understand this critical issue, offering valuable insights for policymakers, legal professionals, and the general public.

**Keywords:** Facial Recognition Technology (FRT), Privacy Rights, Security, National Security, Artificial Intelligence (AI)

## Introduction

Facial recognition is a biometric technique that uses statistical analysis and algorithmic projections to identify and evaluate faces. Once these facial recognition systems catch a recording of a person's face, through computer vision programming, they collect data points and create a facial data map, which is distinct and unique to each person.[2] The utilisation of this technology in various domains and networks has become increasingly widespread, resulting in exceptional tracking of data providers when paired with GPS information. A facial recognition technology system usually consists of four fundamental components: a camera to take an image, an algorithm to build a faceprint, a database of recorded photographs, and an algorithm to compare the captured picture to the database of photos or a single picture in the database.[3] Biometrics is a process through which data is extracted from the human body, converting our unique biological traits into measurable metrics. Facial recognition is a critical element of this process, which can involve verifying, identifying, or classifying a face.

India has increasingly embraced the implementation of facial recognition systems in surveillance technology, with 126 FRT systems deployed throughout the country as of June 2023, with a spending of INR 1,499.41 crores.[4] As per the report of Grand Review Research, in 2022, the global facial recognition market size was USD 5.15 billion, and it is projected to experience a 14.9% compound annual growth rate from 2023 to 2030.[5] In India, there are sixteen different FRT systems set up by the central and state government, which looks after security and identity

[2] Afzal Godil, Sandy Ressler and Patrick Grother, *Face Recognition using 3D Facial Shape and Color Map Information*, NAT. INS. OF STANDARD AND TECH

[3] *Right To Privacy & Facial Recognition Technology: Who's Spying On You*, IJLLR, Dec 14, 2021 https://www.ijllr.com/post/right-to-privacy-facial-recognition-technology-who-s-spying-on-you

[4] *Smart cameras to be set up in Lucknow to track facial expression of women in distress, alert police*, SCROLL.IN (Jan 21st, 2021).

[5] *Facial Recognition Market Size, Share & Trends Analysis Report By Technology (2D, 3D, Facial Analytics), By Application (Access Control, Security & Surveillance), By End-use, By Region, And Segment Forecasts, 2023 - 2030*, Grand Review Research

across the country.[6] However, using artificial intelligence (AI) and its various applications has generated considerable controversy surrounding privacy and security, particularly in India, where AI-powered facial recognition technology (FRT) is employed. This technology, which relies on AI algorithms to identify and authenticate individuals based on their facial features, is increasingly utilised for national security objectives, such as law enforcement and border control. Its implementation raises crucial concerns about privacy, civil liberties, transparency, accountability, and the discrimination inherent in AI systems.[7] Also, errors and inaccuracies may arise in facial recognition, and the results may not always be definitive or precise, as per the European Union Agency for Fundamental Rights (FRA). These data can also be socially biased, and facial recognition may infringe on an individual's ability to seek justice. Indian courts and policymakers must address this pressing issue with care and consideration, considering these competing interests. In light of the implementation of AI-powered FRT, this research article examines the conflict between the augmentation of security measures and the protection of privacy rights in the Indian court system.

## Current Applications of FRT in National Security

The current applications of FRT in national security are innumerable. These functions include military, health, surveillance in public spaces, cybersecurity, law enforcement, and more. Facial recognition technology (FRT) aims to identify, classify, verify, and potentially neutralise perceived threats when deployed in military operations and security contexts. AI systems are being developed for various military and intelligence applications, including intelligence gathering, logistics management, cyber operations, command and control, and control of autonomous vehicles and weapon systems. The goal is to enhance capabilities through AI and automation across domains critical to modern warfare. The 2018 U.S. National Defense Strategy identified AI as a key technology for maintaining military superiority, highlighting it as a strategic capability for prevailing in future conflicts[8]. Ukraine's defence ministry has leveraged Clearview AI's facial recognition to identify Russian assailants, counter misinformation, identify

[6] Cameron Martin, *Facial Recognition in Law Enforcement*, 19 Seattle J. Soc. Just. 309 (2020)

[7] Utegen D., RakhmetovB.Zh., *Facial Recognition Technology and Ensuring Security of Biometric Data: Comparative Analysis of Legal Regulation Models*, Journal of Digital Technologies and Law. 2023;1(3):825-844.

[8] Department of Defense, *Summary of the 2018 National Defense Strategy*, p.3, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

casualties, and vet individuals, demonstrating AI's practical applications.[9] The recent coronation of King Charles III served as a prominent instance where facial recognition technology was employed to surveil the assembled crowd.[10] This technology has also found applications in monitoring refugee populations and identifying deceased individuals amidst the ongoing conflict in Ukraine.[11] Its usage spans high-profile events and humanitarian and military efforts, reflecting the increasing prevalence and varied implementation of facial recognition systems. However, bias, lack of diversity, and inaccurate recognition in these AI systems remain concerns that need to be addressed for their responsible and ethical deployment in high-stakes national security contexts.

The facial recognition software initially intended to identifyauthorised personnel can be adapted for broader military applications beyond facial recognition alone. It can be configured to recognise ships, electronic warfare signals, and other emitters while flagging unknown faces not in its database and alerting personnel about unauthorised individuals. This ability to automatically detect unidentified entities, signals, and threats makes the software a valuable intelligence and security asset in active combat zones. These advanced FRT systems analyse more than just facial mapping; they also track body language, gait, and emotions and predict future movements. The widespread deployment of FRT-enabled CCTV cameras across India allows authorities to monitor and track individuals extensively, granting enhanced tracking capabilities throughout the country.

Concerning the health industry, FRT offers accessibility advantages by enabling people with visual impairments or conditions like Alzheimer's to identify individuals, enhancing their independence and social connections through applications like Microsoft's Project Tokyo

[9] Paresh Dave & Jeffrey Dastin, *Ukraine has started using Clearview AI's facial recognition during war*, Mar 15, 2022, https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/

[10] Vikram Dodd, *Police accused over use of facial recognition at King Charles's coronation,*The Guardian, May 3 2023, https://www.theguardian.com/uk-news/2023/may/03/metropolitan-police-live-facial-recognition-in-crowds-at-king-charles-coronation

[11] Felipe Romero, *Facial recognition technology: how it's being used in Ukraine and why it's still so controversial*, The Conversation, June 14, 2022, https://theconversation.com/facial-recognition-technology-how-its-being-used-in-ukraine-and-why-its-still-so-controversial-183171

headset.[12]FRT also finds applications in healthcare, such as the Polish Ministry of Digitalization's app that uses geolocation and facial recognition to remotely monitor quarantine compliance, reducing the need for physical home visits.[13] Studies have demonstrated the accuracy of FRT mobile apps in identifying paediatric patients, even when unconscious, streamlining verification processes.[14] Companies like ALCHERA leverage FRT to automate hospital admission/discharge, detect unusual patient activities, control access, and flag unauthorised entries.[15] Moreover, AI-powered FRT can detect early signs of diseases through subtle facial changes, identify emotional cues for mental health support, and aid remote patient monitoring, making healthcare more accessible through remote identification capabilities.

Facial recognition technology (FRT) is witnessing rapid global adoption, with 64 countries implementing it for public surveillance, tracking individuals, crime detection, and predicting social behaviours during crises.[16] It augments law enforcement through suspect identification, high-risk area monitoring, border control screening, and providing actionable intelligence.[17] For example, JARVIS software uses facial recognition to process and analyse extensive CCTV video recordings, extracting and synthesising relevant insights.[18] Beyond surveillance, FRT enables innovative attendance systems,[19] analysing interviews for behavioural competencies,[20] and healthcare applications like patient identification and monitoring. In India, the Bengaluru 'Safe City' initiative has deployed over 4,100 FRT-enabled CCTVs out of 7,000 planned,[21] while cities

[12] Microsoft, Project Tokyo, https://ai.org.tr/wp-content/uploads/2022/10/4-Canada-facial-Recognition-and-AI-1.pdf,

[13] Luca Montag et al., *The rise and rise of biometric mass surveillance in the EU*, A LEGAL ANALYSIS OF BIOMETRIC MASS SURVEILLANCE PRACTICES IN GERMANY, THE NETHERLANDS, AND POLAND https://edri.org/wp-content/uploads/2021/07/EDRI_RISE_REPORT.pdf (2021)

[14] Byoungjun Jeon et al., *A Facial Recognition Mobile App for Patient Safety and Biometric Identification: Design, Development, and Validation,* National Center for Biotechnology Information, 2019 Apr 8, https://pubmed.ncbi.nlm.nih.gov/30958275/

[15] *Facial Recognition in Healthcare: Unlocking Potential Medical Applications*, ALCHERA, August 14, 2023 https://alchera.ai/en/meet-alchera/blog/facial-recognition-in-healthcare-unlocking-potential-medical-applications

[16] P. Brey, *Ethical aspects of facial recognition systems in public places Info, Comm & Ethics in Society*, 2 (2004), pp. 97-109

[17] *Facial Recognition Technology (FRT)*, National Institute of Standards and Technology, February 6, 2020 https://www.nist.gov/speech-testimony/facial-recognition-technology-frt-0

[18] What is JARVIS?, https://www.staqu.com/what-is-jarvis/

[19] S. Sawhney, K. Kacker, S. Jain, S.N. Singh, R. Garg, *Real-time Smart attendance system using face recognition techniques*, Confluence, Jan. 1 2019.

[20] Y.S. Su, H.Y. Suen, K.E. Hung, *Predicting behavioral competencies automatically from facial expressions in real-time video-recorded interviews,* J Real-Time Image Proc, 18 (2021), pp. 1011-1021, 10.1007/s11554-021-01071-5

[21] Shyam Upadhyay, *Meet the Facial Recognition Giant Helping Bengaluru Police,* Analytics India, Mar. 28, 2023,

like Delhi[22], Jammu[23], and Andhra Pradesh[24] are also expanding FRT surveillance networks for enhanced monitoring and security across the country.

Law enforcement agencies extensively utilise facial recognition technology (FRT) for live facial recognition (LFR) capabilities, enabling real-time identification of individuals captured by CCTV camera networks[25]. This application, termed 'AFR Locate' by some police forces like South Wales Police, allows authorities to pinpoint and track people of interest through surveilled areas monitored by LFR systems. In India, FRT is implemented through AI-powered CCTV cameras, body-worn police cameras, drones in high-risk zones, and other means. It is deployed in high-footfall public spaces like bus stations, railway stations, marketplaces, and stadiums. The systems generate unique facial data maps for individuals, facilitating identification and tracking across the camera networks. Notably, Delhi Police are using Automated Facial Recognition Systems to identify and screen protesters against the Citizenship Amendment Act and National Register of Citizens. They are labelling them as "rabble-rousers and miscreants," showcasing FRT's current application in monitoring and suppressing dissent.[26] Also, Numerous airports now permit travellers to utilise their facial data as a virtual passport, bypassing lengthy security queues, check bags, and board flights without presenting physical identification or boarding passes. AI offers significant cybersecurity applications through anomaly detection, analysing large data sets, and adapting to evolving cyber threats. It enhances defences by automatically identifying suspicious activities, processing vast security data, and continuously learning to update protections against emerging threats in real time.

https://analyticsindiamag.com/meet-the-facial-recognition-giant-helping-bangalore-police/

[22] *Delhi Police Is Now Using Facial Recognition Software to Screen 'Habitual Protestors'*, The Wire, Dec 29, 2019 https://thewire.in/government/delhi-police-is-now-using-facial-recognition-software-to-screen-habitual-protestors

[23] Kamaljit Kaur Sandhu, *J&K Police steps up effort to get facial recognition technology in Srinagar to track down terrorists,* India Today, Oct 21, 2021, https://www.indiatoday.in/india/story/jammu-kashmir-police-effort-facial-recognition-technology-srinagar-terrorists-1867667-2021-10-21

[24] Syed Ahmed, *Andhra Pradesh Govt Plans to Adopt AI-Driven 'Smart Glasses' with Facial Recognition to Fight Crime*, 23 Nov 2019, https://www.news18.com/news/india/andhra-pradesh-govt-plans-to-adopt-ai-driven-smart-glasses-with-facial-recognition-to-fight-crime-2396391.html

[25] *ICO investigation into how the police use facial recognition technology in public places*, 31 October 2019 https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf

[26] supra note 22.

Facial recognition technology has significantly impacted Indian courts, revolutionising the way criminal identification and investigation are conducted. With facial recognition technology, Indian courts can accurately and quickly identify suspects or individuals involved in criminal cases. This has dramatically improved the efficiency of the judicial system, leading to quicker resolutions and reduced backlog of cases. Furthermore, facial recognition technology has also helped enhance the overall security in Indian courts. It preventsunauthorised access, ensuring that only authorised individuals are granted entry into the court premises. Facial recognition technology has been instrumental in reducing the risk of identity fraud and false impersonations in Indian courts.[27]Law enforcement agencies can quickly identify potential threats or unauthorised individuals by comparing the facial features of individuals entering the court premises with a database of known offenders or suspects. This has significantly enhanced the safety and security of the court environment, assuring both the court personnel and the general public.

## Effectiveness of AI- Powered Facial Recognition in Enhancing National Security within the Justice System

Integrating AI-driven facial recognition technology has become more prevalent in the court system's national security protocols. This technology holds promise for improving the detection and tracking of possible security threats. This technology's precision, capacity to handle large volumes of data, and incorporation of advanced machine-learning algorithms determineits effectiveness. In law enforcement, AI-driven facial recognition has been utilised for predictive policing, data analysis, and crime pattern identification, which can streamline investigative processes and contribute to proactive crime prevention.[28] Facial recognition system implementation is not without difficulties, though. Privacy, prejudice, and ethical concerns have been raised, highlighting the necessity of responsible AI deployment and open, moral

[27] *Delhi: Facial recognition system helps trace 3,000 missing children in 4 days: Delhi News - Times of India, https://timesofindia.indiatimes.com/city/delhi/delhi-facial-recognition-system-helps-trace-3000-missing-children-in-4-days/articleshow/63870129.cms*

[28] Lunhol O, Torhalo P., *Artificial Intelligence in Law Enforcement:current state and development prospects*, Proceedings of 10th Socratic Lectures 2024, 120-124

frameworks to direct law enforcement organisations.[29] The potential for misuse and errors in the system underscores the importance of continuous innovation and ethical responsibility in deploying these technologies.[30]

Analysing the challenges of FRT, we see that it is becoming an increasingly prominent issue in discussions about AI ethics and high-tech monitoring both in India and internationally. Any system that uses face mapping and sensitive biometric data to perform 1:1 verification tasks or 1:1 monitoring and identifying functions of persons is collectively referred to as FRT.[31] Here, the main points of contention appear to be the infringement of legal and constitutional rights, technological errors that provide unreliable results, and even issues with regulation or governance. The most apparentproblem is individual privacy. Informational privacy has been seen as a component of the fundamental right to life and liberty protected by the Indian Constitution since the Supreme Court of India's historic ruling in 2018.[32] This means a person can decide when, why, and how her personal information is processed or disseminated. Nevertheless, FRT's basic architecture breaches this informational autonomy as it uses complex, intelligent algorithms that are trained on large datasets and interfaces with government databases when used.Additionally, FRT's hazards and design defects might lead to erroneous results. Researchers have discovered that FRT algorithms frequently classify darker skin tones incorrectly and with prejudice, particularly in women[33]. In any discussion of AI ethics, accuracy and howspecific algorithms produce results are fundamental issues that must be addressed. But what makes the problem with FRT usage worse is the fallout when someone gets wrongfully

[29] Hälterlein, Jens, '*Facial Recognition in Law Enforcement*', in Christian Borch, and Juan Pablo Pardo-Guerra (eds), The Oxford Handbook of the Sociology of Machine Learning (online edn, Oxford Academic, 20 Nov. 2023)

[30] Santoso, W., Safitri, R. ., & Samidi, S., *Integration of Artificial Intelligence in Facial Recognition Systems for Software Security*, 8(2), 1208-1214, 2024

[31] Ameen Jauhar and Jai Vipra, *Addressing Constitutional Challenges in Use of Facial Recognition Technology by Indian Law Enforcement Agencies*, JURIST – Professional Commentary, February 11, 2022, https://www.jurist.org/commentary/2022/02/jauhar-vipra-FRT-constitutional-challenges-law-enforcement/.

[32] Justice K. S. Puttaswamy vs. Union of India,Writ Petition (Civil) No. 494 of 2012, (2017) 10 SCC 1

[33] Diego Celis and Meghana Rao.*Learning Facial Recognition Biases through VAE Latent Representations* Association for Computing Machinery New York, NY, United States, 15 October 2019

detained, accused, or even convicted[34]. Given the documented cases of improper arrests, such results are not implausible.

However, we cannot prevent this technology's use, as it provides many potential benefits to judges in various ways by improving the general judicial process, efficiency, accuracy and overall effectiveness.[35]One of the main benefits ofFRT is its ability to accelerate the delivery of justice. India is a vast nation, and it is observed that the adjudication of a criminal and civil trial often takes many years. As a consequence, there is ineffective and delayed justice. One solution to this problem is the implementation of FRT, which can be used to handle more cases faster, and thus, justice can be served to the citizens more quickly.[36]As per Mr. William E Gladstone, “Justice delayed is justice denied”. This system would benefit the country's citizens as they spend less time waiting for the court's decision, which will significantly impact their lives.”When we look into the facts as of 15 September 2021, there were around 4.5 crore pending cases across all courts in India, especially in the district and subordinate courts. In 2019, there were 3.3 crore pending cases; this shows that India has added 23 cases every minute to its pendency in the last two years. The total number of pending cases in the Supreme Court of India is 71411 as of 2nd August 2022, of which 56365 are civil matters and 15,076 are criminal matters". [37]The FRT system has the potential to serve as a decision support tool by providing judges with relevant information to aid in the process of decision-making.Using facial recognition technology (FRT), law enforcement can quickly identify suspects by matching their photographs to databases of known people. This effectiveness speeds up investigations, helps find missing people, and deters crime. The workload for investigators and court staff is lessened when the identification procedure is automated using FRT. It simplifies repetitive work so that human resources can concentrate on more intricate facets of court cases.Although these advantages exist, it's crucial to weigh them against privacy protections and deal with issues with bias and accuracy.

[34] *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance, 2024,* https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance

[35] Navneet Kaur , Manpreet Kaur. *Role of artificial intelligence in the Indian courts.*International Journal of Law, Policy and Social Review,Volume 6, Issue 1, 2024, Page No. 18

[36] Srivastava SK. AI for Improving Justice Delivery: International Scenario, Potential Applications & Way Forward for India. Informatica, 2023, 47(5

[37] *Judicial delay in india,* The Times of IndiaFEB 20, 2023https://timesofindia.indiatimes.com/readersblog/lawpedia/judicial-delay-in-india-50731/

## Legal Status of FRT in India with regards National Security

In India, the legal reputation of Facial Recognition Technology is subject to specific rules and considerations. While no particular legislation directly addresses facial recognition technology in India, its utilisation is governed by diverse laws and rules to shield people's privacy and rights. The primary regulation that governs the use of Facial Recognition Technology in India is the Information Technology Act of 2000. The Information Technology Rules, 2011, beneath the Act, lays down guidelines for the collection, storage, and use of private facts, along with biometric records together with facial images. In 2023, the Digital Personal Data Protection Act[38] was enacted to regulate the processing of individuals' digital personal data in a way that balances the right to protect one's data with the legitimate need to process such data for lawful purposes. It establishes rules and provisions governing matters related to digital personal data processing. Furthermore, the Right to Privacy, recognised as a fundamental right under the Indian Constitution, also plays a crucial role in determining the legality and permissible use of Facial Recognition Technology in India.[39]

Courts in India have recognised the capacity advantages of Facial Recognition Technology in investigations and complaints. In the New Delhi Missing Children Case, the police used FRT to pick out nearly 3000 missing youngsters within just four days.[40] The High Court of Delhi commissioned this trial run to hint and reunite missing children. FRT scans snapshots of kids reported missing and compares them in opposition to database images. When the shape is determined, authorities can discover and reunite the child with their circle of relatives. This rapid identity method drastically increased the chances of finding children lacking and brought a remedy to worried parents. This  Technology was also successfully used by the Delhi Police in the riot case to identify and capture people responsible for the violence. Police identified suspected offenders by matching photos from CCTV footage and a database of driving licence photos. The FRT system gathered data from multiple sources, such as voter identification cards

[38] Personal Data Protection Bill, Bill No. 373, Lok Sabha(2019), http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

[39] Vedavalli, P., Misra, P., Sippy, T., Durani, A., Sinha, N., & Sinha, V. (2021). Facial Recognition Technology in Law Enforcement in India: Concerns and Solutions. Data Governance Network Working Paper 16.

[40] *Delhi: Facial recognition system helps trace 3,000 missing children in 4 days*,The Times of India, Apr 22, 2018,https://timesofindia.indiatimes.com/city/delhi/delhi-facial-recognition-system-helps-trace-3000-missing-children-in-4-days/articleshow/63870129.cms

and official documents, without considering religious preferences. As a result, over 1,100 individuals were identified, aiding investigations into serious crimes such as murder and arson.[41] However, the Indian Courts also emphasise the need to make sure that facial recognition technology is utilised in a way consistent with constitutional ideas and privacy. This includes ensuring proper safeguards to prevent misuse or abuse of facial recognition technology, includingunauthorised surveillance or profiling[42].

A National Academy of Sciences study surveyed around 130 people from various Indian states and colleges.[43] The majority were aware of FRT, with 54.6% aware of the government's use, 30.8% only aware of it being used in phones, and the rest not familiar with the term. The survey also asked about legislation for FRT regulation, with 65.2% only knowing about the Right to Privacy, 18.3% about the IT Act, and 9.4% learning about the Digital Data Protection Bill. The survey also asked about data handling by the system, with 58.5% stating it is sold to other companies, 27.7% saying it is secured under the privacy policy, 5.4% stating only the government has access, and 8.5% not knowing. Most respondents believed the Digital Data Protection Bill would give them more control over their data, with 51.5% believing it would.

The judiciary plays a vital role in every country's justice administration. However, when it comes to the Indian judicial system, the situation is strenuous because of the nation's high population, which leads to a steady increase in the filing of lawsuits, which has put more strain on the legal system. One of the primary reasons why the court should resort to these measures of AI is the shortage of judges, and the pending ever-cumulative cases have been a burden on the judicial system. However, it is still unknown how to use the recently discovered field of artificial intelligence to solve this problem.[44]

## Right to Privacy in India

[41] *Over 1,000 Delhi Rioters Identified Using Facial Recognition Software*.https://thewire.in/tech/over-1000-delhi-rioters-identified-using-facial-recognition-software-amit-shah

[42] National Academies of Sciences, Engineering, and Medicine. 2024. *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance.* Washington, DC: The National Academies Press.

[43] National Academies of Sciences, Engineering, and Medicine. 2024. Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance. Washington, DC: The National Academies Press. https://doi.org/10.17226/27397.

[44] Jain P. *Artificial Intelligence for sustainable and effective justice delivery in India*. OIDA International Journal of Sustainable Development,2018:11(06):63- 70

One significant concern FRT is the violation of the right to privacy. The laws of India, apart from the Personal Data Protection Bill, that regulate this technology are minimal. Some of the other Indian laws that regulate the privacy of its citizens are Section 43(A) of the IT Act 2000[45] Article 72A provides the conditions for compensation if there is any failure to protect the data. There have also been several cases and judgments that deal with privacy. In the landmark case of Justice K. S. Puttaswamy  vs. Union of India[46], Supreme Court of India laid down the contours of the right to privacy. The judgement established that the right to privacy is a fundamental right that includes autonomy over personal decisions, bodily integrity and the protection of personal information. The judgement laid down a proportionality test that the court established. The test contained three main aspects: the procedure established by law, reasonable classification and proportional benefit.

In 2019, NCRB took the initiative to establish Automatic Facial Recognition Systems (AFRS) in India throughout numerous sectors, such as regulation enforcement, transportation, and retail[47]. These systems use advanced algorithms to investigate and pick out human faces in photos and video feeds, aiding in protection and operational efficiency. In regulation enforcement, AFRS is used for criminal identity, tracking lacking individuals, and enhancing surveillance talents. Airports and public transport structures utilise facial popularity for streamlined passenger processing and protection tests. Despite its blessings, implementingAFRS in India raises significant privacy and ethical concerns, prompting robust regulatory frameworks and records protection measures to ensure accountable and transparent use.

While the AFRS system would be by the procedure established by law should the Personal Data Protection Bill be passed, without it, there is currently no anchoring legislation for the AFRS. This means that the AFRS would be active all over the country, and every citizen of India would fall under its purview. The AFRS does mention that the intended targets of the system are

[45] THE INFORMATION TECHNOLOGY ACT (2000), Act No. 21, Lok Sabha(2000), https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf

[46] *supra* note 32.

[47] *Request For Proposal To procure National Automated Facial Recognition System (AFRS)*, NCRB,2019, http://ncrb.gov.in/TENDERS/AFRS/RFP_NAFRS.pdf

“criminals, missing children/persons, unidentified dead bodies and unknown traced children/persons.” However, as the Supreme Court stated in the above case, sweeping provisions that target every person in the country cannot be implemented to prevent crime. “As a result, the AFRS system also fails the reasonable classification test because no differentiation is provided”.[48] The system is also stated to have identification capabilities, meaning that the government would have to collect sensitive data and enrol it in the recognition system to make it work. Data collection at this scale would not be proportionate to the slated end objective, as most of the data would likely go unused. Therefore, the system also fails the proportionality criterion of the test.

The right to privacy is a subset of Article 21 of the Constitution, which states that "no person can be deprived of his life or personal liberty, except as per the procedure established by law," is the prerequisite for establishing a law. The Supreme Court interpreted the definition of "procedure established by law" in the Maneka Gandhi v. Union of India[49], where the Supreme Court ruled that a law restricting someone's freedom had to be fair, reasonable, and just—not irrational, repressive, or fantastical in the case of Mohd. Arif v. Registrar[50], the Court noted that Article 21 should be interpreted in conjunction with other fundamental rights; hence, not only does the legal process have to be just, fair and reasonable, but the law itself has to be reasonable.

## The Controversy Surrounding Privacy and Security

Facial Recognition Technology has significant implications for individual privacy rights, raising ethical and legal concerns surrounding autonomy, liberty, and privacy. Privacy is crucial for preserving autonomy, independence, and dignity, allowing individuals to express themselves freely without surveillance concerns. However, the proliferation of AI systems that amass and analyse vast amounts of data poses significant privacy challenges and threats to personal

[48] Facial Recognition Technology in India, ProjectStatecraft, October 01, 2021, https://www.projectstatecraft.org/post/facial-recognition-technology-in-india

[49] Maneka Gandhi v. Union of India(1978) 1 SCC 248

[50] Mohd. Arif v Registrar, Supreme Court of India (2014) 9 SCC 737

freedom of expression, transparency, and accountability concerns due to the lack of regulation in many countries.[51] For example, New York's Lockport School District faced protests over plans to implement facial recognition for all students, leading the state to halt the project pending a privacy assessment.[52]FRT enables matching individuals' faces against databases and retrieving personal information without consent. This technology, coupled with potential data breaches, biassed profiling, lack of informed consent, secondary data use, healthcare privacy violations, lack of transparency in automated decisions, and malicious exploitation of personal data, exacerbates the privacy challenges associated with AI's data collection and processing methods.

Let's look into various privacy concerns of FRT one by one. The widespread adoption of facial recognition technology by private and public sectors, often without consent, has raised concerns among lawmakers and civil rights advocates regarding privacy rights. The Carnegie Mellon study demonstrates how facial recognition technology links an individual's offline identity to their online presence without obtaining consent.[53] Tech reporter Kashmir Hill exposed the disturbing story of Clearview AI, a secretive startup that created a facial recognition app allowing anyone to identify strangers from photos by tapping a massive database scraped from social media without consent.[54] Obtaining informed consent from users is critical, as well as ensuring they understand how their data will be utilised and retaining their right to grant or revoke consent. However, many individuals may not understand how their personal data will be processed or the potential risks involved, undermining their ability to make a truly informed decision. The British case[55]Challenged the police's use of facial recognition technology as a violation of privacy, data protection, and anti-discrimination laws, despite public support for FRT in law enforcement being balanced against privacy concerns from a significant subset opposing

[51] JawahithaSarabdeen, *Protection of the rights of the individual when using facial recognition technology*, Volume 8, Issue 3, March 2022, https://www.sciencedirect.com/science/article/pii/S2405844022003747#bib3

[52] Davey Alba, *Facial Recognition Moves Into a New Front: Schools*, The N.Y. Times, (Feb. 6, 2020) https://www.nytimes.com/2020/02/06/business/facial-recognition-schools.html

[53] *More Than Facial Recognition*, Carnegie Mellon University https://www.cmu.edu/homepage/images/extras/test/asdf/facial-recognition.html

[54] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, The N.Y. Times, (Jan.18, 2020) https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

[55] R (Bridges) v The Chief Constable of South Wales

its use without consent or ethical guarantees. In the Canadian case, the SC held that a woman's right to privacy under Article 5 of the Quebec Charter of Human Rights and Freedoms had been violated when her photograph was taken without her knowledge or consent.[56] If facial data is compromised through hacking or breaches, an individual's privacy and security are severely jeopardised, as their biometric data can no longer serve as a secure identifying feature. This non-replaceable nature of facial data underscores the importance of addressing security and privacy implications surrounding facial recognition technology.

Secondly, Transparency is a significant concern when it comes to FRT, the lack of which severely undermines public trust in these increasingly prevalent technologies. Individuals must fully know how their facial data is collected, utilised, and stored. Organisations should openly disclose how their AI algorithms operate and handle user data for personalisation. Also, they must provide clear notice to individuals when their biometric data is being collected or used for identification purposes, specifying the types of data processed and retention periods along with disclosing who has access to this information and under what circumstances it may be shared with third parties,upholding their autonomy.Adopting transparent practices and explaining the decision-making processes behind these systems can help foster trust and empower individuals to make informed choices regarding their personal information.

Thirdly, those developing and deploying AI systems and the organisationsutilising them must be held accountable for the outcomes and impacts resulting from their AI applications, ensuring responsibility and addressing any negative consequences. Reports prove that government and commercial entities' continuous gathering of images and data through facial recognition technologies may diminish accountability for those making decisions based on that data.[57] Accountability mechanisms foster trust by ensuring that organisations responsibly handle

[56] Aubry v. E′ ditions Vice-Versa Inc [1998] 2 SCR 591

[57] Elizabeth Snyder, *Faceprints and the Fourth Amendment: How the FBI Uses Facial Recognition Technology to Conduct Unlawful Searches*, 68 SYRACUSE L. REV. 255 (2018).

personal data and face consequences for failures to protect individual privacy. This incentivises proactive measures to minimise privacy risks associated with facial recognition technologies.

Another primary concern is the lack of data security and protection, which threatens privacy. As one expert explains, if the government can constantly track people's faces and locations, it can also track all their associations and connections. Improperly stored facial data is vulnerable to hacking, enabling identity fraud, unlawful surveillance, and violating data privacy laws. This erodes public trust in entities using facial recognition technology. Once stored in databases, personal information becomes a target for cybercriminals, heightening the threat of identity theft and other cybercrimes. These issues compromise individual privacy and undermine societal acceptance of this surveillance technology. The lack of the ability for Facial images to be encrypted causes both government and commercial facial recognition databases to be vulnerable to hacking threats. Also, the misuse and exploitation of the data made individuals feel unsafe when undergoing facial recognition scanning. Stringent data protection measures and responsible data handling practices are paramount to addressing the mounting privacy concerns surrounding facial recognition technology's widespread adoption.

Bias and discrimination are other issues inherent in many facial recognition algorithms. For example, convolutional neural networks (CNNs) used for facial recognition are often trained on datasets that lack diversity and contain predominantly white male facial images.[58] Mass surveillance breaches privacy and other fundamental freedoms like association, assembly, expression, and protest, as evidenced by Hong Kong citizens covering their faces and destroying FRT-enabled lampposts during the 2019 democracy protests[59]. When FRT systems exhibit accuracy disparities across demographic groups, it can result in unlawful discrimination.[60] Courts

[58] Barcic, Ena &Grd, Petra & Tomicic, Igor., *Convolutional Neural Networks for Face Recognition: A Systematic Literature Review*, (2023), 10.21203/rs.3.rs-3145839/v1.

[59] Zak Doffman, *Hong Kong Exposes Both Sides Of China's Relentless Facial Recognition Machine*, Forbes (26 August 2019).

[60] Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, (Conference Paper, Conference on Fairness, Accountability and Transparency PMLR 81, 2018) 77.

have acknowledged the potential discriminatory impact of FRT and the need to investigate such possibilities to uphold equality laws.[61] Additionally, there are warnings that FRT can enable unlawful profiling and discrimination based on characteristics like race, ethnicity, or gender, resulting in disproportionate errors and potentially discriminatory treatment against specific individuals or communities[62] and also a threat to political activism and dissenting voices. The right against arbitrary arrest or detention is also at risk, as false positive matches from FRT used by law enforcement for suspect identification could lead to wrongful arrests or detentions. Furthermore, the lack of transparency of FRT system outputs threatens the rights to equality before the law and a fair trial when such outputs are used as evidence in legal proceedings without the ability to assess their accuracy.

With the multiple privacy concerns seen above, one still cannot dispute the security benefits of FRT, which were discussed previously. Facial recognition enhances security through accurate identification, reducing unauthorised access risks. Law enforcement leverages it to identify and track subjects of interest, aiding investigations and public safety. Additionally, facial recognition allows customisable security levels and trigger responses based on the application's needs.  Some examples of facial recognition already being used for security include Chinese authorities identifying criminals through surveillance and airports using it to expedite the screening trusted/pre-cleared travellers. The technology is also employed in privacy contexts - creating anonymising masks or facial obfuscation algorithms to conceal identities from facial recognition systems. This allows protesters or other individuals to avoid being identified and tracked by authorities utilising facial recognition.

According to the report, the deployment of facial recognition technology (FRT) could assist in achieving national security goals in a relatively cost-effective manner.[63] The report suggests that

[61] R v South Wales Police [2020] EWCA Civ 1058, [210].

[62] Australian Human Rights Commission, Human Rights and Technology Final Report, (Report March 2021) 115; UN Committee on the Elimination of Racial Discrimination, General Recommendation No 36: Preventing and Combating Racial Profiling by Law Enforcement Officials, CERD/C/GC/36 (24 November 2020) [35]-[36].

[63] *Special report to Parliament on the OPC's investigation into the RCMP's use of Clearview AI and draft joint guidance for law enforcement agencies considering the use of facial recognition technology*, Use of Facial

implementing FRT offers a path to bolstering national security objectives through enhanced surveillance while leveraging current systems and requiring comparatively less investment. Retailers are deploying facial recognition systems to combat shoplifting and theft. A 2019 survey found that around 6% of stores had implemented facial recognition across all their locations to prevent loss.[64] Around half of U.S. adults favour facial recognition for security in retail and apartment buildings, while 57% oppose its use on social media for identifying people in photos. Also, apartment buildings and residential communities are adopting facial recognition entry systems as an access control and security measure to verify residents while keeping unauthorised individuals out automatically. So,businesses across the retail, gaming, entertainment, and residential sectors are turning to facial recognition to enhance security, prevent crime, enforce bans and trespass policies, and control access to restricted areas.

It has to be noted that the ability to track people everywhere with facial recognition creates a situation where security comes at the expense of privacy. We need to carefully consider these trade-offs before widely using this powerful technology. Protecting the right to privacy is paramount in an AI-driven future. While AI offers transformative societal benefits, it raises significant ethical and privacy concerns. Governments, companies, and individuals must recognise the importance of safeguarding privacy rights while leveraging AI's advantages. Adequate checks, privacy-centric AI development, transparency, and accountability ensure that AI respects individual privacy. Striking this balance enables responsible AI adoption that advances technology while upholding fundamental human rights.

## Ethical and Legal Guidelines for using FRT

Robust data protection mechanisms are needed to address facial recognition and privacy rights effectively. This will involve procedures like the secure storage and encryption of biometric data,

Recognition Technology in Canada and the Way Forward, Office of the Privacy Commissioner of Canada Police (2021)https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/Google Scholar

[64] National Retail Federation and Richard Hollinger, 2019 National Retail Security Survey (June, 6 2019), https://nrf.com/research/national-retail-security-survey-2019.

conducting regular tests on facial recognition algorithms to minimise false positives and misidentifications, and setting up stringent guidelines for cross-platform integration and data sharing. These measures would help prevent unauthorised access or misuse of personal information while ensuring that facial recognition technology is deployed responsibly with maximum privacy protection. The following are a few ethical and legal recommendations that address privacy concerns while guaranteeing the security benefits of FRTs.

1. Individuals should be informed when their facial data is collected, how it will be used, and have the ability to opt out in situations. Clear and accessible consent mechanisms must be implemented to empower individuals to make informed participation decisions, ensuring their privacy preferences are respected.
2. The government must forbid any use of algorithmic technologies, such as mass surveillance, specify in relevant legislation what applications of facial recognition and other technologies are permissible and impose strict penalties for violating facial recognition regulations.
3. The government can create a public AI registry listing all algorithmic tools used domestically for national security. Also, a committee should be appointed to review the regular performance and updates to the technology to maintain high accuracy and reliability. An expert panel on facial recognition technology could be established to provide regulatory guidance on its use.
4. The government must enact privacy protections mitigating individual risks from facial recognition, including measures addressing accuracy, data retention, accountability, privacy protection, civil liberty preservation, transparency, and ensuring informed consent for using personal information.
5. Ensure that the FRT system used is validated using local demographic data to address the diverse population of India to reduce potential biases based on ethnicity,region,or socio-economic status.Eliminate prejudice when applying algorithms to treat all individuals or groups fairly. Both data and algorithmic biases must be addressed to guarantee impartiality in decision-making.

6. The use of the FRT system shall adhere to and advocate strong data protection regulations like the Personal Data Protection Bill to ensure the secure handling of biometric data. A secure technological environment is necessary for models designed across multiple disciplines to improve system resilience when processing judicial decisions and data with accurate sources and permanent records.
7. Make sure that human judges have the last word in judicial decisions by using FRT as a supporting instrument rather than as the primary decision-maker
8. The FRT system shall be subjected to transparency, i.e., clear communication through court notification. The court should also provide a detailed explanation for the decisions influenced by FRT to indicate how the technology impacts judicial outcomes.
9. Organisations should establish explicit data handling, consent, and transparency policies, adhering to best practices like anonymisation and secure storage to balance security and privacy.
10. The Government should take initiatives to increase investment to study AI's impact on diverse groups, enhance digital literacy programs, and educate citizens about their privacy rights regarding AI technologies. In collaboration with private entities, governments should conduct public education campaigns informing about the risks and benefits of facial recognition technology.
11. The government could provide guidelines on collecting, storing, and sharing biometric data, as well as how facial recognition technology (FRT) can be utilised for law enforcement and global security purposes.
12. Organisations using FRT should be mandated to specify the data collected, its usage (including any third-party sharing), retention duration, deletion policies, and opt-out provisions. This would promote transparency around FRT data practices.
13. Adopting a privacy-by-design approach is essential to overcoming facial recognition privacy concerns. This involves integrating privacy considerations from facial recognition systems' initial design and development phases.

## Conclusion

In conclusion, the increasing need to introduce AI systems into courtrooms is a crucial requirement within current legal structures. With the breakthrough in technology, many ethical issues have been raised regarding privacy and security approaches, considering how advanced AI-powered facial recognition is nowadays in court. However, as evidenced by some of the materials cited in this article, those AI-driven systems that learn to recognise faces successfully help fight crimes and preserve public safety. However, there are also heightened worries about personal privacy rights and the ability to abuse private data. Given the evolution of technology, a balance between security and privacy is now more critical than ever. Additionally, the input from the sources suggests that we should deeply consider these algorithms' security and robustness for confidentiality. Future avenues should also concentrate on improving the accuracy and repeatability of face recognition methods, together with adequate privacy protection mechanisms.Ultimately, balancing national security interests and individual privacy rights is paramount. From the sources here, it should be understood that facial recognition technology has positive and negative sides. Policymakers, technologists, and legal experts must work together to set broadly applicable standards and regulations that afford the public adequate privacy protection when using AI-powered facial recognition in court.