Page 4513 - 4529 **DOI:** *https://doij.org/10.10000/IJLMH.119497*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 2

2025

Facial Recognition Technology and Privacy: A Legal and Ethical Inquiry

PRACHILEKHA SAHOO[1]

ABSTRACT

Facial recognition systems, a subset of biometric technologies, have transformed the process of identifying individuals by analysing distinct facial features. While this innovation has enhanced efficiency in areas such as mobile security, social media, and air travel, it has simultaneously raised significant concerns around privacy and consent. The rapid deployment of facial recognition tools, often without public awareness or explicit consent, poses serious threats to individual freedoms. Being unknowingly recorded in public spaces undermines the right to privacy and fosters a climate of constant surveillance, which can alter human behaviour and strain the relationship between citizens and the state.

Moreover, the indiscriminate use of such technology; especially by law enforcement and private enterprises risks creating a culture of pre-emptive suspicion, thereby eroding the fundamental legal principle of presumed innocence. In India, the swift adoption of facial recognition technology across multiple sectors, including policing and governance, has far outpaced the development of adequate regulatory safeguards. This article critically examines key facial recognition initiatives in India, highlighting the pressing need for comprehensive oversight to protect civil liberties in an era increasingly defined by algorithmic scrutiny and digital surveillance.

Keywords*: FRT, Surveillance, Privacy, Record, Concern.*

I. INTRODUCTION

In a group of closest of friends, people often let their guard down, exhibit their vulnerable side which they would not show or reveal to the rest of the world. There are spaces in our lives where laughter comes easily, secrets are spoken without hesitation, and truth flows in its most natural form. These are the raw, unscripted moments we often cherish is shared only with those closest to us, meant to fade gently into memory.[2] But what if those fleeting slices of life were no longer private recollections? What if, instead, they were captured by a lens and instantly transmitted across the globe?

[1] Author is a doctoral student at National Law University Odisha, India.

[2] 'In the Face of Danger: Facial Recognition and the Limits of Privacy Law' (2007) 120 *Harvard Law Review* 1870 http://www.jstor.org/stable/40042639

 [ISSN 2581-5369]

A candid photo or spontaneous video today is no longer just a record of a moment rather it is a gateway. Each image feeds into an enormous and ever-expanding digital ecosystem. Somewhere, in a remote data centre buzzing with machines, a facial recognition algorithm processes these visuals by scanning expressions, comparing features, and matching faces against vast databases. What emerges is a highly organized, searchable archive which weaves an intricate catalogue of human existence, preserved frame by frame.

This is not science fiction. It is the present.

Facial recognition technology (FRT) is already embedded in our world. And its influence is magnified by a generation that views images not as keepsakes, but as extensions of self which is alive, dynamic, and constantly in circulation. As every photograph becomes part of a larger, interconnected digital puzzle, the boundary between personal and public becomes increasingly indistinct. What was once a private moment now has the potential to be permanent and universally accessible.[3]

India, in particular, has witnessed a dramatic surge in the deployment of facial recognition systems over the last five years. From policing and public safety to healthcare services, educational institutions, and even quick-service restaurants, FRT has found varied applications. While these tools promise efficiency and enhanced security, their rapid expansion has far outpaced the development of adequate legal and regulatory frameworks. As a result, serious concerns around data protection, surveillance, and individual privacy have come to the forefront.

In this context, the article undertakes an examination of key facial recognition projects being implemented across India, assessing their expansion into multiple domains. It highlights the absence of comprehensive legal and policy frameworks governing their use and considers the resulting challenges to privacy, autonomy, and fundamental freedoms. By exploring the intersection of technology and civil liberties, the article aims to contribute to the growing discourse on state surveillance and the need for robust safeguards in a digitally evolving society.

II. UNDERSTANDING FRT AND ITS MECHANISM

Facial recognition technology (FRT) operates as a biometric identification method, comparable to techniques like fingerprinting or iris recognition. It works by analyzing specific facial features such as the contour of the jawline or the spacing between the eyes by using

[3] Andrew J McClurg, 'Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality' (2006) 74 University of Cincinnati Law Review 887

 [ISSN 2581-5369]

sophisticated local feature analysis algorithms.[4] These distinguishing traits are transformed into a mathematical model referred to as a facial template, which uniquely corresponds to an individual. FRT systems can function using both standard light and infrared imaging, enabling the detection and identification of faces from still images, video recordings, or real-time camera feeds. Much like a fingerprint, a facial template acts as a singular biometric marker, capable of accurately distinguishing one person from another.[5]

Facial Recognition Technology (FRT) operates mainly in two distinct modes. The first involves identification, where the system captures an unknown person's facial image, converts it into a digital template, and compares it against entries in a database to determine a possible match. This method is commonly utilized by law enforcement agencies for tracking and identifying suspects. The second mode is authentication, where an individual's face is matched with a previously stored template such as when unlocking a personal device using facial recognition.

Contemporary FRT systems employ advanced machine learning techniques, especially deep learning, to enhance their performance. During the training process, these systems evaluate visual elements like contours and edges that are associated with specific facial features and labelled data. A new facial image is interpreted as a grid of pixels, which is then processed through successive layers of artificial neurons. Each layer applies weighted calculations based on various attributes such as texture, shading, and spatial arrangement. As the system processes a broad dataset of labelled images, it fine-tunes these weights to build a predictive model capable of recognizing faces accurately.

When presented with a new image, the system generates confidence scores that estimate the probability of a correct match. To guard against fraudulent attempts, such as using photographs or videos, many systems incorporate live detection mechanisms requiring the subject to perform actions like blinking or slight head movements to verify that the input is from a live person.

Despite its technological advancements, Facial Recognition Technology (FRT) continues to grapple with inherent limitations in accuracy. A fundamental challenge lies in balancing two types of errors: false positives - where a person is mistakenly identified as someone else and false negatives - where the system fails to recognize a valid match. Efforts to reduce one often increase the likelihood of the other; for example, tightening parameters to prevent false matches may result in more frequent recognition failures. Moreover, the reliability of FRT can be

[4] International Network of Civil Liberties Organizations (INCLO), 'What is Facial Recognition Technology (FRT)?' (INCLO) https://inclo.net/pillars/surveillance-and-digital-rights/principles-for-use-of-frt/what-is-frt/ accessed 16 April 2025

[5] Amber Sinha, 'The Landscape of Facial Recognition Technologies in India' (Tech Policy Press, 1 April 2024) https://www.techpolicy.press/the-landscape-of-facial-recognition-technologies-in-india/ accessed 16 April 2025

 [ISSN 2581-5369]

significantly influenced by external variables such as lighting conditions, background settings, facial expressions, and the angle at which the face is captured. These factors can collectively hinder the system's precision, raising concerns about its consistency and overall effectiveness in real-world applications.[6]

III. HISTORICAL BACKGROUND AND IMPORTANCE OF FRT

Woodrow Wilson Bledsoe is often credited as a pioneer in the field of facial recognition technology.[7] In the 1960s, he developed an innovative system that could sort and classify human faces using a RAND tablet.[8] This early device enabled users to plot points by recording horizontal and vertical coordinates on a grid through a stylus that emitted electromagnetic signals.[9] Users would manually input the coordinates of various facial features such as the eyes, nose, mouth, and hairline.[10]

As the technology progressed, facial recognition became increasingly automated. It evolved to detect individuals based on defined facial characteristics like the distance between the eyes or the shape of the mouth, making identification more efficient.

By the 1990s, the development of computerized algorithms further advanced the field. However, it was after the terrorist attacks on September 11, 2001, that facial recognition technology gained significant public and governmental attention.[11] The U.S. federal government began heavily investing in the technology, allocating substantial funding to support the creation of facial recognition databases at both the state and local levels.

Originally nurtured through publicly funded research in computer science, the technology eventually found widespread application in the private sector. Law enforcement agencies adopted it to assist in suspect identification and border security screenings. At the same time, commercial uses of facial recognition began to grow. Businesses started using it for diverse purposes i.e. monitoring high-risk gamblers in casinos, providing personalized greetings to hotel guests, matching users on dating platforms, verifying age in bars, and even tracking attendance in educational institutions.[12]

---

[6] M Gentzel, 'Biased Face Recognition Technology Used by Government: A Problem for Liberal Democracy' (2021) 34 *Philosophy & Technology* 1639 https://doi.org/10.1007/s13347-021-00478-z

[7] FACEFIRST, 'The History of Face Recognition' (FaceFirst, 28 March 2020) https://www.facefirst.com/blog/brief-historyof-face-recognition-software/ accessed 28 March 2025.

[8] Ibid

[9] Ibid

[10] Ibid

[11] Jia Jen Low, 'Biometrics – The Most Secure Solutions for Banking' (Tech HQ, 2 September 2020) https://techhq.com/2020/09/biometrics-the-most-secure-solution-for-banking/ accessed 17 April 2025.

[12] Elizabeth McClellan, 'Facial Recognition Technology: Balancing the Benefits and Concerns' (2020) 15 *Journal of Business and Technology Law* 363, 372.

 [ISSN 2581-5369]

While the origins of facial recognition technology (FRT) date back over half a century, its advancement has surged significantly in the last ten years. This rapid progress is largely attributed to the integration of artificial intelligence, particularly deep convolutional neural networks, which have revolutionized the ability to extract facial features from extensive image datasets. The development of these systems has been fuelled by the creation and use of vast collections of facial images; many of which have been gathered without the explicit consent of the individuals involved. Furthermore, practical insights gained through widespread commercial implementation have contributed to refining and optimizing the technology for various applications.[13] The term FRT references a large number and variety of face recognition systems that are produced by an array of vendors, each of which uses its own algorithms, data sets used to train the models, and data sets used for comparison. The acceleration in development, which continues today, has led to deployment in many different applications.

The term Facial Recognition Technology (FRT) encompasses a broad range of systems developed by various vendors, each with its unique algorithms, training datasets, and comparison datasets. The rapid advancements in the field, which continue to this day, have led to its widespread adoption across numerous sectors. FRT is now commonly used for unlocking smartphones and personal devices and is increasingly deployed in law enforcement investigations, at border checkpoints, in airports, and across various other government and commercial settings. Governments collect vast facial image databases through the issuance of identity documents like driver's licenses and passports, as well as from mugshots taken during arrests. In parallel, private companies build their own databases using images gathered from online sources or captured in their facilities. The division between public and private FRT databases is often blurred, as law enforcement agencies frequently access private-sector databases for investigative purposes. As a result, both government and commercial databases collectively enable the potential identification of a significant portion of the U.S. population through FRT.

While still in its early stages and characterized by a variety of smaller vendors, the facial recognition technology (FRT) market is expanding quickly. According to a 2020 industry report, the FRT market was valued at approximately $4 billion, with an expected annual growth rate of around 15% over the next ten years. Projections indicate that by 2030, the global FRT market could reach nearly $17 billion in value.[14] Facial recognition technology has gained

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

[14] Allied Market Research, 'Facial Recognition Market' (2023) https://www.alliedmarketresearch.com/facial-

significant traction in law enforcement, with a 2021 report from the Government Accountability Office revealing that 20 out of 42 federal law enforcement agencies have adopted the technology.[15]

Beyond law enforcement, facial recognition technology (FRT) is becoming more common in airports and other transportation hubs. The Transportation Security Administration (TSA) has extended a pilot program that employs FRT to authenticate traveller identities at security checkpoints in 25 airports across the United States.[16] At the same time, Customs and Border Protection has implemented facial recognition technology (FRT) to monitor travellers departing from the U.S. at 32 airports, as well as to track those arriving at all international airports nationwide.[17]

IV. EXPANSION OF FACIAL RECOGNITION TECHNOLOGY ACROSS SECTORS

The use of facial recognition technology (FRT) in policing is becoming more prevalent in India. The National Crime Records Bureau (NCRB) had previously issued a tender for the nationwide implementation of an Automated Facial Recognition System (AFRS). However, several critical issues surrounding FRT remain unaddressed in India, including the absence of a clear legal framework, concerns over individual privacy violations, the rise of a surveillance state, and the erosion of anonymity. It is crucial that appropriate guidelines are established before deploying such technologies.

The pandemic has accelerated the adoption of contactless technologies worldwide. India, like many other nations, employed a contact tracing app and used various technological tools to enforce quarantine measures. As these technologies become normalized in the pandemic context, there is a risk they will continue to be used without sufficient consideration in the post-pandemic era. Meanwhile, resistance to FRT is growing. The death of George Floyd in the U.S. sparked widespread protests, raising serious concerns about the practices and legitimacy of law enforcement agencies. In response, several companies have reconsidered their involvement in FRT. IBM, for instance, announced it would cease the development and research of FRT for law enforcement applications, citing concerns over accuracy and inherent racial and gender

recognition-market

[15] Government Accountability Office (GAO), 'Facial Recognition Technology: Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used by Employees' (2021) https://www.gao.gov/products/gao-21-105309

[16] K.V. Cleave, 'TSA Expands Controversial Facial Recognition Program' CBS News (5 June 2023) https://www.cbsnews.com/news/tsa-facial-recognition-program-airports-expands

[17] Government Accountability Office (GAO), 'Facial Recognition Technology: CBP Traveler Identity Verification and Efforts to Address Privacy Issues' (2022) https://www.gao.gov/products/gao-22-106154

 [ISSN 2581-5369]

biases.[18] Amazon followed suit, implementing a one-year moratorium on offering its facial recognition technology, Rekognition, to police forces.[19]

(A) Research Objectives

- To examine the ethical implications of FRT.
- To assess its impact on privacy and human rights.

V. ETHICAL CONCERNS SURROUNDING FRT

Facial recognition technology (FRT) has its roots in computer vision research dating back to the 1960s.[20] At its core, the system relies on machine learning techniques and complex mathematical models. While algorithms are a fundamental part of modern computing, the application of these algorithms in facial recognition has revealed notable flaws particularly due to the lack of diverse data sets during the training phase.[21] This limitation has led to significant disparities, especially when individuals subjected to surveillance seek employment or financial services. In some cases, people have been wrongly identified as suspects in criminal investigations.

The evolution of this technology involved the use of deep learning, a process where the software learns to recognize and map facial features by analyzing large volumes of image data.[22] Through repeated exposure to such datasets, the system refines its ability to detect and identify unique facial patterns with increasing accuracy.

(A) Informed Consent

Facial recognition technology (FRT) is anticipated to become increasingly integral to the healthcare sector, particularly in areas such as patient identification, monitoring, and diagnostics. In fact, several applications are already in use. As these tools become more prevalent in medical environments, it will be essential to obtain informed consent not just for

[18] J Peters, 'IBM Will No Longer Offer, Develop, Or Research Facial Recognition Technology' (2020) The Verge https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software

[19] N Statt, 'Amazon Bans Police From Using Its Facial Recognition Technology For The Next Year' (2020) The Verge https://www.theverge.com/2020/6/10/21287101/amazon-rekognition-facial-recognition-police-ban-one-year-ai-racial-bias

[20] Samuel D Hodge Jr, 'The Legal and Ethical Considerations of Facial Recognition Technology in the Business Sector' (2022) 71 *DePaul Law Review* 731 https://via.library.depaul.edu/law-review/vol71/iss3/2 accessed 17 April 2025.

[21] Vivian D Wesson, 'Why Facial Recognition Technology Is Flawed' (2020) 92 *New York State Bar Association Journal* 21 (August).

[22] Jake Bechtel, 'Two Major Concerns About the Ethics of Facial Recognition in Public Safety' (Design World, 14 March 2019) https://www.designworldonline.com/two-major-concerns-about-the-ethics-of-facial-recognition-in-public-safety/ accessed 17 April 2025.

capturing and storing patients' facial images, but also for clarifying the specific ways in which those images might be processed or analyzed.[23]

A key ethical concern lies in the fact that patients may not always be fully informed that their images could be used to extract further clinically relevant insights beyond their original purpose.[24] Although FRT systems in healthcare often employ methods to anonymize or de-identify patient data, some experts remain unconvinced that complete anonymity is genuinely achievable. This raises important clinical and ethical questions, emphasizing the need to clearly communicate such potential risks to patients.

Moreover, certain machine learning models depend on ongoing data input to refine their algorithms like how quality improvement research operates, where consent is generally not required.[25] For instance, improving facial recognition systems for genetic diagnoses would necessitate regular access to new image datasets of individuals already diagnosed with particular genetic conditions.[26]

To foster transparency and preserve patient trust, healthcare institutions are encouraged to include community representatives in the planning and implementation stages of FRT. These stakeholders can help shape policies around patient communication and consent. As the capabilities of FRT expand to detect conditions such as behavioural or developmental disorders, careful consideration must be given to what types of analyses are included in the system.[27] Furthermore, institutions must establish clear protocols on whether and how patients will be informed about incidental findings that arise during these analyses.

(B) Bias

Facial recognition technology (FRT) must meet specific standards of accuracy for its intended uses, ensuring that the benefits it provides clearly outweigh any potential risks. It is equally important that any biases in the data or the outcomes are carefully examined from an ethical perspective.[28] In machine learning, the quality of the results is directly linked to the quality of

[23] Balthazar P, Harri P, Prater A and Safdar NM, 'Protecting Your Patients' Interests in the Era of Big Data, Artificial Intelligence, and Predictive Analytics' (2018) 15(3 pt B) *Journal of the American College of Radiology* 586 - 590.
[24] Mohapatra S, 'Use of Facial Recognition Technology for Medical Purposes: Balancing Privacy with Innovation' (2016) 43(4) *Pepperdine Law Review* 1017–1064.
[25] Watson M, 'Keeping Your Machine Learning Models Up-to-Date: Continuous Learning with IBM Watson Machine Learning (Part 1)' (Data Lab, March 2018) https://medium.com/ibm-watson-data-lab/keeping-your-machine-learning-models-up-to-date-f1ead546591b accessed 26 April 2025.
[26] Cohen IG, Amarasingham R, Shah A, Xie B and Lo B, 'The Legal and Ethical Concerns That Arise from Using Complex Predictive Analytics in Health Care' (2014) 33(7) *Health Affairs* 1139–1147.
[27] Wen L, Li X, Guo G and Zhu Y, 'Automated Depression Diagnosis Based on Facial Dynamic Analysis and Sparse Coding' (2015) 10(7) *IEEE Transactions on Information Forensics and Security* 1432–1441.
[28] Ghaemi SN and Goodwin FK, 'The Ethics of Clinical Innovation in Psychopharmacology: Challenging

the data fed into the system, a principle often referred to as "garbage in, garbage out."[29] For instance, if the images used to train a system lack sufficient racial diversity, the resulting system may be biased and less effective for certain racial or ethnic groups.

An example of such bias occurred with an FRT system designed to identify gay men from a collection of photos.[30] Instead of identifying individuals based on their sexual orientation, the system appeared to rely on stereotypical patterns of grooming and dress associated with gay men. Although the developers did not intend for this tool to be used in clinical settings, the case highlighted how inherent biases in FRT can affect its performance and reliability.[31]

Facial recognition technology (FRT) has been shown to be less accurate when identifying individuals with darker skin tones, which significantly increases the risk of wrongful identification and prosecution of ethnic minorities in criminal investigations. This problem, if unaddressed, is likely to intensify the interaction of these communities with law enforcement and exacerbate their over-representation in the criminal justice system. A notable case occurred in 2020, when Robert Williams, an African American man, was wrongfully arrested for shoplifting in Detroit based on a facial recognition match. Williams was detained for 30 hours before being released, with the mismatch being identified through a comparison of his driver's license photo and distorted crime scene footage.[32] The police later apologized and began reviewing their use of FRT, while Williams pursued legal action for compensation. This incident underscores the dangers of relying on inaccurate technology for criminal identification, which can perpetuate racial bias and further marginalize minority groups within the justice system.[33]

This case occurred alongside the public outcry over the murder of George Floyd and the subsequent rise of the Black Lives Matter movement, highlighting the broader issue of racial discrimination. The disproportionate representation of minority groups in police databases only increases the likelihood that they will be flagged by FRT systems. In the U.S., for instance, over

Traditional Bioethics' (2007) 2(1) *Philosophy, Ethics, and Humanities in Medicine* 26.

[29] Tunkelang D, 'Ten Things Everyone Should Know About Machine Learning' (Forbes, 6 September 2017) https://www.forbes.com/sites/quora/2017/09/06/ten-things-everyone-should-know-about-machine-learning accessed 13 January 2025.

[30] McCullom R, 'Facial Recognition Technology is Both Biased and Understudied' (Undark, 17 May 2017) https://undark.org/article/facial-recognition-technology-biased-understudied/ accessed 31 March 2025.

[31] Agüera y Arcas B, Todorov A and Mitchell M, 'Do Algorithms Reveal Sexual Orientation or Just Expose Our Stereotypes?' (Medium, 11 January 2018) https://medium.com/@blaisea/do-algorithms-reveal-sexual-orientation-or-just-expose-our-stereotypes-d998fafdf477 accessed 17 March 2025.

[32] Drew Harwell, 'Wrongfully arrested man sues Detroit police over false facial recognition match' (13 April 2021) *Washington Post* https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/.

[33] Brian Jefferson, *Digitize and Punish: Racial Criminalization in the Digital Age* (University of Minnesota Press 2020) 11.

75% of the Black male population is included in criminal justice databases, meaning their facial images are accessible for analysis through facial recognition. This increases the likelihood that these individuals will be targeted by law enforcement, particularly as FRT may direct police to people already in their databases.

Additionally, there are significant data-based reasons behind the higher mis-identification rates for minority groups. A 2019 report by the National Institute of Standards and Technology (NIST) revealed that FRT systems had much lower accuracy rates when identifying African American and Asian faces, with these faces being 10 to 100 times more likely to be misidentified compared to white male faces.[34] Other studies have shown that dark-skinned women have a mis-identification rate of around 35%, which is 50 times higher than that for white males.

This issue stems from the data inputs that the algorithms rely on, with training datasets consisting of about 80% lighter-skinned individuals on average.[35] The problem is therefore likely rooted in the lack of racial diversity in the datasets used to train FRT systems. Developers must address this by ensuring more balanced racial representation in these datasets. Failing to do so could perpetuate systemic racial bias, whether intentional or not.[36]

The underrepresentation of ethnic minorities in the datasets is particularly troubling given that these communities are already disproportionately targeted by law enforcement and over-represented in the criminal justice system. The increased likelihood of mis-identification by FRT and other emerging technologies could worsen this problem.[37] It is vital that developers design facial recognition systems with racial fairness in mind, embedding measures to prevent discrimination within the data used for training. Furthermore, FRT should never be used in isolation but as part of a broader investigation that includes other forms of evidence. However, as noted by Damien Patrick Williams, simply adding more Black faces to the training datasets will not solve the deeper issue: these technologies are often deployed within a framework that already embodies racial and gendered inequalities in the criminal justice system.[38]

(C) Misidentifying

[34] Patrick Grother, Mei Ngan and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 2: Identification* (National Institute of Standards and Technology 2019).
[35] Joy Buolamwini and Timnit Gebru, 'Gender shades: Intersectional accuracy disparities in commercial gender classification' (2018) 81 *Proceedings of the 1st Conference on Fairness, Accountability and Transparency* 77–79.
[36] Ibid
[37] Clare Garvie, Alvaro Bedoya and Jonathan Frankle, 'The perpetual line-up: Unregulated police face recognition in America' (18 October 2016) *Georgetown Law Center on Privacy and Technology* https://www.perpetuallineup.org/.
[38] Damien Patrick Williams, 'Fitting the description: Historical and sociotechnical elements of facial recognition and anti-black surveillance' (2020) 7 *Journal of Responsible Innovation* 74–83.

 [ISSN 2581-5369]

A significant limitation of facial recognition technology (FRT) lies in the fact that people's facial features evolve over time, which can lead to incorrect identifications based on older images. Even subtle daily changes, like a different hairstyle or varying facial expressions, can result in misidentifications. Additionally, the quality of the image plays a crucial role in the performance of FRT systems.[39] Low-quality images, especially those captured through video scanning, pose a challenge as they are typically less clear than those taken with a digital camera.[40] Moreover, the relative size of the face in the image also impacts the system's ability to accurately identify it; smaller images can complicate the recognition process.

(D) Differential Treatment

The increased accessibility and low operational cost of Facial Recognition Technology (FRT) raises concerns about the potential for differential treatment based on identity. This ease of identification can lead to both exclusion and selective advantages that were previously impractical. For instance, luxury retailers might deploy FRT to recognize affluent customers and offer them exclusive services, while property owners could potentially use it to deny access to individuals outside preferred or non-protected categories.

Historically, certain marginalized communities have already experienced such targeted surveillance. A stark example is the treatment of the Hijra community under the Criminal Tribes Act of 1871.[41] Labelled as inherently criminal, members of this group were subjected to systematic monitoring by the police. They were confined to designated areas, forced to carry identification documents, submit fingerprints, and report their presence multiple times daily. They were often the first to be suspected and detained in the event of any crime, regardless of actual involvement. Reports of police brutality, custodial violence, and sexual abuse were disturbingly frequent.[42]

Given this context, empowering law enforcement with advanced surveillance tools like FRT without proper safeguards raises legitimate fears of reinforcing historical patterns of discrimination and abuse.

VI. IMPACT ON PRIVACY AND HUMAN RIGHTS

Privacy is universally acknowledged as a core human right, affirmed by key international

[39] Jeffrey Edgell and Andrew Trimpe, '4 Limitations of Facial Recognition Technology' (FedTech, 22 November 2013) https://fedtechmagazine.com/article/2013/11/4-limitations-facialrecognition-technology accessed 17 April 2025.
[40] Ibid
[41] The *Criminal Tribes Act 1871* (Act 27 of 1871)
[42] Mrinal Satish, 'Bad Characters, History Sheeters, Budding Goondas and Rowdies: Police Surveillance Files and Intelligence Databases in India' (2011) 23 National Law School of India Review 133.

instruments such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and various regional and global treaties. It serves as a foundation for human dignity and is closely tied to other essential freedoms, including the rights to free expression and association. In the digital era, privacy has emerged as a pressing human rights concern.

The rapid evolution of information technology which enables the collection, analysis, and widespread dissemination of personal data has intensified calls for robust legal safeguards. Innovations in fields like healthcare, telecommunications, transportation, and financial services now generate vast volumes of data about individuals. When combined with high-speed networks and sophisticated processing capabilities, this infrastructure allows for the assembly of detailed personal profiles, even without relying on centralized databases.[43]

Many of these advanced surveillance technologies, initially developed for military purposes, are increasingly being adopted by law enforcement, public authorities, and private sector entities. Public anxiety over privacy breaches has reached unprecedented levels, as reflected in numerous global opinion polls. This growing unease has spurred a wave of legislative action, with countries around the world enacting laws to better protect citizens' personal data.[44] However, human rights organizations remain alarmed by the export of such surveillance tools to developing nations, where legal frameworks may not yet provide adequate privacy protections.

(A) Privacy Concerns in FRT

Many facial recognition systems rely on databases compiled from photographs sourced online often from social media or other websites without obtaining consent from the individuals depicted.[45] A notable example is Clearview AI, which rapidly built massive image repositories by harvesting pictures from public platforms.[46] While this approach enabled fast database expansion, it has triggered serious concerns about individual privacy rights, the fairness of data usage, and the overall quality of such datasets. Furthermore, real-time image capture for identification purposes introduces additional challenges. These include inappropriate retention of data, repurposing of facial data for secondary uses, and inadequate or missing options for

[43] Global Internet Liberty Campaign, *Privacy and Human Rights: An International Survey of Privacy Laws and Practices* (1998) https://gilc.org/privacy/survey/ accessed 17 April 2025.
[44] Ibid
[45] Kashmir Hill, 'The Secretive Company That Might End Privacy as We Know It' *The New York Times* (18 January 2020) https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html accessed 17 April 2025.
[46] 'Clearview AI fined €30.5 million by Dutch regulator for GDPR violations' *The Verge* (3 September 2024) https://www.theverge.com/2024/9/3/24234879/dutch-regulator-gdpr-clearview-ai-fine accessed 17 April 2025.

 [ISSN 2581-5369]

individuals to opt out. Such practices also raise critical legal and ethical questions about the extent to which governments can access or utilize this information.[47]

(B) Chilling effect on free speech and movement.

Facial Recognition Technology (FRT) poses significant challenges across privacy, civil liberties, and equity. These systems are deeply personal, highly powerful, and can be invasive. For many individuals, opting out of being captured by FRT is simply not feasible in most situations. When employed for real-time surveillance, FRT can expand the scale and lower the costs of gathering detailed data on a person's movements, activities, and associations. Without stringent and responsible regulations, FRTs can facilitate the indiscriminate accumulation of facial data, even when there is no specific individual or event targeted.

Equity concerns are especially pertinent here. Historically marginalized communities are already disproportionately subjected to surveillance, and the expanded use of FRT could exacerbate this imbalance. In Uttar Pradesh, during the protests against the Citizenship Amendment Act (CAA) and the National Register of Citizens (NRC) in 2020, police employed aerial surveillance to monitor homes in protest areas, claiming it was necessary to track the movement of "anti-social" elements.[48] In February of that year, reports indicated that the police detained over 1,100 individuals for allegedly having ties to violent activities during the protests, identifying them using footage captured by drones.[49]

Similarly, the Delhi police used facial recognition technology at a political rally in December 2019 to identify potential troublemakers. A police officer involved in the operation revealed that every attendee was captured on camera as they passed through metal detectors, and within five seconds, the live video feed was compared to a facial database in a control room set up at the event.[50] This facial dataset included images taken from previous protest footage.

When used extensively and without proper safeguards, facial recognition technology (FRT) can enable authoritarian regimes to track individuals' movements and activities in great detail, particularly around political protests or activism. This could result in the exclusion of specific individuals from participating in public life. Unfortunately, this is not merely a theoretical

[47] Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 *Proceedings of Machine Learning Research* 1 http://proceedings.mlr.press/v81/buolamwini18a.html accessed 17 April 2025.

[48] The Quint, 'Uttar Pradesh Police Drone Surveillance of Houses: Right to Privacy, Security Law, Constitution' .

[49] Alexandra Ulmer and Zeba Siddiqui, 'India's Use of Facial Recognition Tech During Protests Causes Stir' (17 February 2020) Reuters https://www.reuters.com/article/world/indias-use-of-facial-recognition-tech-during-protests-causes-stir-idUSKBN20B0ZP/ accessed 17 April 2025.

[50] Jay Mazoomdaar, 'Delhi Police Film Protests, Run Its Images Through Face Recognition Software to Screen Crowd' (28 December 2019) The Indian Express https://indianexpress.com/article/india/police-film-protests-run-its-images-through-face-recognition-software-to-screen-crowd-6188246/ accessed 17 April 2025.

concern; there are documented instances where such practices have been implemented in various countries.

(C) Case Studies & Real-World Examples

Several instances of facial recognition technology (FRT) being employed during the COVID-19 pandemic in India highlight its growing role in public safety and monitoring:

- The Technology Development Board (TDB) under the Department of Science and Technology (DST) has approved initiatives aimed at supporting India's fight against COVID-19, including a project that uses facial recognition to track and identify individuals, even if they are wearing masks.[51]
- In Pune, the police have implemented the Maharashtra Home Quarantine Tracking System (MH HQTS), which requires individuals under home quarantine to download an app. The app prompts them to take regular selfies, which are then analyzed through facial recognition and location tracking to confirm they are complying with quarantine measures.[52]
- The Telangana state government has announced plans to transition from biometric attendance systems to facial recognition systems as part of its post-pandemic strategy. This shift has prompted private sector interest in deploying similar technologies for purposes such as attendance tracking, access control, and secure hotel locks. However, the use of facial masks has raised concerns about the accuracy of these systems, and private companies are awaiting government guidelines before scaling their deployment.[53]

VII. SUMMARY OF KEY FINDINGS

These technologies have the capacity to track, monitor, and identify individuals wherever they are, putting at risk fundamental civil liberties and human rights such as privacy, data protection, freedom of speech, and the right to peacefully assemble and associate. This could lead to the criminalization of protest and induce a chilling effect on free expression. Many uses of facial recognition and biometric systems suffer from significant scientific weaknesses, resulting in

[51] Singh, J., 'AI-Based Solution Amongst 6 COVID-19 Projects Receive Government Support' (2020) NDTV Gadgets 360 https://gadgets.ndtv.com/science/news/technology-developmentboard-covid-19-coronavirus-tech-projects-approval-facial-recognition-2232056 accessed 17 April 2025.

[52] The Indian Express, 'Pune Police Use Drones To Track Home-Quarantined Persons' (29 March 2020) https://indianexpress.com/article/cities/pune/pune-police-use-drones-to-track-home-quarantined-persons-6337618/ accessed 17 April 2025.

[53] Telangana Today, 'Telangana Government Plans to Replace Biometric Attendance with Facial Recognition Post-COVID-19' (2020).

inaccurate conclusions. In some cases, these systems are rooted in outdated and discriminatory theories, such as phrenology and physiognomy, which have historical ties to eugenics, thus reinforcing harmful biases. The data used for training these systems such as face databases and biometric information are often collected without consent, facilitating both widespread and targeted surveillance that is discriminatory by design. The more individuals can be instantly identified and tracked in public spaces, the more their human rights and civil freedoms are compromised.

The use of facial recognition technology (FRT) has sparked concerns regarding discriminatory surveillance based on factors like socioeconomic status, caste, gender, and race. Since FRT relies heavily on its base dataset, it is crucial to ensure that these training datasets represent a broad range of characteristics that reflect the diversity of the real world. Algorithms are typically tested on these datasets to assess their performance. To enhance accuracy, it is important that these datasets capture the full spectrum of gender, age, skin tone, and other demographic factors, avoiding disproportionate representation of any particular group. These considerations should be addressed during the procurement phase of the technology. Reducing false negatives and false positives is vital to improving FRT effectiveness and preventing unjust treatment of individuals. As mentioned, the quality of images and the underlying algorithm play a critical role in determining the accuracy of FRT. The National Institute of Standards and Technology (NIST) has established international standards to assess the accuracy of such systems and identify optimal conditions for their use. Recognizing these limitations is essential during the due diligence process.

VIII. SUGGESTION AND CONCLUSION

- Purpose Limitation: It is essential to have a clear policy of purpose limitation, which ensures that data is collected only for specific, legitimate purposes. Clearly defining and restricting the use of data to its intended purpose reduces the risk of potential misuse and harm.[54]
- Regulation and Oversight: Establishing independent oversight bodies is crucial for addressing concerns related to data collection, processing, storage, and usage. This includes determining who will have access to the data, how long it will be stored, and the safeguards to prevent misuse. Additionally, oversight bodies must ensure

[54] Matthan, R., Venkataraman, M. and Patri, A., 2018. *A Data Protection Framework for India*. [online] Takshashila.org.in. Available at: http://takshashila.org.in/wp-content/uploads/2018/02/TPA-DataProtection-Framework-for-India-RM-MV-AP-2018-01.pdf [Accessed 17 April 2025].

transparency and conduct impact evaluations of facial recognition technology (FRT).

- Citizen Oversight: The incorporation of citizen oversight boards can serve as a useful check on surveillance practices, ensuring accountability through public pressure. The framers of the Indian Constitution envisioned citizens as the ultimate source of authority, and applying this principle to surveillance would strengthen public trust. Some US cities, such as Cambridge, require police departments to obtain City Council approval before acquiring or using surveillance technology. These cities also mandate regular reports on data handling practices and safeguards to protect civil liberties.

If not restricted, law enforcement agencies should be required to disclose the algorithms used in facial recognition technology (FRT), including information on their accuracy, the sources of data, and any biases identified during testing. Transparency is crucial for building public trust and allows for external scrutiny to address concerns regarding the ethical use and effectiveness of these technologies. FRT protocols should incorporate safeguards to prevent biases that disproportionately affect marginalized communities, particularly addressing higher error rates and profiling risks. Establishing specific accuracy standards tailored to diverse demographic groups could help mitigate the risk of unjust targeting.

Strict guidelines should be implemented to govern the storage, access, and retention of data. This should include secure data storage practices, restricting access to authorized personnel only, and enforcing short retention periods for data that is no longer relevant to active investigations.

It is essential to inform communities about the use of FRT through public disclosures, impact assessments, and transparent reporting. Engaging with the public helps ensure accountability and ensures that the deployment of FRT takes into account community concerns and the ethical implications.

When people's private lives are accessible at the touch of a button, minor missteps or youthful mistakes could be permanently etched in the digital world, overshadowing their entire identity. This permanent record of one's actions poses a significant risk, as it can define individuals by their most vulnerable moments, rather than their whole life's worth of character and integrity. Unlike lies, which may be corrected, the damage caused by uncomfortable truths is much harder to repair. The permanence of such information, often captured in public spaces, feels unjust—personal interactions from years ago can continue to define a person. This digital permanence undermines the reputational efforts people invest in, and forces individuals to live under the constant shadow of their past mistakes. Life should not demand that a person forfeit the hope

of being remembered for more than their lowest points.

*****

 [ISSN 2581-5369]