International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 12 | Dec 2025 www.irjet.net p-ISSN: 2395-0072

The Privacy-Bias-Accountability Triad: Diagnosing Systemic Ethical Failures in Facial Recognition Technology

Rania Khan[1], Safa Fatima[2], Nazifa Hajwane[3], Shashi Saxena[4], Prof Ashok Yadav[5]

[1] Student, Department of Information Technology, Reena Mehta College of Arts, Commerce, Science & Management Studies, Mira Bhayandar West, Maharashtra 401101
[2,3,4] Student Department of Information Technology, Reena Mehta College of Arts, Commerce, Science & Management Studies, Mira Bhayandar West, Maharashtra 401101
[5] Prof and Head of department (Department of information technology), Reena Mehta College of Arts, Commerce, Science & Management Studies, Mira Bhayandar West, Maharashtra 401101, India

---

Abstract - *Facial recognition technology (FRT) is a rapidly growing technology that has already established its presence in many sectors, offering great benefits in terms of security, convenience, and efficiency. At the same time, however, the technology's coming into use on such a large scale poses many ethical issues that are serious enough to attract the attention of scholars. The ethical scenario related to FRT is presented in a thorough manner in this paper, which discusses the three major aspects: individual privacy violation, systemic algorithmic bias, and institutional accountability. A qualitative research design that comprises systematic literature review, legal-policy mapping, and case-study synthesis is used to process the data and come up with the current state of ethical debate and regulatory response. The main results show that there is a conflict between technological utility and fundamental human rights, which happens to be the case with anonymity, dignity, and non-discrimination issues. The paper proposes a conceptual model (the Privacy–Bias–Accountability Triad) to clarify the relationship between these ethical dimensions. In the absence of strong regulatory frameworks, the ethical risks that are brought about by FRT can exceed the social benefits*

***Key Words*: Privacy, Algorithmic Bias, Accountability, Surveillance, Ethics, Facial Recognition, Governance.**

1. INTRODUCTION

The widespread use of digital technologies has led to the point where biometrics, and especially facial images, is used more and more often as identifiers. Face Recognition Technology (FRT) relies on deep learning algorithms to map and authenticate facial features and thus becomes a revolutionary tool in security, commerce, and everyday digital activities. Its uses range. From unlocking smartphones to recognizing people in large gatherings, and still continue to grow. However, as its use moves away from controlled settings into over-the-top public surroundings, the ethical implications become clearer. FRT raises questions about the right to stay anonymous, the need for consent, and the quality of participation in democratic processes. Newer literature has pointed out that privacy loss and lack of governance in AI surveillance systems are among the main concerns [1], [2], [8]. The paper addresses how the societies can Coe exist the legitimate advantages of FRT and simultaneously protect individual rights.

1.1 BACKGROUND AND CONTEXT

The development of FRT was particularly fast at the end of the 20th century and the beginning of the 21st century when it changed from basic pattern-matching systems to complicated neural networks that could do high-speed recognition. The use of FRT by both the public and private sectors has been the main topic of a worldwide discussion about the extent of privacy invasions, misuse of data, and worst- case scenarios. Among the fears are constant surveillance, police overreach, and biometric monitoring becoming commonplace.

1.2 STATEMENT OF THE PROBLEM

The use of unregulated FRT in many places presents a threat to democratic values and civil liberties, although it does have operational benefits. Without a globally accepted standard, societies will suffer the consequences of privacy violations, inequitable outcomes, and lack of responsibility. Wrong identification in law enforcement creates serious ethical and legal risks such as wrongful arrests and discrimination against races [9].

1.3 RESEARCH OBJECTIVES

1. Determine the manners in which FRT violates individual's right to privacy.
2. Look into the factors and consequences of bias in algorithms that come with FRT systems.
3. Examine the regulations that are there to hold FRTs accountable in cases of misuse and mistakes.
4. Build a concept model that connects the areas of privacy, bias, and accountability.

1.4 SIGNIFICANCE OF THE STUDY

By bringing the ideas of privacy, bias, and accountability together into one analytical model, the research puts forward an important argument in technology ethics. The results do not only help decision-makers in designing regulations but also provide support to developers in incorporating ethics into their designs, and make the public more aware of the social trade-offs that come with biometric surveillance.

2. LITERATURE REVIEW

2.1 Technical Literature

Technical literature shows that FRT accuracy is very much affected by light conditions, angle of the face, resolution, and demographic factors. A pioneering work by Buolamwini and Gebru pointed out large differences in racial and gender performance of the commercial systems [1]. The 2023–2024 multistage survey credits the entire FRT pathway—image capturing to verification—with racial bias and indicates that training data and system architecture are the main sources of this bias [2]. The 2025 review of privacy-preserving FRT methods is inclined towards synthetic data, cryptographic masking, and federated learning architectures, but it still warns that there is large accuracy–privacy trade-offs [10].

2.2 Legal and Regulatory Literature

According to legal literature, the regulatory framework is fragmented. The GDPR is the provider of some of the strictest biometric safeguards in Europe whereas most other parts of the world have no similar regulations. The U.S. is rather decentralized in that it adopts city level restrictions instead of federal regulations. A 2024 review suggests that the inconsistencies in privacy enforcement and governance are still remote, even though AI regulatory efforts are coming up [8].

Table -1: Selected Global Regulatory Responses to FRT

Country/City	Type of Action	Year	Description
San Francisco, USA	Government Ban	2019	First major city to ban police use of FRT.
Boston, USA	Citywide Ban	2020	Prohibited use by city agencies due to civil rights concerns.
European Union	Proposed AI Act	2021	Restricts real-time biometric surveillance in public spaces.
Toronto, Canada	Temporary Moratorium	2022	Halted FRT use in public housing due to privacy risks.
India	No Formal Ban	—	Police use continues; Legal frameworks under debate.
UK (London)	Regulated Use	2020	Police use allowed with strict proportionality rules.

2.3 Ethical Discourse

Ethics has raised eyebrows at "surveillance capitalism," the continuous tracking of people's behavior's which, according to the critics, leads to the demise of control and anonymity [4]. The ethical issues become more serious when the FRT application spreads beyond its initial deployment gaining the infamous "mission creep" label. The existing accountability mechanisms are weak; hence they do not challenge and control the prevailing privacy violations and the biased outcomes. The contemporary academic debate emphasizes that lack of accountability boosts, privacy and bias harms [11].

2.4 Identification of research gaps

Literature comprehensively covers the issues of privacy and harms caused through algorithmic biases but does not connect the concepts of accountability as a major factor that influences both. Moreover, in the rare cases where all three factors - liability, auditability, and transparency - are brought together, they are not included in the governance models. The proposed study fills this gap by using the PBA Triad.

3. RESEARCH METHODOLOGY

3.1 Research Design

The basis of this investigation is a systematic review of the preexisting literature regarding the Facial Recognition Technology's (FRT) ethical landscape. In addition, we conducted a comparative policy analysis to assess the various regulatory measures. This qualitative method is very suitable for addressing multidimensional ethical issues, where interpretation and normative reasoning play a central role.

3.1 Data Collection Methods

We aimed at forming a complete understanding and therefore, we took the literature from four major academic databases: Google Scholar (to get the widest coverage), IEEE Xplore (for the technical side), Scopus (for the social

sciences), and JSTOR (for law and philosophy area). Our search was based on a strategy that was specific with terms like "facial recognition", "ethics", "privacy", "bias", and "accountability" to find the most relevant literature. Our main focus was on the publications made between 2018 and 2025 covering both the basic studies [1, 4], and the latest debates [2, 8, 10, 11].

3.2 Sampling Technique

The most informative sources were selected following a purposive sampling. This implies that we used the fixed criteria: the included sources must be peer-reviewed articles or major institutional reports that offer in-depth information on privacy, bias or accountability in FRT. Technical papers lacking an ethical discourse were excluded. The selection procedure consisted of an initial screening of titles and abstracts followed by a full-text reading to filter a large initial set of results down to a focused and high-quality literature collection which was then subjected to in-depth analysis.

3.3 Data Analysis Methods

The literature selected was analyzed in two interlinked steps:

3.4.1. Thematic Analysis: First of all, we read and reread the texts thoroughly, and in doing so, we pinpointed and coded the main areas of discourse and arguments that came up repeatedly (for example, loss of anonymity or demographic disparity). These codes were then gathered and assigned to the overarching themes that form the backbone of this paper's findings: Privacy infringement, algorithmic bias, and the accountability deficit.

3.4.2. Normative Synthesis: Next, we went further than just mere theme identification; we went a critical evaluation of the arguments, and weighed opposing values and solutions. It was during this process of synthesis that the Privacy–Bias–Accountability (PBA) Triad emerged as a new model to show how the ethical challenges are interrelated.

4. CONCEPTUAL MODEL: THE PRIVACY BIAS ACCOUNTABILITY (PBA) TRIAD:

The PBA Triad demonstrates the dynamic interaction of the three dimensions of privacy, bias, and accountability:

- **Privacy:** FRT leads to the risk of anonymity loss, purpose creep, and violation of consent.
- **Bias:** The problems relate to the differences in accuracy, misidentification, and impact on certain groups.
- **Accountability:** There are issues such as lack of liability, absence of auditing, and poor redress mechanisms.

An accountability failure will result in an escalation of privacy and bias issues while a biased system will erode the trust in privacy safeguards. This comprehensive model is the basis for ethical governance.

5. RESULTS AND DISCUSSION

Table -2: Summary of Key Ethical Challenges in FRT Deployment.

Ethical Concern	Domain Affected	Observed Consequence
Privacy Violation	Individual Rights	Chilling effect on freedom of speech and assembly; loss of anonymity in public spaces.
Algorithmic Bias	Social Equity	Misidentification, wrongful arrests, discrimination in access to services.
Accountability Deficit	Governance & Rule of Law	Institutional denial of responsibility, slow regulatory response, lack of redress for harm.

5.1 Privacy as the Central Ethical Loss

FRT is one of the most significant violations of privacy among the ethical issues in present-day automated facial recognition technology. Although it is to a certain extent possible to revoke consent to the processing of facial data, that is often not true for the purposes the data has been repurposed—this is the case of function creep. Effective privacy protections must therefore always be structural safeguards preventing misuse, extending beyond the mere consent given by the data subjects.

5.2 Persistence of Algorithmic Bias

The occurrence of bias in FRT is not simply a technical error, but it signifies a whole system problem that is caused by entering prejudiced datasets, building models poorly, and allowing wrong socio-technical deployment contexts. Analysis throughout the 2024 pipeline confirmed the existence of racial disparities at every phase [2]. Policing studies conducted in recent years demonstrate that the enforcement contexts augment such biases, leading to a mix of wrongful arrests and racial disparity [9].

5.3 Accountability Deficit

Failures to hold accountable represent one of the main gaps in governance. It is the ambiguity whether the responsibility lies with the developers, integrators, or deplorer's that allows them to evade liability. In the absence of external audits and mandated transparency, commitments in the areas of privacy and fairness will be ineffective as there will be no means of enforcing the rights of the subjects involved. The PBA Triad highlights that accountability is the key on which the privacy and fairness protection rely.

6. COMPARISON WITH PREVIOUS STUDIES

The disclosure of privacy violations and discrimination by the technology confirmed the basic concepts of the researchers like Zuboff [4] and Buolamwini & Gebru [1]. However, the main contribution of the current paper is not to highlight these problems again but to link them through the Privacy–Bias–Accountability (PBA) Triad. Previous studies have frequently analyzed these issues separately, but this framework shows their inherent connections and puts the lack of accountability as the main problem that exacerbates privacy and bias harms. One example is that the image of bias is [1, 3] while the ethical prescription of [4] points morality in terms of surveillance; the PBA Triad acts like a common diagnostic framework linking the cause (accountability failure) to the effect (privacy and bias harms). This integrated view, alluded to in the budding governance literature [11], is here mapped out as a unified framework, thus presenting a new way of looking at the diagnosing and solving of the systemic ethical failures of FRT.

7. CONCLUSION AND RECOMMENDATIONS

7.1 Summary of Key Findings

The findings of this study are that the ethical challenges of facial recognition technology (FRT) are not independent matters, but rather an intra-acted coming together of the issues of privacy invasions, algorithmic bias, and presumably lack of accountability. The use of the PBA Triad model leads to the conclusion that no issue can be resolved without to couple it with others. The latter cannot be solved without integrated governance that at the same time secures the privacy rights of individuals, guarantees fairness in the algorithmic process, and gives accountability to the developers and users of the FRT. If not, the use of FRT will remain a double-edged sword cutting deeper into democratic values and social justice.

7.2 Limitations of the Study

This research being only a qualitative study and being based on literature review does not have the full authority that empirical research can give. In fact, the findings would gain more weight and strength through taking into account and reporting the psychological and behavioral impact of FRT surveillance on different communities.

7.3 Suggestions for Future Research

- **Standardized Audit Frameworks:** The first step is to create and validate very specific and replicable protocols for the bias audits in FRT systems that will include the use of standardized datasets and metrics for evaluation.
- **Cross-Cultural Governance Models:** The next point is to carry out comparative studies of FRT regulation in different political and cultural contexts to identify best practices that can be transferred.
- **Technical Solutions Evaluation:** The third suggestion is an empirical assessment of the use of privacy-enhancing technologies (PETs) in real-world FRT deployments, with a focus on the trade-offs between privacy preservation and system performance.
- **Longitudinal Behavioral Studies:** Finally, research is suggested to measure the impact of long-term exposure to FRT surveillance on public behavior, free expression, and participation in public life among various demographic groups

7.4 Practical Recommendations

- **Tiered Moratorium:** Disallowing facial recognition technology (FRT) in mass surveillance and social scoring would be an immediate measure, meanwhile pre-approval criteria would be applied for the public-sector applications of FRT that are not yet in place.
- **Mandatory Algorithmic Auditing:** Prior to the deployment of new technologies, the requirement will be for an independent, third-party bias audit, followed by regular audits, with the results and plans for dealing with any issues made public.
- **Clear Liability Frameworks:** It is essential to map out the responsibility of all actors at each stage of the FRT lifecycle—from developers and integrators through end-users—so that there are clear routes to legal action when people suffer harm.
- **Data Governance Protocols:** The rigour of data governance applied would include no more data being kept than necessary, specific purposes for which data is collected, and the imposition of timelines for deletion, with technical safeguards such as encryption and federated learning deployed additionally.
- **Adopt an Integrated Governance Approach:** The PBA Triad is one of the frameworks regulators could use to ensure that a policy addressing one ethical dimension—privacy, for example—does not inadvertently exacerbate others— such as by making the surrounding systems less transparent and accountable.
- **Multi-Stakeholder Oversight:** Regulatory frameworks should create independent oversight bodies, with public representation, to approve and monitor the deployment of facial recognition technology (FRT), especially in sensitive areas such, as law enforcement and public services.

REFERENCES

[1] J. Buolamwini and T. Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," Proc. FAT, pp. 77–91, 2018.

[2] S. Yücer et al., "Racial Bias Within Face Recognition: A Survey," arXiv:2305.00817, 2023.

[3] I. Raji and J. Buolamwini, "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results," Proc. AAAI/ACM AIES, pp. 429–435, 2019.

[4] S. Zuboff, The Age of Surveillance Capitalism. PublicAffairs, 2019.

[5] European Commission, "Artificial Intelligence Act," COM (2021) 206 final, 2021.

[6] Privacy International, "Facial Recognition: A Threat to Privacy, Democracy, and Freedoms," 2020.

[7] G. Smith and T. Miller, "Regulating Facial Recognition Technology: Balancing Innovation and Human Rights," Computer Law & Security Review, vol. 41, 2021.

[8] X. Wang et al., "Beyond Surveillance: Privacy, Ethics, and Regulations in Face Recognition Technology," Frontiers in Big Data, 2024.

[9] S. Pour, "Police Use of Facial Recognition Technology and Racial Bias," American Journal of Artificial Intelligence, vol. 7, no. 1, pp. 17–23, 2023.

[10] "Ensuring Privacy in Face Recognition: A Survey on Data Generation, Inference and Storage," Discover Applied Sciences, vol. 7, 2025.

[11] "A New Epoch of Face Analytics: Technological Evolution Through Ethical and Legal Challenges," AI and Ethics, 2025.