Page 291 - 304 **DOI:** *https://doij.org/10.10000/IJLSI.112317*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 6 | Issue 6

2024

Facial Recognition Technology (FRT) and Privacy: A Delicate Balance

LAKSHMI POOJA K.[1] AND SHRUTHI B.[2]

ABSTRACT

The swift advancement of facial recognition technologies (FRT) has created challenging ethical dilemmas regarding the trade-off between personal privacy and public safety. The conflict between developing AI technologies and upholding private rights is examined in this paper. This paper examines the complex ethical, regulatory, and privacy issues surrounding the rapid deployment of Facial Recognition Technology (FRT) by law enforcement agencies in the United States (US), United Kingdom (UK), European Union (EU), and India. With FRT becoming a critical tool for crime investigation, public surveillance, and identity verification, its increased use by governments and law enforcement has raised significant concerns about privacy, civil liberties, and potential biases in implementation. In India, the widespread adoption of FRT has highlighted the country's lack of a comprehensive legislative framework, as the Digital Personal Data Protection (DPDP) Act remains under consideration, leaving biometric data largely unprotected. While the US, UK, and EU have introduced various regulatory measures, none fully address the potential for misuse of FRT, with the US notably lacking federal oversight and relying on a fragmented state-level approach. By contrast, the EU's General Data Protection Regulation (GDPR) and the proposed AI Act set a higher standard, demanding accountability and transparency. This paper explores the ethical challenges associated with balancing public safety, innovation, and personal privacy. Ultimately, it concludes that a global regulatory standard and stricter oversight measures are essential for responsible FRT deployment, ensuring that technological advancements do not compromise fundamental human rights. There is no standardized global human rights framework or regulatory requirements that can be directly applied to the rollout of facial recognition technology (FRT).

***Keywords**: Facial recognition technology, Data Protection, Artificial Intelligence (AI), Privacy, Transparency, Regulation, Innovation.*

I. INTRODUCTION

Law enforcement agencies around the world are continually exploring new technologies to

[1] Author is a student at SASTRA Deemed University, India.

[2] Author is a student at SASTRA Deemed University, India.

enhance their ability to detect and prosecute crimes, thereby ensuring the safety of citizens and society as a whole. Additionally, there is public pressure to demonstrate value for money and to seek economic efficiencies, which new technologies can help achieve by reducing labour costs. Over the past decade, various technologies have been adopted by law enforcement, including surveillance cameras, automated license plate readers, body cameras, drones, and most recently, facial recognition technologies (FRT).Law enforcement agencies have been leaders in adopting facial recognition technology (FRT) because of its perceived benefits.

However, each of these technologies alters the dynamics between law enforcement personnel and citizens, necessitating the establishment of new boundaries and updated accountability standards. Numerous questions regarding the use of facial recognition technology (FRT) and artificial intelligence (AI) remain unresolved. The application of FRT by law enforcement agencies serves as a compelling case study for examining the broader ethical implications of FRT and AI. It highlights a clear example of personal data usage and its significant effects on individual rights. This article explores these multifaceted issues, beginning with an overview of FRT and examining its use in law enforcement across jurisdictions such as the United States (US), United Kingdom (UK), and European Union (EU), each of which has implemented varying degrees of regulatory oversight to mitigate FRT’s potential risks. In these regions, data protection laws like the EU’s General Data Protection Regulation (GDPR) and the UK’s Data Protection Act provide specific guidelines for biometric data usage. However, these frameworks also reveal gaps in addressing FRT-specific challenges, such as potential biases and surveillance overreach, underscoring the need for more robust regulations.

Comparatively, in India, FRT usage by law enforcement has expanded without a dedicated regulatory framework to protect citizens’ data privacy, despite its potential for misuse in mass surveillance. India’s Digital Personal Data Protection (DPDP) Act, 2023, is a recent attempt to safeguard personal data, including biometric information, but lacks FRT-specific guidelines. This contrasts with the GDPR and proposed AI regulations in the EU, which impose strict rules on biometric data and high-risk AI applications. India's reliance on broad exemptions for law enforcement data processing further highlights the regulatory gap, prompting calls for tailored regulations to prevent privacy infringements and ensure accountability.

II. Facial recognition technologies (FRT)

Facial recognition technology (FRT) is a sophisticated biometric system that utilizes artificial intelligence (AI) to identify and verify individuals based on their facial features. The process begins with capturing an image or video of a person's face, which is then converted into a digital format. Advanced algorithms analyse facial geometry, focusing on key features such as the distance between the eyes, the shape of the jawline, and the contours of the cheeks. This data is transformed into a unique mathematical representation known as a facial template.

FRT systems typically operate in two main modes: identification and verification. In identification mode, the system compares the captured facial template against a database of known faces to find a match, while in verification mode, it confirms whether a specific individual matches a provided facial template. The technology relies heavily on machine learning techniques, allowing systems to improve their accuracy and efficiency over time by learning from new data. Recent advancements in deep learning and neural networks have further enhanced FRT capabilities, enabling real-time processing and increased accuracy in diverse environments.

However, these improvements also raise concerns regarding privacy and ethical implications, particularly when deployed in public spaces without consent. As FRT becomes increasingly integrated into law enforcement, security, and commercial sectors, understanding its technical workings is crucial for assessing its impact on society and individual rights.

With the goal of connecting "identity to the body," facial recognition systems are biometric identification and classification technologies driven by artificial intelligence. These facial recognition technologies identify people by comparing their distinct traits with pictures or videos of faces stored in a database. For example, law enforcement organizations can only use facial recognition technology to identify a suspect from a video if they have access to a database containing the suspect's face data, such as a database of known offenders[3].

Since the nineteenth century, facial photographs and their detailed examination have been regarded as crucial resources by law enforcement agencies. The emergence of facial recognition technology (FRT) in the twenty-first century has significantly modernized this practice, transitioning from manual analysis to automated processes that use artificial intelligence (AI) and algorithms.

This shift facilitates the automatic extraction and comparison of facial features, allowing for precise measurement of even the smallest details[4].On a scale of how it fits with people' security vs confidentiality issues in various scenarios, the bigger picture of the FRT deployment and data gathering may be crucial. Lenovo introduced a new line of laptops in 2008 that could

[3] Gates, K.A.: Our Biometric Future. Facial Recognition Technol- ogy and the Culture of Surveillance. New York University Press, New York (2011) https://ijoc.org/index.php/ijoc/article/viewFile/1278/570

[4] Mann, M. and Smith, M. (2017) ‘Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight’ University of New South Wales Law Journal 40, no. 1 (2017)

identify the face of an authorized user in place of a password.

III. The EU and UK legislative landscape for FRT in a law enforcement context

Facial Recognition Technology (FRT) has emerged as a powerful tool for law enforcement, offering enhanced capabilities for identifying suspects, monitoring public spaces, and streamlining investigations. However, its increasing use has raised significant concerns around privacy, data protection, and civil liberties. Both the European Union (EU) and the United Kingdom (UK) have implemented robust legislative frameworks that, while not explicitly targeting FRT, have significant implications for how the technology is governed.

One of the most critical pieces of legislation affecting FRT in both regions is the General Data Protection Regulation (GDPR), introduced in 2018 to protect personal data and ensure privacy rights for individuals across the EU. Although the GDPR was enacted while the UK was still a member of the EU, it was incorporated into UK domestic law through the Data Protection Act 2018 and continues to apply post-Brexit. GDPR is widely regarded as setting the global standard for data protection and privacy, and its influence extends beyond the EU due to its extraterritorial scope, applying to any company that processes the personal data of EU residents, regardless of location.

This has led to the so-called "Brussels Effect," where non-EU companies adhere to GDPR standards to continue doing business in the region. Under GDPR, personal data must be processed lawfully, fairly, and transparently, with collection limited to specific, legitimate purposes, a principle especially relevant for FRT, as biometric data, including facial images, is categorized as sensitive personal data. Biometric data, such as facial features, fingerprints, and DNA, is considered highly sensitive under GDPR. Article 9 of the regulation prohibits the processing of biometric data for identifying individuals unless certain conditions are met, such as obtaining explicit consent from the data subject or fulfilling an exception, like processing for reasons of substantial public interest or law enforcement purposes.

The processing of biometric data for law enforcement falls under Article 23, allowing for derogations in cases of national security, defence, or public safety, provided strict oversight and legal justifications are in place. Furthermore, GDPR mandates the implementation of "Privacy by Design" and "Privacy by Default," principles requiring privacy protections to be embedded into systems and processes from the outset. In the case of FRT, this involves minimizing the collection of personal data, ensuring secure storage, and preventing unauthorized access, while Privacy by Default demands that default settings offer the highest level of privacy protection, such as limiting data retention periods and anonymizing data where possible.

Each EU Member State has a designated national data protection authority (DPA) responsible for overseeing GDPR compliance, with the European Data Protection Supervisor (EDPS) overseeing EU institutions, while the UK's Information Commissioner's Office (ICO) plays a similar role domestically. These authorities have the power to investigate data breaches, issue fines, and enforce corrective actions, and in cases involving FRT, they may scrutinize how law enforcement agencies handle biometric data to ensure compliance with GDPR and other regulations.

Beyond GDPR, the European Convention on Human Rights (ECHR), which is enshrined in UK law through the Human Rights Act 1998, plays a crucial role in regulating the use of FRT by law enforcement. Article 8 of the ECHR protects the right to privacy, guarding individuals against arbitrary interference with their private lives, raising concerns about whether the widespread use of FRT in public spaces constitutes mass surveillance and infringes on privacy rights.

However, the ECHR also recognizes that certain rights, including the right to privacy, can be restricted for public safety or national security reasons, provided such restrictions are necessary, proportionate, and legally prescribed. Balancing the interests of law enforcement and individual privacy rights is a complex issue that frequently requires judicial intervention. Individuals can challenge the use of FRT in national courts, and in the EU, cases may progress to the European Court of Human Rights (ECtHR). Although the UK is no longer part of the EU, it remains a signatory to the ECHR, allowing UK citizens to bring cases before the ECtHR. Despite existing legal frameworks, there has been growing pressure for both the EU and the UK to impose stricter regulations or even a moratorium on FRT's use by law enforcement.

Critics argue that FRT poses significant risks to privacy, may lead to discriminatory outcomes, and lacks adequate transparency and accountability. High-profile cases of FRT misidentifying individuals, particularly within minority groups, have fuelled concerns about bias and potential human rights violations. Several advocacy groups have called for a halt to FRT use until comprehensive regulations address these issues.

While the EU has not yet imposed a blanket moratorium, it is currently considering the Artificial Intelligence Act (AIA), a proposal aimed at regulating high-risk AI systems like FRT. The AIA could introduce stricter oversight mechanisms and clear standards for AI's use in law enforcement, although its final form is still under debate. The use of FRT by law enforcement thus presents a complex regulatory challenge, with implications for privacy, civil liberties, and public safety. While neither the EU nor the UK has enacted laws explicitly governing FRT, existing legislation such as GDPR and the ECHR provides a robust framework for regulating its use.

However, the evolving nature of technology and growing concerns about potential misuse have led to calls for more specific and stringent regulations. As this debate continues, both the EU and the UK must carefully balance the benefits of FRT for law enforcement with the need to protect individual rights, ensuring transparency and accountability in its deployment.

IV. USA’S LEGISLATIVE LANDSCAPE IN FRT

The legislative landscape for facial recognition technology (FRT) in the United States presents a far more fragmented and less robust framework compared to the European regulatory environment. While Europe has established overarching data protection laws such as the General Data Protection Regulation (GDPR) to govern the use of personal data and ensure ethical considerations, the United States lacks a comparable federal law, leaving FRT largely unchecked in many contexts. FRT is widely used by law enforcement across the U.S., impacting over 117 million adults—more than a third of the country’s population. Despite this extensive use, the average citizen has very limited means to hold operators accountable in the event of misuse. Although the U.S. was an early adopter of freedom of information laws, passing the federal Publication Information Act in 1966 with state-specific laws following, there remains no unified approach to data privacy that could offer protection on par with GDPR in Europe.

Instead, the U.S. relies on sector-specific privacy laws, such as the Children's Online Privacy Protection Act (COPPA), which only cover narrow areas of personal data protection. These laws are enforced by the Federal Trade Commission (FTC), which has a broad mandate to protect consumers from deceptive practices, but the FTC lacks the specialized authority and regulatory power of data protection authorities found in Europe. This gap is particularly problematic given the massive deployment of FRT, as there is no central regulatory body or ombudsman tasked with investigating potential misuse or ensuring that FRT operators act transparently. Instead, accountability largely falls on individual citizens, who must resort to legal action if they wish to challenge the improper use of FRT. The absence of a dedicated data protection authority at the federal or state level leaves citizens without an entity to actively protect their interests, and they must initiate court proceedings to address conflicts regarding FRT and the associated handling of personal data. This process can be lengthy, expensive, and inaccessible for many people, particularly since U.S. law does not allow for the kind of administrative enforcement actions seen in Europe, where data protection authorities can intervene on behalf of citizens without requiring court involvement.

The considerable state-by-state differences in data privacy laws further exacerbate this issue. While certain states like California have made strides with more comprehensive data protection laws, such as the California Consumer Privacy Act (CCPA), many other states have little to no regulation governing the use of FRT. The lack of consistent standards across the country means that FRT operators may face stricter oversight in some states while operating with near- total impunity in others. This inconsistency creates a patchwork of protections that makes it difficult for individuals to know their rights or to expect uniform enforcement of those rights. Additionally, there is a notable lack of transparency requirements around the use of FRT in many jurisdictions. Unlike Europe, where GDPR requires clear legal justifications and explicit consent for processing biometric data, the U.S. often lacks such mandates, leaving citizens in the dark about when and how their facial data is being collected or used.

This reliance on individual action to hold FRT operators accountable highlights the weakness of the current U.S. framework. In many cases, individuals must seek legal assistance from non-profit organizations, as the cost and complexity of legal battles can be prohibitive. Those unable to secure such support may find it impossible to challenge the misuse of FRT or to demand transparency from operators. Without a centralized regulatory authority to investigate, monitor, or enforce compliance with ethical standards, the U.S. system puts the burden squarely on individuals. This absence of robust, proactive oversight is a significant cause for concern, especially as FRT becomes more widespread in law enforcement and other sectors. While Europe’s regulatory framework ensures that data protection authorities can step in and enforce decisions without needing lengthy court battles, the U.S. approach leaves many citizens without recourse, particularly those without the financial or legal resources to initiate court proceedings. This disparity between the U.S. and European approaches underscores the challenges of implementing FRT ethically and transparently in a legal environment that lacks strong data protection laws or a centralized body to enforce citizens' rights.

V. INDIA'S LEGAL FRAMEWORK FOR FACIAL RECOGNITION TECHNOLOGY

In India, the use of Facial Recognition Technology (FRT), particularly by law enforcement, has been expanding, but the country currently lacks a comprehensive legislative framework that specifically governs its deployment. FRT is increasingly being adopted by law enforcement and security agencies in India for a range of applications, including:

- **Crime investigation**: Identifying suspects, locating missing persons, and detecting criminal activity.
- **Public surveillance**: Monitoring public spaces like airports, train stations, and protests for security purposes.
- **Verification of identity**: Use in government schemes such as the Aadhaar- based identification system and voter verification.

India does not yet have a robust data protection law similar to the EU's GDPR. The Personal Data Protection Act, first introduced in 2019, aims to address issues of data protection and privacy but has not been passed into law as of yet. The act was reintroduced in an updated form as the Digital Personal Data Protection (DPDP) Act in 2023, which is currently under consideration.

Section 5 of the **Digital Personal Data Protection (DPDP) Act** emphasizes the principle of *data minimization* and the need to process personal data strictly for specified purposes. This means that for Facial Recognition Technology (FRT), any entity processing facial data (such as law enforcement or private organizations) must collect only the minimum amount of data necessary to achieve their intended purpose. Moreover, the data collected should not be stored longer than required, and its use should align with the specified reason for collection. For FRT in particular, Section 5 implies that organizations must justify why facial data is necessary and must implement robust safeguards to ensure that any data captured through FRT is used exclusively for the designated purposes—such as identification, verification, or security. The widespread use of FRT by law enforcement in India has raised significant concerns, including:

1. **Lack of transparency**: There are few publicly available details about how law enforcement agencies use FRT, which raises questions about accountability.
2. **Potential for mass surveillance**: Critics argue that FRT can be used to monitor individuals without their consent, leading to potential human rights violations.
3. **Bias and accuracy**: Similar to global concerns, there are worries that FRT systems in India may suffer from biases that disproportionately affect marginalized communities and minorities, leading to discriminatory outcomes.

The Information Technology (IT) Act, 2000 is India's primary law governing electronic commerce, cybercrime, and electronic data. However, it does not specifically regulate or protect against the use of Facial Recognition Technology (FRT). The IT Act primarily addresses cyber offenses, electronic records, and data security but lacks provisions for biometric data, such as facial images, and its use in technologies like FRT.

1. **Section 43A**: This section mandates that companies handling sensitive personal data must implement reasonable security practices. While this includes biometric data, it is more applicable to private companies and less relevant to government use of FRT.
2. **Section 72A**: It penalizes unauthorized access to personal data, which could extend to facial recognition data if misused. However, this does not provide comprehensive protection in cases of government surveillance or law enforcement use of FRT.

The Criminal procedure (identification) act, 2022: It outlines provisions that indirectly relate to **Facial Recognition Technology (FRT)** by allowing for the collection and processing of biometric and other identifying data of individuals involved in criminal investigations. Here are the key provisions in the Act relevant to FRT:

1. Definition of Measurements (Section 2(b))

Inclusion of Biometric Data: The term "**measurements**" includes not only physical attributes like fingerprints, palm prints, and footprint impressions but also photographs, iris and retina scans, which can encompass facial data used in FRT. This provision grants authority to collect and process facial images that are necessary for FRT.

2. Collection from Various Categories of Persons (Section 3)

The Act specifies that biometric and facial data can be collected from:

- Convicted individuals;
- Individuals ordered to provide security for good behaviour;
- Individuals arrested or detained under preventive detention laws.

However, biological samples (e.g., DNA) need not be collected unless the offense involves certain types of crimes against women or children or is punishable with seven years or more of imprisonment. This restriction does not specifically extend to facial data, implying FRT-related data can be broadly collected for investigative purposes.

3. Centralized Data Collection and Retention (Section 4)

National Crime Records Bureau (NCRB) is responsible for collecting, storing, processing, and sharing records of "measurements" (which include facial scans). This includes:

- Collecting biometric recordsfrom State Governments and law enforcement.

- Storing data for up to 75 years, which implies long-term retention of FRT- related data.
- Sharing and disseminating data with law enforcement agencies for investigative purposes.
- Destruction of records is mandated if a person is acquitted or discharged, but only after exhausting all legal remedies.

4. Magistrate's Order for Data Collection (Section 5)

Magistrates are empowered to order individuals to submit to measurements, including FRT data, if deemed necessary for an investigation or proceeding under the Code of Criminal Procedure. This grants judicial oversight to authorize FRT data collection when required for specific cases.

5. Enforcement (Section 6)

Compulsory Collection: If an individual resists or refuses to provide measurements, law enforcement officials are authorized to take the measurements, including FRT data, by force if necessary. Refusal constitutes an offense under Section 186 of the Indian Penal Code, which covers obstruction of public servants.

6. Data Sharing, Preservation, and Destruction (Section 4(1)(b) and (c))

The NCRB and state-appointed agencies are empowered to share and process FRT data in conjunction with crime records for identification purposes. The data retention duration of 75 years aligns with FRT data, allowing long-term retention unless court orders mandate destruction in cases of acquittal or discharge.

7. Rule-Making Powers (Section 8)

The Central and State Governments may establish specific rules on how biometric and FRT data should be collected, stored, and disseminated, allowing for flexibility and detailed guidance in the use of FRT.

VI. CASE STUDIES OF FRT DEPLOYMENT

1. **San Francisco's Ban on FRT**:

San Francisco, which has been attacked for its efficacy to increase pervasive government monitoring and perpetuate police bias, is taking the lead in legislating technology after being the first large city to outlaw the use of facial recognition by local authorities. The city council of managers voted 8-1 to approve the "Stop Secret Surveillance" policy. The proposed rule will completely prohibit the use of face surveillance by San Francisco city agencies. At present, internet giants like Amazon and Microsoft offer this technology to a number of US government organizations, including US police departments and US prisons. These systems are able to identify faces in photos or real-time video feeds and correlate those features with an individual's database identity[5].

2. **London's Facial Recognition Surveillance**:

According to AFP, London police have been using sophisticated AI- powered cameras in the Croydon district to do live face recognition (LFR) scans on gullible people. Using this technology, which generates biometric face signatures and compares them to a watchlist of suspects, ten people have been arrested for a variety of offenses, including theft, a bank scam,crossbow possession, and threats to kill. The UK government has pushed for the broader use of facial recognition technology as a weapon for combating crime as a result of the trials' effectiveness[6].

3. **Airports - Dubai International Airport (UAE):**

As part of Emirates' commitment to continuous innovation and an unmatched customer experience, the airline has launched an integrated biometric path at Dubai International airport (DXB). The contactless airport experience is now open to Emirates passengers traveling from and through Dubai. The integrated biometric path will give passengers a seamless travel journey from specific check-in to boarding gates, improving customer flow through the airport with less document checks and less queuing. Utilizing the latest biometric technology – a mix of facial and iris recognition, Emirates passengers can now check in for their flight, complete immigration formalities, enter the Emirates Lounge, and board their flights, simply by strolling through the airport. The various touchpoints in the Biometric path allow for a hygienic contactless travel journey, reducing human interaction and putting emphasis on health and safety.[7]

4. **Education - University of Sao Paulo (Brazil):**

The University of Sao Paulo adopted facial recognition technology (FRT) in classrooms to

[5] San Francisco facial recognition ban explained, https://www.vox.com/recode/2019/5/14/18623897/san-francisco-facial-recognition-ban-explained

[6] London polices use of ai facial recognition sparks controversy, https://timesofindia.indiatimes.com/gadgets-news/london-polices-use-of-ai-facial-recognition-sparks-controversy/articleshow/106576248.cms#

[7] emirates launches integrated biometric path at the airport for added convenience, https://www.emirates.com/media-centre/emirates-launches-integrated-biometric-path-at-the-airport-for-added-convenience/

streamline attendance tracking by scanning students' faces as they enter. This eliminates the need for traditional roll calls, enhancing administrative efficiency and allowing instructors to focus more on teaching. FRT’s automation simplifies the process, ensuring that attendance is recorded accurately and in real time, which can be particularly useful in large classes. However, the use of FRT in educational settings raises significant concerns about student privacy and the potential for misuse of biometric data. Collecting sensitive information like facial scans means that stringent measures must be in place to ensure this data is securely stored and used responsibly. There are concerns about how long the data is retained, who has access to it, and whether it could be used for purposes beyond attendance tracking, such as surveillance or commercial exploitation. While FRT can enhance operational efficiency, educational institutions must prioritize student privacy by implementing robust data protection frameworks, transparency, and ensuring compliance with ethical guidelines.

VII. Findings

- Article 9 of GDPR, prohibits the processing of biometric data for identifying individuals unless certain conditions are met, such as obtaining explicit consent from the data subject or fulfilling an exception, like processing for reasons of substantial public interest or law enforcement purposes.
- Article 8 of the ECHR protects the right to privacy, guarding individuals against arbitrary interference with their private lives, raising concerns about whether the widespread use of FRT in public spaces constitutes mass surveillance and infringes on privacy rights.
- Section 5 of the *Digital Personal Data Protection (DPDP) Act* emphasizes the principle of *data minimization* and the need to process personal data strictly for specified purposes. This means that for Facial Recognition Technology (FRT), any entity processing facial data (such as law enforcement or private organizations) must collect only the minimum amount of data necessary to achieve their intended purpose.
- Section 43A of IT Act, mandates that companies handling sensitive personal data must implement reasonable security practices.

VIII. Conclusion

Facial Recognition Technology (FRT) is no longer confined to science fiction; it is now a reality, profoundly affecting people’s lives in various ways, including wrongful arrests, privacy violations, and human rights infringements. Its rapid and widespread adoption by law enforcement and other sectors raises serious concerns, particularly in the absence of comprehensive regulations.

The unchecked deployment of FRT without proper ethical considerations and safeguards could lead to significant societal harm, potentially even prompting some jurisdictions to ban its use indefinitely. This outcome would not only hinder the technology's development but also diminish its potential benefits in areas like public safety and security.

The success of FRT relies on transparency, accountability, and enforceable mechanisms for auditing and challenging misuse. Without these safeguards, public trust will erode, and the risks will outweigh its potential. Discussions must also address the power dynamics FRT creates between governments, corporations, and individuals. Ultimately, FRT should be deployed in a way that empowers people and upholds fundamental rights, not undermines them. Accountability and transparency are key to achieving this balance, ensuring FRT's development aligns with ethical standards and respects human rights.

To ensure accountability, transparency is needed throughout the FRT lifecycle, from design to deployment, including scrutiny of algorithms, data sets, and usage contexts. This helps identify biases that can lead to unequal treatment of demographic groups. Incorporating openness and the ability to challenge FRT processes is not just regulatory but a moral imperative for fairness and inclusion.The General Data Protection Regulation (GDPR) serves as a robust starting point for addressing privacy concerns related to FRT. It emphasizes data protection principles, including the necessity of transparency and accountability in data handling.

For example, FRT systems have been shown to have higher error rates for individuals with darker skin tones, raising concerns about racial profiling and discrimination. As such, there is an urgent need for inclusive practices that not only prioritize transparency but also actively involve diverse stakeholders in the development and evaluation of FRT systems.Furthermore, the integration of equity and inclusion principles is crucial in addressing the power dynamics inherent in FRT. The potential for misuse by authorities, coupled with the lack of public awareness about how these systems operate, creates an environment ripe for exploitation. To combat this, it is essential to engage communities, particularly those most affected by FRT applications, in discussions about its use. This participatory approach fosters trust and empowers individuals to challenge decisions made by institutions.

(A) Recommendations

1. Specify and restrict FRT deployment to particular cases, such as serious crimes or specific threats to public safety, avoiding its broad use in general surveillance.

2. Establish an independent body to oversee FRT use by law enforcement. This body should have the power to audit, investigate misuse, and enforce penalties for violations to ensure accountability.

3. If not restricted, require law enforcement agencies to disclose the algorithms used in FRT, including details on accuracy, data sources, and any biases found during testing. Transparency builds trust and allows for external scrutiny to assess ethical and effectiveness concerns. Design FRT protocols with safeguards against biases affecting marginalized communities, addressing higher error rates and profiling risks. Tailored accuracy standards for diverse demographic groups could help reduce unfair targeting.

4. Implement strict guidelines for data storage, access, and retention. This includes secure storage practices, limiting data access only to authorized personnel, and enforcing short retention periods for data irrelevant to ongoing investigations.

5. Inform communities about the use of FRT through public disclosures, impact assessments, and transparent reporting. Engaging the public fosters accountability and ensures that deployment considers community concerns and ethical implications.

6. Prohibiting the use of facial recognition technology for identifying criminal suspects and conducting public surveillance by government and private entities in public areas. For instance, San Francisco, Boston, Portland, California, banned FRT to stop secret surveillance.

7. Deleting data collected from the facial recognition technology system once the task is completed. For instance, DIGI YATRA deletes passenger’s data after their journey is Finished.

*****