EMBRACING ARTIFICIAL INTELLIGENCE FOR SUSTAINABILITY & LIFE SKILLS

An International Bhutan Conference Proceedings

IJISEM
INTERNATIONAL JOURNAL OF INNOVATIONS IN SCIENCE ENGINEERING AND MANAGEMENT

International Journal of Innovations In Science Engineering And Management

AI And The Right To Privacy: A Comparative Study of Digital Democracies And Surveillance Status In India And The USA

OPEN ACCESS

Volume: 3

Issue: Special issue 2

Month: December

Year: 2024

ISSN: 2583-7117

Citation:

Ashok Kumar and Anonnza Priyadarshini & Pallavi, "AI And The Right To Privacy: A Comparative Study of Digital Democracies And Surveillance Status In India And The USA" International Journal of Innovations In Science Engineering And Management, vol. 3, no. Special issue 2, 2024, pp.274-283.

DOI:

10.69968/ijisem.2024v3si2274-283

Prof. (Dr.) Ashok Kumar[1], Anonnza Priyadarshini &Pallavi[2]

Professor, Department of Law, Central University of South Bihar, Gaya
Research Scholar, Department of Law, Central University of South Bihar, Gaya.

Abstract

The strife between the Right to Privacy and the need for Surveillance has long been a contentious issue between citizens and the state. The present research focuses on the tension between facial recognition technologies (FRT) and the right to privacy in two digital democracies- India and USA. With video surveillance developing underpinned by AI, biometrics and FRT, individual privacy has new challenges. This chapter aims at investigating potential misuses of these technologies as well as addressing importance of data protection legislations.

The study stresses balancing security and personal privacy. Issues of transparency and potential bias arise from AI-powered video surveillance. In this manner, by exploring these matters, this chapter underscores the importance of an ethical and legitimate implementation of FRT that protects individual privacy.

Keyword: Facial Recognition Technology, Privacy, Data Protection, Machine Learning, Video Surveillance

1. INTRODUCTION TO FACIAL RECOGNITION TECHNOLOGY

Facial recognition Technology, or FRT is finding its ways in our life more and more with aspect of daily needs, from auto-tagging any photo we upload on Facebook to unlocking our phones we can find FRT everywhere. Now a days FRT is also being used by employers to monitor employee productivity as well as it is used by law enforcement agency to monitor rallies. The photos that are captured are compared by the facial recognition technology by the picture which is already available by in the database or is present in watch lists maintained by government. FRT is a very intrusive type of monitoring which can have significant amount of negative effect on people's privacy and eventually the society as a whole will be affected.

The Facial Recognition Technology is an automatic computer program which is made to associate two different picture of a faces to find out whether they belong to the same individual or not. This programme change all the distinctive feature of face, such as nose, eyes, lips and distance between eyes, chin and lip etc., into mathematical representation as soon as the picture is uploaded. This mathematic representation is known as face template. This face template is then compared with the already available facial data in the data based maintained by the agency, to find the match.

Charles Bisson, Helen Chan Wolf and Woddy Bledsoe are among the innovators of Facial Recognition technology. In 1964 and 1965; Bledsoe, Helen Chan and Charles Bisson worked on training the computer to recognize the facial

features. Since the fund for this was coming from an unidentified spy agency, even after doing a splendid job not much was published. After Bledsoe, this work was carried forwarded at the Stanford Research Institute, by Peter Hart in 1966. The machine regularly beat the human at the recognition task which was conducted on a database which included more than 2000 images. Chritoph Von Der Malsburg along with graduate student of the University of Bochum, Germany and the University of Southern California, United States in 1997, developed an automated system which outperformed majority of the programme related to FRT. The United State Army Research Lab funded the research for the development of the Bochum system; which was sold to the ZN-Face and was used by customer like Deutsche Bank & airport operators etc. This software was strong enough to make identification from the less than perfect facial views. It is said that this FRT was capable to past see all the barrier of identification like moustaches, beards, hairstyles, spectacles etc.

Facial Recognition Technology (FRT) has countless benefits, but along with that it also poses grave threat to privacy and security. One of the major concerns is the lack of consent, as without individuals' permission the businesses gather and utilize biometric data leading to violation of core data privacy rules. This is especially bothersome in situations like real-time public surveillance or the collection of illegally created databases. Another challenge is that facial data is unencrypted which make it easier to grab and store from a far. Facial data can't be encrypted like passwords or credit card information, making the process to secure it difficult. The misuse of facial recognition data can result into serious repercussions such as identity theft, stalking and harassment. Furthermore, the lack of knowledge about how FRT is used lead to serious privacy concerns. Like facial scans can be collected discreetly and remotely unlike other biometrics such as fingerprints, exacerbating these problem. Every technology have some technical flaw, similarly FRT also can be fooled with photos or 3-D masks made from the victim image. This open the way to the presentation attacks or digital spoofs like deep fakes. The accuracy of FRT can be sometime also questioned, especially when there is significant change among the group of people. There can be long term effect of misidentifications, mainly when false positive rate unreasonably affect women and people of colour leading to unjust results such as wrongful arrests. The problems highlight the necessity to strictly supervise and regulate the FRT to minimize the concern and maximize the advantage.

The need to achieve a delicate balance between utilizing benefit of FRT and protection individuals' privacy and security is a crucial in this quickly moving field of FRT. Few of the potential advantages of FRT; improving security, optimizing workflows and elevating user experiences; are evident as FRT is little by little incorporated into more aspects of daily life. However the implementation of this technology also raises a serious concern for the individuals' privacy that is in dire need to be resolved in order to guarantee a moral and responsible use of technology. Some of the prominent company in the industry, such as IBM, Amazon, and NEC, have showed how to efficiently handle these privacy concerns while fully using FRT. For example, IBM has said that it will stop generating general purpose facial recognition systems, quoting the worries about racial profiling and widespread surveillance. This action shows the company's inclement toward moral business conduct and the need of strong law and regulation governing the technology. In similar manner, Amazon has put hold on police use of its facial recognition software, Rekognition, for a year; giving time to the government to form stringent regulation for the moral and ethical use and governance of FRT. NEC, a leading biometric technology company have shift their concentration on improving system accuracy while also bringing in privacy enhancing techniques like differential privacy, which mask users' identities by adding statistical noise to the data. These true life success stories that by keeping privacy and transparency first, it is possible to successfully minimise the challenges of FRT. These companies not only safeguarded the individual right but also build public believe in technology through the responsible implementation, thus guaranteeing FRT ethical and sustainable integration into the society

2. PRIVACY CONCERNS IN DIGITAL DEMOCRACIES

There has been increase in privacy discussion, trigged by the penetration of FRT into digital democracies like the United State and India. A great percentage of government agency have started using FRT for their border security as well as law enforcement, continuous raising the worries about the potential impairment of individuals' privacy right. This part of the chapter will try to explore the legislation that is governing the right to privacy and the relationship between the governmental surveillance and individual liberties, digging into the disputes of privacy concern unique to these two democracies.

2.1. The Right to Privacy

In India, the have been a significant changes when it comes to right to privacy, especially in relation to digital technologies. Earlier, there was no specific acknowledgement about the privacy as a fundamental right to an individual in our Indian Constitution. In 2017, all this changed due to a landmark judgement by Supreme Court of India in the case of K.S. Puttaswamy (retd.) vs. Union of India[1]. The supreme court of India firmly upheld the right to privacy to be under article 21 as being intricately linked to the right to life and personal liberty. This landmark judgment becomes the basis for how the privacy including digital privacy, should be treated under Indian law. The decision made it certain that any interference with the privacy must be justified and meets three criteria i.e. necessity, proportionality and legality. Still with such a positive decision, there is a raise in concern with implementation of FRT, as how effective these principles will be upheld. In recent years, the Indian government is rapidly expanding its use of facial recognition technology (FRT), especially for surveillance and law enforcement. Projects like the Automated Facial Recognition System (AFRS), intended to assist police to recognize criminals, have raised concerns about mass surveillance with no appropriate legal safeguards. Critics contend that the absence of comprehensive legislation regarding data protection in India worsens these concerns, since there is no rigorous statutory structure.[2]

In contrast, the United States takes a more scattered approach to privacy, with not a single comprehensive federal statute covering the use of FRTs. Rather, safeguards for privacy are contained in a variety of statutes and regulations, such as the Fourth Amendment, which prohibits arbitrary seizures and searches, and the Privacy Act of 1974, which restricts the ability of government agencies to gather and utilize personal data.Despite these safeguards, the utilization of FRT by agencies of government, especially for surveillance purposes, caused worries regarding possible misuse. In 2020, the Government Accountability Office (GAO) revealed that numerous federal departments used FRT with minimal transparency or supervision. This absence of legislation is made worse by the presence of private firms, who frequently gather and store massive volumes of facial data with no adequate safeguards.States and cities in the United States have started to take things into their own hands by introducing legislation that regulates or completely prohibits the implementation of FRT. Cities such as San Francisco and Portland, for example, have strictly forbidden government departments from using FRT, expressing increasing concerns about privacy and civil liberties. Yet, this municipal legislation provides an inconsistent framework for protection which might fail to tackle the broader consequences of FRT for privacy.[3]

Judicial interpretations about privacy rights in the light of FRT have fluctuated across jurisdictions, highlighting the constant battle to combine technical progress with social liberties. In India, the K.S. Puttaswamy (retd.) vs. Union of India[4] decision is an important precedent because it not just acknowledged the right to privacy but additionally established a structure for determining the legitimacy of governmental actions that violate privacy. However, subsequent court decisions have not fully addressed the consequences of FRT and other technologies being developed.The legal landscape in the United States is still unclear with on-going debates about how conventional privacy protections apply to new technologies like FRT. In the United States, courts have usually supported the use of surveillance technologies within certain circumstances, often citing concerns about public safety and national security. Still, there are some instances where courts have fought again against the unregulated implementation of FRT. For instance, in United States v. Jones (2012)[5], the Supreme Court ruled that the use of GPS tracking without an authorization infringed the Fourth Amendment.

2.2. Surveillance vs. Privacy

In digital democracies, where the preservation of private liberties frequently coincides with the requirement for security, state surveillance continues to be a sensitive topic. Government use of FRT has heightened these discussions since it allows for previously unheard-of levels of mass surveillance.

The use of FRT by the Indian government fits within an overall trend of expanded surveillance. For example, the purpose of the AFRS is to build a national database of face imagery that law enforcement agencies can consult. This creates questions about the possibility of abuse, particularly given the lack of an adequate legal framework to control the processing of this kind of information. Human rights groups have issued a warning that FRT may be utilized to track political activities, target underprivileged areas, and crush protest, all of which might have a crippling impact on the right to free speech.The same problems are present in the USA, especially with regard to the application of FRT by both local and federal law enforcement. The technology is being applied to anything from tracking protesters to tracking down criminals, which has raised concerns that it

can be abused to restrict civil freedoms and discourage political activism. These worries are made worse by the lack of federal laws and the lack of transparency around the use of FRT, as citizens have little options for contesting or opting out of monitoring.

Cultural, social, and political aspects greatly impact public perception of FRT and its privacy consequences. Though perspectives on how FRT is to be utilized are different in both India and USA, there is a rising awareness of the privacy dangers involved with FRT in both place.

The trajectory of monitoring in India, as well as the government's concentration on security, has affected public opinion. Although there has been considerable support for using FRT to tackle crime and boost security for the public, there is also widespread concern about the possibility for exploitation. The absence of transparency surrounding government monitoring operations has exacerbated scepticism, especially within civil liberties organizations and privacy advocates.In the United States, sentiments toward FRT are equally separated. Research have found that, while a lot of Americans have reservations about their privacy, they are nevertheless prepared to comply with some surveillance methods in for the sake of security. Yet this acceptability is not universal; underprivileged communities, in particular, are more inclined to distrust FRT due to its capacity for bias and discrimination.

The argument about FRT and privacy in digital democracies such as India and the United States emphasizes the intricate interplay of technology, security, and individual rights. As governments continue to adopt FRT, there is an increasing demand for clear legal frameworks, transparency, and public accountability. Without these safeguards, the right to privacy in the digital era is jeopardized, with serious consequences for the viability of democracy itself.

3. ETHICAL CONSIDERATIONS AND POTENTIAL MISUSES

The ethical implications of the rapid expansion of facial recognition technology have generated substantial concerns, highlighting the delicate balance between scientific advancements and moral principles. The benefits of Facial Recognition Technology (FRT) encompass enhanced security, streamlined identification verification procedures, and assistance in criminal investigations. However, one must also examine the potential drawbacks and hazards associated with its misuse, given its significant impact. Innovation and ethics are therefore intrinsically connected as civilizations slowly adopt this technology.

An important ethical concern related to FRT is the development of bias and discrimination. Machine learning algorithms used in facial recognition technology (FRT) are typically trained on datasets that may not adequately represent all demographic groups, resulting in accuracy differences. In a major 2018 study, aptly dubbed "Gender Shades," by Joy Buolamwini and TimnitGebru, huge variations were identified in error rates based upon demographic groups: 34.7% for darker-skinned women vs. 0.8% for lighter-skinned males in recognizing facial recognition systems.[6] These results emphasize that the use of FRT may increase the impact on females and persons of colour, particularly in law enforcement. The results of these mistakes include the tendency to lead to false allegations, unjust profiling, and maintenance of systemic biases.

Data Protection and Privacy

The broad implementation of FRT poses a lot of problems as far as data protection and privacy are concerned. The technique naturally includes the collecting and processing of huge volumes of biometric data, frequently without individuals' explicit agreement.[7] There is sometimes little awareness on the side of the people getting scanned and their faces saved in public areas, therefore this also raises problems of transparency and ethics involved in the procedures. Besides, the liability of FRT is being aggravated by the lack of stringent norms and protocols regulating its use. In India, for example, despite a 2017 decision by the Indian Supreme Court on the right to privacy being a basic right under the Indian Constitution[8], the landscape of FRT now varies from mismatch to mismatch in legislation by various states due to digital disparity.[9] This disparity creates a few difficulties of making sure biometric data of people are safeguarded adequately from being exploited or illegal handled.

Security Breaches and Data Vulnerability

FRT is emerging in dependence as well, and posing a concern for the security of data. Just comparable to all other digital technologies, databases holding the facial photographs and any other biometric identifications are subject to cyber-attacks. High-profile security breaches have revealed that even the most protected systems are vulnerable to compromise, with potentially disastrous repercussions.[10] FRT application in other contexts where suitable regulatory controls were not established has generated privacy concerns; for example, the ACLU in the United States has highlighted cases that resulted in major privacy violations.[11] This reiterates the significance of improving security on the use and disposal of information

on people' biometrics, considering that this is sensitive data.

There exists a big question of inadequate regulation and insufficient oversight both in India and the United States regarding FRT. Some states and towns have taken measures to regulate or even ban the application of FRT by security agencies. For instance, police restrictions of FRT in San Francisco and Boston were recorded over concerns for privacy and civil liberties.[12]On the other hand, in other locations with a focus on India, deployment of FRT is being boosted without any regulation, bringing up a complicated and in many ways contradicting legal landscape.[13] This non-uniformity of rules and regulations poses extremely critical considerations regarding what is appropriate use versus an invasive practice and how to ensure technology is put to good use and ethical practice.

Mass Surveillance and Government Exploitation

Perhaps the most disconcerting ethical worry is the potential for FRT to be utilized as a tool for widespread surveillance. For the safety and security of the public, governments will be able to abuse FRT and spy on and follow citizens at a degree exceeding anything that has ever been seen in the actual world, much like a dystopia in some work of fiction. This is notably troubling when dealing with at-risk circumstances such as immigration and refugees. There is growing danger that FRT may be used to follow, detain, or otherwise target them in ways that further marginalize these groups or add to the list of their vulnerabilities.[14]

In all democracies globally, while there is potential to grow in this technology sector, the question will always be the same—how best to seize the value of FRT, respect individual freedoms, and assure at the same time that its use is equitable, transparent, and responsible. The discussion in FRT is not technological but it determines what society we shall be living in and what ideals we shall ascribe to and use as a guideline as we walk through this digital age.

3.1. Bias and Discrimination

While FRT portrays itself as a powerful technology with applications in numerous areas, at the same time, it also offers major ethical concerns. The most major difficulty is bias and discrimination, which lies at the heart of FR technologies, where machine learning algorithms are built on massive datasets. If the data sets are not varied or representative of the population, then the outputted systems will have biased outputs that could disproportionately impact specific demographic groups.[15]

It has been proved time and again that facial recognition misidentifies a disproportionate number of people from underrepresented areas. For example, research has found that women and people of colour are more prone to face false positives—situations in which the system wrongly identifies them. This issue is more intense for Black women, whose rates of misidentification are higher than those of white males[16]. The subsequent consequence of such blunders is significant, and they could potentially destroy lives. For example, ACLU researchers have uncovered incidents in which individuals were incorrectly recognized by facial recognition systems and then falsely jailed.[17] These incidents demonstrate the serious hazards of using biased technologies in very vital domains, such as law enforcement.

The usage of FRT all have an effect on and lead to other systemic implications in public policy implementations and law enforcement activities. Using biased FRT data in their possession, such agencies will, therefore, target specific demographic groups unjustly and be the primary reason for over-policing in specific neighbourhoods. In doing so, they increasingly mistrust the policed and policing communities. For example, in the United States, there are more surveillance cameras utilizing facial recognition in black and brown communities. This is on the account of surveillance that is heightened in these communities at the expense of the same.[18] Such techniques bring systematic prejudice against these populations since most of the time, these victims might not know what is happening or even have the willingness to be involved in the monitoring program.

The problem of algorithmic bias is not confined to racial imbalances but also extends to gender and age considerations. For instance, facial recognition algorithms have not been trained on enough data displaying and portraying older faces; hence, they are less accurate in distinguishing older persons.[19] Likewise, transgender and non-binary individuals would have difficulty with the systems which fail to account in the wide range of gender expressions.[20] Such biases would perpetuate disparities and promote societal biases across multiple contexts, from security checks at airports to features like tagging friends on social media.

Addressing these biases requires a multi-faceted strategy that involves increased transparency in how

algorithms are built and tested. These systems have to be properly evaluated with varied datasets well in advance before implementing FRT into real-world settings like video surveillance or law enforcement activities. Open and transparent talks about data-sourcing procedures are vital to ensure all demographics will be represented effectively during the training phase. The danger of embedding prejudices inside such technological infrastructures is further emphasized by the fact that, without such meticulous ethical considerations, FRT will further cement systemic inequality. This conclusion would be particularly worrying for nations aspiring toward equity and justice in an increasingly digital world.

3.2. Data Protection and Security

With the advent of facial recognition technology, questions around the privacy and security of data are also on the rise. The combining of machine learning algorithms with FRT has clearly increased accuracy and broadened applicability, but in the meantime, it has produced substantial ethical concerns relating to biometric data collecting, storage, and utilization.[21] These challenges are especially pressing in digital democracies like the USA and growing economies like India.

Video surveillance networks with incorporated facial recognition algorithms acquire huge volumes of biometric data, frequently without users' knowledge or consent. This provides a distinct set of set of risks.[22] Once personal photos are saved on databases, they might be open to misuse including unauthorized tracking, profiling, and even identity theft. The legal frameworks in securing this data still lag behind technical improvements, so the gaps remain wide open.

In India, privacy rules are still grown to their ultimate despite the landmark verdict by the Supreme Court in 2017, recognizing privacy as a basic right.[23] But with this critical position, rules and regulations controlling the use of facial recognition technology remain limited and far from universal application across jurisdictions. This makes it impossible to verify that biometric data is appropriately protected from misuse. In the USA, meantime, a patchwork of state laws regulating privacy also creates for confusing legal terrain which hampers efforts to safeguard people from potential abuses of facial recognition technology. Although there are some states that have established legislation either banning the use of FRT by the police or regulating it, there are others that have not yet covered these concerns, and there is significant misunderstanding and under-protection.[24]

But the significance of facial recognition technology goes beyond simply individual privacy rights, touching base with the more general standards for functioning as a society in terms of consent and governance. Do citizens completely comprehend that their faces can be used as identifiers in governments or corporates' databases? These systems will lose credibility if there are no solid safeguards around openness and accountability, and their loss might happen quickly, possibly in a public backlash and resistance.

Data leaks also weigh up vulnerabilities in this facial recognition technology. Incidents have highlighted how readily information can be hacked if strong cybersecurity procedures are not applied. Take, for example, a facial recognition database--millions of personal identifications would be exposed in such a type of security breach, creating rampant identity theft, fraud, and a lot of other kinds of crimes.[25] Such situations necessitate adequate sanctions for breaches and particular reparation actions on any level they are committed.

Strong legal and ethical frameworks must assure balance between the benefits of facial recognition technologies and the preservation of individual rights. Strict data protection rules, clear instructions on consent and openness, and strong security measures can be put in place to prevent unwanted access to biometric data. The goal, ultimately, should be to create an enabling climate in which technological innovation can thrive without compromising the fundamental rights and freedoms of people. Both India and the USA have the chance to lead by example, proving that the power of facial recognition technology can be exploited while respecting ideals of privacy, fairness, and justice.

4. BALANCING SECURITY AND PRIVACY

As facial recognition technology continues to evolve, maintaining a balance between security and privacy becomes more complex. On one side, modern technology offers better public safety and more efficient processes. For example, the New York Police Department (NYPD) has successfully deployed facial recognition to identify and catch suspects in real-time, highlighting its potential to increase public safety.[26] However, it also raises substantial concerns about privacy rights and the danger of misuse. Navigating this difficult balance is vital for democratic countries like India and the USA as they strive to utilize the benefits of facial recognition while maintaining civil rights.

4.1. Transparency and Accountability

Achieving this balance demands establishing transparency and accountability in the implementation of facial recognition technology. People have a right to know how their personal data is being collected, stored, and used by both public and commercial bodies. Without clear guidelines and control, there is a heightened danger of abuse and a loss of confidence. In the USA, the absence of comprehensive federal restrictions has resulted in a patchwork of state laws and local ordinances governing facial recognition. While some states have implemented rigorous standards, others remain essentially uncontrolled. This non-uniformity generates confusion and makes it difficult for individuals to grasp their rights and protections.

For instance, in 2019, San Francisco outlawed the use of face recognition by law enforcement and other city departments due to privacy concerns and potential exploitation.[27] Despite these problems, there have been positive uses of the technology. Major airports in the USA, like Hartsfield-Jackson Atlanta International Airport, have incorporated facial recognition into their security operations, enabling faster check-ins and boarding, boosting the travel experience for customers while bolstering security.[28] This technology helps airports to manage high volumes of travellers quickly, ensuring that security procedures are upheld without generating substantial delays.

India, on the other hand, has yet to implement a comprehensive data protection law, despite a landmark 2017 Supreme Court verdict recognizing privacy as a fundamental right. The Personal Data Protection Act,2023, which aims to control the gathering and processing of personal data, had encountered delays and amendments. Meanwhile, in the absence of clear national norms, various governments have implemented varying techniques to facial recognition, leading to a lack of uniformity and transparency.For example, the Delhi Police's use of face recognition technology has raised discussions due to its 80% accuracy rate, prompting privacy concerns and worries about the system's dependability.[29]

Meanwhile, India has created programs like DigiYatra, which seeks to provide passengers with a smooth experience at airports using facial recognition technology.[30] Implemented in major airports such as Delhi and Bengaluru, this project reduces wait times and enhances the entire travel experience, however transparency in how facial data is collected and used remains a problem. Similarly, the introduction of Herta Security's facial recognition systems at Indian railway stations, while meant to enhance safety and security, raises worries about the potential misuse of personal data and the need for strong control.[31]

To solve these difficulties, both countries must prioritize the development of comprehensive legal frameworks that define clear guidelines for the use of facial recognition technology. These frameworks should include protections for:

Transparency: Requiring public and private institutions to declare their use of facial recognition, the goals behind it, and the data collecting and storage procedures involved.

Consent: Ensuring that persons are notified when their facial data is being collected and given the chance to opt out or withdraw consent, save in circumstances of legitimate law enforcement needs. This is particularly crucial for Indian Railways passengers, who may not fully grasp their rights regarding the usage of their facial data.

Data Rights: Granting individuals the right to access, correct, and delete their facial data, as well as the capacity to dispute automated decisions based purely on facial recognition. This is essential in sectors like healthcare, where hospitals in the USA are employing face recognition to verify patient IDs, lowering the chance of medical errors but also raising issues about data rights and privacy.[32]

Oversight: Establishing independent oversight agencies to monitor the use of facial recognition technology, investigate complaints, and enforce compliance with legislation. The ASTR (AI and Facial Recognition Powered Solution) utilized by the Department of Telecommunications in India for SIM subscriber verification underlines the significance of oversight to prevent misuse and ensure ethical usage of technology.[33]

By stressing transparency and accountability, India and the USA may establish public trust and ensure that the use of facial recognition technology aligns with democratic norms and individual rights.

4.2. Ethical Frameworks

In addition to legal frameworks, the appropriate development and implementation of facial recognition technology must be governed by strong ethical values. These principles should be formed through inclusive, multi-stakeholder procedures that involve input from civil society, academia, industry, and government officials. By embracing multiple viewpoints andexperiences, these

ethical frameworks can more effectively handle the particular issues and intricacies of each environment.

Some key ethical principles that should guide the usage of facial recognition technology include:

Non-discrimination: The technology must be developed and utilized in ways that do not discriminate against individuals or groups based on race, gender, age, or other protected characteristics. For instance, facial recognition technology utilized by the New York Police Department (NYPD) should be rigorously regulated to ensure it does not unfairly target minority neighbourhoods or contribute to racial profiling.

Purpose Limitation: The use of facial recognition technology should be restricted to specified, legal reasons, preventing its use for mass surveillance or other unwanted applications. This notion was a crucial element in San Francisco's decision to ban facial recognition, spurred by worries about its potential for mass surveillance. Data Minimization: Only the least amount of facial data necessary to achieve the defined objective should be gathered and stored, with data being discarded when it is no longer needed. This notion is crucial in programs like Digi Yatra in India, where data collection should be limited to what is necessary to enhance the passenger experience without compromising privacy.

Algorithmic Accountability: Developers and users of facial recognition technology must be held accountable for the accuracy, impartiality, and transparency of the algorithms they employ. For example, the facial recognition systems employed by Herta Security in Indian railway stations should undergo frequent audits to ensure the algorithms do not exhibit prejudice or inaccuracies that could negatively harm individuals.

Human scrutiny: Critical choices made utilizing facial recognition technology, particularly in sensitive areas like law enforcement or immigration, must be subject to substantial human review and scrutiny. This is critical in areas like healthcare, where facial recognition is used to authenticate patient identities, ensuring that technology errors do not lead to major medical implications.

CONCLUSION

As India and the USA navigate the complex world of facial recognition technology, it is clear that balancing security and privacy will remain a significant concern. However, by emphasizing openness, accountability, and ethical frameworks, both nations can work towards a future where the benefits of this technology are realized without compromising individual rights and liberties. Through inclusive, multi-stakeholder processes, India and the USA can build comprehensive legal and ethical frameworks that provide clear guidelines for the use of facial recognition technology. These frameworks should prioritize the protection of individual rights, encourage non-discrimination, and ensure that the technology is deployed for lawful purposes that serve the public good. By proactively addressing the ethical challenges posed by facial recognition technology, India and the USA can set a global e[34]xample for the responsible development and deployment of emerging technologies. Ultimately, the goal should be to harness the power of innovation while safeguarding the essential principles of democracy, human rights, and social justice.

REFERENCE

[1] (2017) 10 SCC 1 (India)

[2] Supra note 2

[3] Vaibhav Chadha, Thajaswini Coimbatore Balasubramanian & Anshul Bhuwalka, Privacy and Surveillance Conflict: A Comparative Analysis of the Laws in the USA and India, 13 Janus.net, e-journal of Int'l Rel. 201, 202 (2022).

[4] (2017) 10 SCC 1 (India)

[5] 565 U.S. 400 (2012)

[6] Joy Buolamwini&TimnitGebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification* , 81 PROCEEDINGS OF MACHINE LEARNING RESEARCH 1 (2018), https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf (last visited Aug 17, 2024).

[7] National Research Council (US) Whither Biometrics Committee, Joseph N Pato & Lynette I Millett, *Cultural, Social, and Legal Considerations*, NATIONAL ACADEMY OF SCIENCES (2010), https://www.ncbi.nlm.nih.gov/books/NBK219893/ (last visited Aug 17, 2024).

[8] *Puttaswamy (Retd.) &Anr. v. Union of India &Ors*., (2017) 10 SCC 1 (India).

[9] AI FOR ALL ADOPTING THE FRAMEWORK: A USE CASE APPROACH ON FACIAL RECOGNITION TECHNOLOGY, (2024), https://www.niti.gov.in/sites/default/files/2024-07/Responsible%20AI%20AIForAll.pdf (last visited Aug 17, 2024).

[10] LiudmylaPryimenko, *Top 5 Real-Life Examples of Breaches Caused by Insider Threats*, EKRAN

SYSTEM (2024), https://www.ekransystem.com/en/blog/real-life-examples-insider-threat-caused-breaches (last visited Aug 17, 2024).

[11] Privacy & Technology Court Cases, AMERICAN CIVIL LIBERTIES UNION (2024), https://www.aclu.org/court-cases?issue=privacy-technology (last visited Aug 17, 2024).

[12] Kate Conger, Richard Fausset & Serge F Kovaleski, *San Francisco Bans Facial Recognition Technology*, THE NEW YORK TIMES, May 14, 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html (last visited Aug 17, 2024).

[13] Deployment of Facial Recognition Technology for State Surveillance and Monitoring • Software Freedom Law Center, India, SOFTWARE FREEDOM LAW CENTER, INDIA • DEFENDER OF YOUR DIGITAL FREEDOM (2024), https://sflc.in/deployment-of-facial-recognition-technology-for-state-surveillance-and-monitoring/ (last visited Aug 17, 2024).

[14] Genia Kostka, Léa Steinacker & Miriam Meckel, *Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology*, 40 GOVERNMENT INFORMATION QUARTERLY 101761 (2022).

[15] David Leslie, *Understanding Bias in Facial Recognition Technologies*, THE ALAN TURING INSTITUTE (2020), https://arxiv.org/ct?url=https%3A%2F%2Fdx.doi.org%2F10.5281%2Fzenodo.4050457&v=e0b972fd (last visited Aug 17, 2024).

[16] Matt Field, *It's Time to Address Facial recognition, the Most Troubling Law Enforcement AI Tool*, BULLETIN OF THE ATOMIC SCIENTISTS (2021), https://thebulletin.org/2021/11/its-time-to-address-facial-recognition-the-most-troubling-law-enforcement-ai-tool/ (last visited Aug 17, 2024).

[17] Marissa Gerchick& Matt Cagle, *When it Comes to Facial Recognition, There is No Such Thing as a Magic Number | ACLU*, AMERICAN CIVIL LIBERTIES UNION (2024), https://www.aclu.org/news/privacy-technology/when-it-comes-to-facial-recognition-there-is-no-such-thing-as-a-magic-number (last visited Aug 17, 2024).

[18] ACLU, *The Fight to Stop Face Recognition Technology*, AMERICAN CIVIL LIBERTIES UNION (2023), https://www.aclu.org/news/topic/stopping-face-recognition-surveillance (last visited Aug 17, 2024).

[19] D. Norton, R. McBain & Y. Chen, *Reduced Ability to Detect Facial Configuration in Middle-Aged and Elderly Individuals: Associations With Spatiotemporal Visual Processing*, 64B THE JOURNALS OF GERONTOLOGY SERIES B: PSYCHOLOGICAL SCIENCES AND SOCIAL SCIENCES 328 (2009), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2905137/ (last visited Aug 17, 2024).

[20] Sayantan Datta, *How Facial Recognition AI Reinforces Discrimination Against Trans People*, THE SWADDLE (2022), https://www.theswaddle.com/how-facial-recognition-ai-reinforces-discrimination-against-trans-people (last visited Aug 17, 2024).

[21] Sunil Gupta et al., *Comparing the performance of machine learning algorithms using estimated accuracy*, 24 SCIENCE DIRECT 100432 (2022).

[22] Jake Laperruque, *Limiting Face Recognition Surveillance: Progress and Paths Forward*, CENTER FOR DEMOCRACY AND TECHNOLOGY (2022), https://cdt.org/insights/limiting-face-recognition-surveillance-progress-and-paths-forward/ (last visited Aug 17, 2024).

[23] Supra n 3.

[24] Regulating Police Use of Face Recognition Technology, THE POLICING PROJECT, https://www.policingproject.org/regulating-police-use-of-face-recognition-technology (last visited Aug 17, 2024).

[25] Nabeel Ahmed, *How the personal data of 815 million Indians got breached | Explained*, THE HINDU, Nov. 7, 2023,

[26] https://www.thehindu.com/sci-tech/technology/how-the-personal-data-of-815-million-indians-gotbreached-explained/article67505760.ece (last visited Aug 17, 2024).

[27] FACIAL RECOGNITION: IMPACT AND USE POLICY, (2023),

[28] https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/facial-recognition-nypd-impact-and-use-policy_10.26.23.pdf (last visited Aug 17, 2024).

[29] Supra n 7.

[30] Kaitlyn Luckow, *Atlanta Airport to Begin Facial Recognition for Passports*, PASSPORT HEALTH USA

(2018), https://www.passporthealthusa.com/passports-and-visas/blog/2018-9-atlanta-airport-facial-recognition-for-passports/ (last visited Aug 17, 2024).

[31] Kanika Saxena, *Delhi Police's facial recognition tech at 80% accuracy, stokes privacy concerns again!*, THE ECONOMIC TIMES (2022), https://economictimes.indiatimes.com/news/india/delhi-polices-facial-recognition-tech-at-80-accuracy-stokes-privacy-concerns-again/articleshow/93587861.cms?from=mdr (last visited Aug 17, 2024).

[32] Kanika Saxena, *Delhi Police's facial recognition tech at 80% accuracy, stokes privacy concerns again!*, THE ECONOMIC TIMES (2022), https://economictimes.indiatimes.com/news/india/delhi-polices-facial-recognition-tech-at-80-accuracy-stokes-privacy-concerns-again/articleshow/93587861.cms?from=mdr (last visited Aug 17, 2024).

[33] Abhishek Jadhav, *Indian Railways deploys Herta facial recognition to secure train stations*, BIOMETRIC UPDATE (2024), https://www.biometricupdate.com/202405/indian-railways-deploys-herta-facial-recognition-to-secure-train-stations (last visited Aug 17, 2024).

[34] Jackie Wheeler, *How Biometric Security is Changing the Healthcare Industry*, JUMIO: END-TO-END ID, IDENTITY VERIFICATION AND AML SOLUTIONS (2023), https://www.jumio.com/biometric-security-in-healthcare/ (last visited Aug 17, 2024).

[35] Vallari Sanzgiri, *Why is Telecom department using facial recognition on SIM users?*, MEDIA NAMA (2023), https://www.medianama.com/2023/01/223-explained-astr-sim-facial-recognition-2/ (last visited Aug 17, 2024).