IDFC Institute

DGN Policy Brief 13

April 2021

Data Governance Network
Anchored by IDFC Institute

Facial Recognition Technology (FRT) in Law Enforcement in India: Concerns and Solutions

Priya Vedavalli, Prakhar Misra, Tvesha Sippy, Avanti Durani, Neha Sinha, Vikram Sinha

Reliance on FRTs in India is premature. We highlight this whilst acknowledging FRTs' use cases—in aiding the police's preventive and investigative functions, in potentially reducing 'third-degree methods', and improving police's functional autonomy. FRT deployment creates risk and has implications in several areas: accuracy errors, bias, and discriminatory and real-time surveillance. These technologies should therefore be implemented in a modular manner with fair, transparent, and reasonable operational safeguards. As a first step, there should be a clear definition and limitation of purpose and data use, with police training and independent oversight bodies to follow.

Current Context

COVID-19: The COVID-19 pandemic has accelerated FRTs' emergence. Contactless technological solutions are replacing touch-based fingerprint detection systems. In India, the Technology Development Board (TDB) of the Department of Science and Technology (DST), Government of India, approved projects to augment India's efforts to combat COVID-19. This includes detecting and tracking multiple people using facial recognition even if they're wearing masks (Singh, 2020).

NCRB's tender for Automatic Facial Recognition System (AFRS): The National Crime Records Bureau (NCRB) first issued the request for proposals for AFRS in July 2019 to supplement police capacity. It attracted significant criticism and the tender was later revised to exclude CCTV camera footage. Concerns still surrounding the tender include legality (addressed by NCRB by citing the cabinet note), privacy concerns and the tender attracting foreign bidders for an internal surveillance system. Additionally, the tender does not specifically identify an exhaustive list of databases that it will be linked to but identifies Crime and Criminal Tracking System (CCTNS) and Interoperable Criminal Justice System (ICJS) as initial contenders.

Usage of FRT in policing: According to the data released by Maharashtra State Home Department, over 1,000 crimes have been solved and nearly 972 arrests have been made in Mumbai and Pune with the use of CCTV cameras (Vyas, 2019). In 2018, the Delhi Police had identified 3,000 missing children as a part of their trial usage of facial recognition software (PTI, 2018).

International pushback: The death of George Floyd in the US was a watershed moment which raised questions about the actions of law enforcement agencies and concerns regarding accuracy, racial and gender biases. This has led to many companies backtracking on FRT investment for law enforcement. IBM recently announced a complete pullback from developing and researching FRTs for law enforcement (Peters, 2020). Amazon followed suit, announcing a one-year moratorium on selling police access to its facial recognition technology—Rekognition (Statt, 2020).

Use cases and concerns

A. Use cases of FRTs in law enforcement in India: There are 19 known FRT use cases for law enforcement spanning field use, investigative use and custodial/supervisory use (Law Enforcement Imaging Technology Task Force, 2019). The key use cases are summarised below:

- **Aiding crime investigation:** Crime investigations are undercut by the poor quality of evidence. Three-fourths of the First Information Reports (FIR) that were closed without an investigation in 2017 were due to insufficient or untraceable evidence. Further, investigations that place their evidentiary burden on oral testimonies are at risk of witnesses turning hostile (Bothra, 2019). In such cases, FRTs represent empowering tools in terms of their evidentiary value.

- **Reducing 'Third-Degree' means:** One of the main reasons behind the use of 'third-degree' methods to extract evidence is the short duration of police custody that limits the time available for preliminary investigation (Lokaneeta, 2020), along with the admissibility of confessions as evidence vide Section 27 of the Indian Evidence Act. Here too, FRTs have potential value in better evidence, subject to its acceptance.

- **Procedural transparency and functional autonomy:** FRTs could also engender greater functional autonomy for the police. Where delinquent officers and criminals enjoy political patronage, it is difficult to follow due process (Singh, 1996). But where technology automates the process of criminal identification, one could argue it leaves less scope for discretion.

- **Crime deterrents:** FRTs can also serve as deterrents of crime. Media reports suggest that these technologies have served as crime deterrents and reduced crime incidence; Surat's city police credit their FRT system with a 27% reduction in crime (Gershgorn, 2020). The impact of such systems on displacement of crime still needs to be studied.

B. Concerns with FRT deployment:

- **Risk of systemic inconsistencies in FRTs' deployment:** State police forces do not operate in a unified way when it comes to surveillance in India (Kharbanda, 2015). The absence of a uniform operational code in both technology use and the underlying processes allows for inconsistencies. Hyderabad city police reportedly scanned facial data and fingerprints of random passersby ultra vires of the usual procedure (Barik, 2019). Deploying FRTs in the absence of a basic minimum unified approach could lead to perverse consequences.

- **Risk of discriminatory surveillance:** FRTs run the risk of presumptive policing, especially when they are used in real-time and layered upon a past record of discriminatory surveillance. Recently, media reports indicated that the Delhi police used FRTs to screen and filter law and order “miscreants” at a political rally in December, 2019 against a facial dataset containing images collected from prior protest sites (Mazoomdaar, 2019).

- **Risks of inaccuracy and bias:** FRTs' accuracy and biases are still being determined and remedied. As per the National Institute of Standards and Technology's (NIST) extensive tests, no FRT system has 100% accuracy (Jain, 2020). Pete Fussey, a surveillance expert found London's FRTs' to be accurate in just 19% of cases (Dodd, 2020). There are also racial and gender-based variances in FRTs' performance; MIT's Gender Shades project found them to work better on lighter skin tones and the error difference of IBM Watson's accuracy on gender was almost 34.4%.

These inaccuracies may be further exacerbated by the following variables which have yet to be adequately addressed by FRT systems:

- **Uncontrolled environments:** Accuracy seems to be directly correlated with more controlled environments—unfeasible in policing. As per NIST's Face in Video Evaluation, accuracy in less controlled environments (like a sporting venue) varies between 36% and 87%, depending on camera placement (Crumpler, 2020).

- **Impersonation or presentation attacks:** These represent a major challenge to even sophisticated systems (Singh, et al., 2020). The ability of the system to address situations where criminals are in disguise or where a recent image of the person is unavailable remains to be seen.

- **Use of masks:** Face masks block access to a large amount of biometric data that uniquely sets people apart (Ng, 2020). Although training datasets are being developed to upgrade the algorithms, their robustness will need to be thoroughly verified.

Policy recommendations

A. Immediate safeguards

- **Defining the scope of use:** A part of the framework outlines best practices for the responsible design of FRT at the stage of defining the scope of work. This includes a clear understanding of the purpose for which FRT is being deployed and designing evaluations that particularly address these concerns.

- **Due diligence in procurement of the technology:** Since FRTs depend largely on the base dataset, steps should be taken to ensure that the training dataset captures as variance in characteristics as possible to reflect reality. Training datasets need to be checked to ensure the data does not suffer from disproportionate representation from certain sections of the society.

- **Defining a Data Management Policy:** To formalise these practices and ensure uniform application, police must define a clear data management policy outlining the integrity and confidentiality of data and the period of retention of the collected data (State of Washington, Bill on Facial Recognition, 2020).

- **Enforcing purpose limitation:** In order to foster trust, the police must collect and use data only for its intended purpose. A clear policy of purpose limitation—collecting of data for explicit and legitimate purposes—is required.

- **Undertaking a data impact & proportionality assessment:** The four-pronged test put forth by the nine-judge bench of the Supreme Court in KS Puttaswamy vs. Union of India (2017), i.e. legality, legitimacy, proportionality and procedural guarantee, must be applied to ensure the right to privacy (AK, 2018). Purpose and usage should be mandatorily defined and limited to absolutely necessary objectives in consonance with the international principles of surveillance.

B. Long-term measures

- **Need for improving police training and ensuring technology upgradation:** Several commissions have noted the lack of police training and expertise in conducting professional investigations. They also suffer from the lack of basic technology upgradation. A NITI Aayog paper by Jain and Gupta (2016) mentions that the CCTNS, which was sanctioned in 2009, was still not fully implemented and functional across all states.

- **Improving police accountability:** The Model Police Act and the landmark Prakash Singh vs. Union of India (2006) Supreme Court ruling prescribed the setting up of a Police Complaints Authority (PCA) at the district and state level to look into charges of misconduct by police officers. Presently, only 15 states and seven union territories have operational PCAs and only six states have them at both state and district levels.

- **Regulation and independent oversight boards:** The Personal Data Protection Bill will play a crucial role in the regulation and monitoring of FRT usage. The Bill advocates for the setting up of an independent 'Data Protection Authority'. If the body created is not independent, it will fail to build public trust in the technology and by extension the police. Grievance redressal mechanisms are critical for public trust when it comes to new technologies.

References

AK, A., 2018. Proportionality Test For Aadhaar: The Supreme Court'S Two Approaches. [online] Bar and Bench - Indian Legal news. Available at: <https://www.barandbench.com/columns/proportionality-test-for-aadhaar-the-supreme-courts-two-approaches>.

Bailey, R., Bhandari, V., Parsheera, S. and Rahman, F., 2018. [online] Use of personal data by intelligence and law enforcement agencies. Available at: <https://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf>.

Barik, S., 2019. 'Fingerprint Is Not A Big Issue': Hyderabad Police On Collecting Biometrics Of 'Suspects'. [online] MediaNama. Available at: <https://www.medianama.com/2019/10/223-hyd-police-on-collecting-biometrics-of-suspects/>.

Bothra. 2019. Why is our conviction rate so low?. Available at: <https://www.newindianexpress.com/opinions/2019/feb/21/why-is-our-conviction-rate-so-low-1941680.html>

Crumpler, W., 2020. How Accurate Are Facial Recognition Systems – And Why Does It Matter?. [online] Center for Strategic & International Studies. Available at: <https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter>.

Dodd, V., 2020. Met Police To Begin Using Live Facial Recognition Cameras In London. [online] the Guardian. Available at: <https://www.theguardian.com/technology/2020/jan/24/met-police-begin-using-live-facial-recognition-cameras>.

Fussey, P. and Murray, D., 2019. Independent Report On The London Metropolitan Police Service's Trial Of Live Facial Recognition Technology. [online] Available at: <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf>

Gershgorn, D., 2020. NEC Is The Most Important Facial Recognition Company You'Ve Never Heard Of. [online] Medium. Available at: <https://onezero.medium.com/nec-is-the-most-important-facial-recognition-company-youve-never-heard-of-12381d530510>.

Jain, S. and Gupta, A., 2020. Building Smart Police In India: Background Into Needed Public Reforms. [online] Niti.gov.in. Available at: <https://niti.gov.in/writereaddata/files/document_publication/Strengthening-Police-Force.pdf>.

Kharbanda, V., 2015. Policy Paper On Surveillance In India. [online] Cis-india.org. Available at: <https://cis-india.org/internet-governance/blog/policy-paper-on-surveillance-in-india>.

Law Enforcement Imaging Technology Task Force. 2019. Law Enforcement Facial Recognition Use Case Catalog. Available at: <https://cdn.ymaws.com/www.ijis.org/resource/collection/93F7DF36-8973-4B78-A190-0E786D87F74F/Law_Enforcement_Facial_Recognition_Use_Case_Catalog.pdf>

Lokaneeta, J. 2020.The Truth Machines: Policing, Violence, and Scientific Interrogations in India

Mazoomdaar, J., 2019. Delhi Police Film Protests, Run Its Images Through Face Recognition Software To Screen Crowd. [online] The Indian Express. Available at: <https://indianexpress.com/article/india/police-film-protests-run-its-images-through-face-recognition-software-to-screen-crowd-6188246/>.

Ng, A., 2020. Facial Recognition Firms Are Scrambling To See Around Face Masks. [online] CNET. Available at: <https://www.cnet.com/health/facial-recognition-firms-are-scrambling-to-see-around-face-masks/>.

Ng, A., 2020. Your Face Mask Selfies Could Be Training The Next Facial Recognition Tool. [online] CNET. Available at: <https://www.cnet.com/news/your-face-mask-selfies-could-be-training-the-next-facial-recognition-tool/>.

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

Singh, NK 1996. The Plain Truth: Memoirs of a CBI Officer New Delhi: Konark Publishers

Singh, R., Agarwal, A., Singh, M., Nagpal, S., & Vatsa, M. (2020). On the robustness of face recognition algorithms against attacks and bias. arXiv preprint arXiv:2002.02942.

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

The Indian Express. 2020. Pune Police Use Drones To Track Home-Quarantined Persons. [online] Available at: <https://indianexpress.com/article/cities/pune/pune-police-use-drones-to-track-home-quarantined-persons-6337618/>.

Vyas, S., 2019. CCTV cameras help solve 1,100 crimes in Mumbai, Pune. [online] The Hindu. Available at https://www.thehindu.com/news/cities/mumbai/cctv-cameras-help-solve-1100-crimes-in-mumbai-pune/article29336384.ece

Data Governance Network

The Data Governance Network is developing a multi-disciplinary community of researchers tackling India's next policy frontiers: data-enabled policymaking and the digital economy. At DGN, we work to cultivate and communicate research stemming from diverse viewpoints on market regulation, information privacy and digital rights. Our hope is to generate balanced and networked perspectives on data governance - thereby helping governments make smart policy choices which advance the empowerment and protection of individuals in today's data-rich environment.

About Us

IDFC Institute has been set up as a research-focused think/do tank to investigate the political, economic and spatial dimensions of India's ongoing transition from a low income, state-led country to a prosperous market-based economy. We provide in-depth, actionable research and recommendations that are grounded in a contextual understanding of the political economy of execution. Our work rests on three pillars – 'State and the Citizen', 'Strengthening Institutions', and 'Urbanisation'. The State and the Citizen pillar covers the design and delivery of public goods, ranging from healthcare and infrastructure to a robust data protection regime. The Strengthening Institutions pillar focuses on improving the functioning and responsiveness of institutions. Finally, the Urbanisation pillar focuses on the historic transformation of India from a primarily rural to largely urban country. All our research, papers, databases, and recommendations are in the public domain and freely accessible through www.idfcinstitute.org.

Acknowledgments

The authors would like to thank an anonymous reviewer and N.S. Nappinai for comments on the paper. We would also like to thank M.N. Reddi and Niranjan Rajadhyaksha for their ideation and comments on numerous drafts of the paper. Special thanks to Alex Fager and Seshadri Govindan who helped in the initial stages of the paper. The authors benefited from comments received at the 5th Quarterly Roundtable of the Data Governance Network, where an early draft of this paper was presented.

About the Authors

Priya Vedavalli is an Associate at the IDFC Institute and her current research focuses on the criminal justice system in India, particularly policing. Her other research interests include economic history and impact evaluation.

Prakhar Misra is a Senior Associate at IDFC Institute. His research interests are in state capacity and governance, and focuses on the use of technology to improve the same.

Tvesha Sippy is a Senior Analyst at IDFC Institute and her current research focuses on the criminal justice system in India.

Avanti Durani is an Assistant Director and Junior Fellow at IDFC Institute. Her research focuses on criminal justice with a focus on policing, special governance zones and rural development.

Neha Sinha is Deputy Director and Associate Fellow at IDFC Institute. In addition to her management responsibilities, she leads research on criminal justice with a focus on policing.

Vikram Sinha is Head, Data Governance Network, at IDFC Institute. He leads research focused on technology use for governance, data empowerment, privacy and digital competition.

IDFC Institute
301, 3rd Floor, Construction House 'A', 24th Road, Off Linking Road,
Khar West, Mumbai 400052

/idfcinstitute @idfcinstitute /IDFCInstitute