Data Governance Network
Anchored by IDFC Institute

April 2021

Working Paper 16

Facial Recognition Technology in Law Enforcement in India: Concerns and Solutions

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

IDFC Institute

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.

Disclaimer and Terms of Use

The views and opinions expressed in this paper are those of the authors and do not necessarily represent those of the organisation.

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Design

Cactus Communications

Suggested Citation:

Vedavalli, P., Misra, P., Sippy, T., Durani, A., Sinha, N., & Sinha, V. (2021). Facial Recognition Technology in Law Enforcement in India: Concerns and Solutions. Data Governance Network Working Paper 16.

Supported by a grant from Omidyar Network

Abstract

In a post-COVID world, we see the adoption of facial recognition technologies further intensifying. Law enforcement agencies have observed immense benefits in criminal tracing and crime prevention with facial recognition technologies, yet the dangers to privacy and misuse of data are widely recognised as well. This paper outlines the use cases of facial recognition technologies in the Indian context and unpacks the technological and institutional aspects, with respect to the police, governing facial recognition technologies. It further gives short-term and long-term solutions that must be implemented before wide-scale deployment of these technologies is undertaken.

Table of Contents

1. Introduction

Digitisation is core to governance today. However, the transformation from analogue to digital governance is fraught with challenges. It alters the dynamics of State-citizen interaction considerably. Unsurprisingly, when this happens in an area of governance where the State regularly exercises a monopoly over the use of force, the consequences of something going wrong are potentially severe. Governments must now confront these problems with regards to one of the latest digitisation pivots—Facial Recognition Technologies (FRTs).

Policing in India is increasingly using FRTs. The National Crime Records Bureau (NCRB) had earlier proposed a tender for nationwide deployment of Automated Facial Recognition System (AFRS). However, India has not addressed many important criticisms in relation to FRTs—lack of legal basis for use of the technology, breach of privacy of individuals, emerging facets of a surveillance state and loss of anonymity for individuals, to name a few. It is important that guidelines are set in place before the deployment of such technologies. The pending Personal Data Protection Bill, 2019 (PDP Bill) would form the backbone of any regulatory framework, of course, but it is only one component. Long overdue reforms in policing are necessary; so is setting up an independent oversight body to regulate the use of such technologies. Together, these form an essential package of long-term structural reforms.

The ongoing COVID-19 crisis has increased the urgency of such remedial measures. The pandemic has put the use of contactless technologies into overdrive. India, like other countries, has used a contact tracing application and maintained and enforced quarantine lists through various technological means. With the pandemic normalising the use of such technologies, there is a risk that these will continue to be used without adequate thought in the post-pandemic world as well.

Concurrently, we are seeing a pushback against FRTs. The death of George Floyd in the US was a watershed event which raised questions about the actions and legitimacy of law enforcement agencies. This has led to many companies to begin backtracking on FRT investments. IBM recently announced a complete pullback from developing and researching FRTs for law enforcement (Peters, 2020). The principal reason behind this is that it thinks the technology is still not completely free of inaccuracy and racial or gender biases. Amazon followed suit, announcing a one-year moratorium on selling police access to its facial recognition technology—Rekognition (Statt, 2020). In this paper, we make a case that these concerns with FRTs can and must be addressed by immediate, short-term measures until the long-term reforms are in place.

We examine applications of FRT and recognise that FRTs can be crucial in fighting crime and the pandemic in India. While the legitimacy of the use of FRTs by law enforcement is being debated, that is beyond the scope of our paper. We analyse limitations and benefits of FRTs, and elaborate on safeguards that need to be put in place before implemented. Section 2 of this paper discusses why using FRTs would be premature and hurt the policing process. Section 3 details the applications and use cases of FRT for police in India. Section 4 elaborates on technical aspects for consideration of the police. Section 5 details the concerns surrounding FRTs. Section 6 gives prospective safeguards that are critical to FRT deployment. Section 7 concludes the paper.

2. FRT use cases: premature load-bearing

2.1 Use cases during the COVID-19 pandemic

The COVID-19 pandemic has accelerated FRTs' emergence. Contactless technological solutions are replacing touch-based fingerprint detection systems. Carlaw (2020) had predicted that COVID-19 will have a significant short- and long-term impact on biometric companies and the lives of people. Here are a few examples of FRT use during the pandemic in India:

1. The Technology Development Board (TDB) of the Department of Science and Technology (DST), Government of India, has 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).
2. In Pune (The Indian Express, 2020), the police have been using the Maharashtra Home Quarantine Tracking System (MH HQTS) which is an application used to monitor persons who have been home quarantined. They have been asked to download the application and click a picture of themselves at regular intervals. The tracking system uses a facial recognition programme along with location tracking to ensure that the person is at home.
3. The Telangana state government announced its plan to replace its biometric attendance system with a facial recognition system post-COVID-19 (Sur, 2020).

The increasing use of this technology has set in motion private sector use case scenarios. Companies want to install face recognition machines for attendance, access and hotel locks (Mathur & Ahaskar, 2020). The fallout of this could be massively problematic considering that the use of facial masks further reduces the accuracy of the matches. Private companies must wait for government regulations before large scale deployment.

2.2 Prior government uses cases

However, the use of FRT predates the pandemic. Consider the following government uses of such technologies:

1. The NCRB first issued the request for proposals for AFRS in July 2019 to supplement the business carried out by the police. It attracted significant criticism and the tender was later revised to exclude CCTV footage. However concerns still surrounding the tender include legality (which was substantiated by NCRB by citing the cabinet note) and 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).
2. The Hyderabad Airport, as a part of Digi Yatra, an initiative by the Ministry of Civil Aviation which involves digital processing of passengers at the airports, launched FRT in July 2019 where passengers were given the option of signing up for the pilot project.
3. The Delhi International Airport rolled out facial recognition systems on a trial basis in collaboration with Vistara Airlines in September 2019.
4. The Telangana government piloted the use of FRT in 10 polling stations during the municipal elections in January 2020 to verify voters (The Hindu, 2020).
5. The police deployed FRT during the protests against the Citizenship Amendment Act-National Register of Citizens (CAA-NRC) in Delhi in early 2020.

Given that regulations governing such technologies are still being debated and the performance of FRT is globally under question, we believe it is too soon to start large scale deployment in India. Lant Pritchett, Michael Wolcock and Matt Andrews talk about premature load-bearing in their paper 'Capability Traps? The Mechanisms of Persistent Implementation Failure' (2010). The analogy is that of a scaffolding of a bridge being mistaken for the bridge itself. If we drive a truck on the scaffolding, it will collapse, defeating the purpose, undermining the progress so far and bringing it all back to square one (Pritchett et al., 2010). FRT use cases in India point towards a similar scenario.

Deploying FRTs at this time in India will thus be premature on two counts. First, the performance of the technology is suspect, undercut by ethnic, gender and other biases. Second, Indian law enforcement is not institutionally equipped with the skills, procedures and protocols to deal effectively with FRTs. We look at these issues more closely in section 5. Before that, however, we turn to the use cases of FRTs in law-enforcement and analyse the technical aspects of the same.

3. FRT use cases in law enforcement

Law and order is the purest form of a public good, and the police is often the public's first interface with the state. Their core duties, such as crime prevention, investigation and public order maintenance, involve surveillance in differing degrees. This, of course, has implications for individuals' privacy. Privacy is a fundamental right, with the primacy in citizen-state relations that entails. While it is subject to reasonable restrictions — as are all fundamental rights — in cases of national security and criminal investigation, the bar for abrogating it should be high. The procedure followed must be just, fair and reasonable. While it may be legitimate for governments to surveil citizens in certain contexts, it must be in proportion to the necessity.[1] In this paper, we make a case for embedding a few key safeguards, building on those proposed by Bailey et. al (2018). We root our discussions in practice and implementation of FRTs, analysing their use cases.

In terms of substantive outcomes, there are 19 known use cases of facial recognition technologies for law enforcement.[2] These are broadly classified into field use cases, investigation use cases and custodial and supervisory use cases (Law Enforcement Imaging Technology Task Force, 2019).

3.1 Categories of use cases in law enforcement

3.1.1 Field use and investigative use cases of FRTs—towards better evidence?

On the investigative front, FRTs carry potential in terms of their evidentiary value. Triangulating data from call records, automobile number plates, fingerprints and FRTs can empower investigating officers. India's Automatic Facial Recognition System envisages facilitating the investigation of crime and

[1] Laws, legislations and other oversight mechanisms that place limits and build in checks when it comes to the use of such technologies are critical. The legal framework around surveillance in India is covered in the Telegraph Act, 1885, the Information Technology Act, 2000 and the Code of Criminal Procedure, 1973 (CrPC). Apart from these acts, the police manuals serve as guiding poles requiring surveillance of 'bad characters', 'suspicious strangers' and 'history sheeted' individuals.

[2] This is according to the findings of the 'Law Imaging Task Force'—comprising members from the Integrated Justice Information Systems Institute and International Association of Chiefs of Police.

detection of criminals, missing children/persons, unidentified dead bodies and unknown traced children/persons (NCRB, 2020). In 2017, 75 percent of the First Information Reports (FIRs) that were closed without investigation were due to insufficient or untraceable evidence. Quality of investigation, particularly given high vacancies in policing and case pendency, can benefit immensely from the use of technology. Presently, investigations are based mostly on oral testimonies and therefore, if witnesses turn hostile, the cases often cannot be pursued due to insufficient evidence (Bothra, 2019).

Better forensic evidence, along with inputs in the form of visual feeds from CCTVs/FRT, can go a long way in addressing not just the issue of quality of evidence but also pendency. 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). The Delhi police were able to locate 3,000 missing children using FRTs. Recently, in the Gauri Lankesh case, the police were able to narrow down on the suspect using such technologies. Since the suspect's face was covered, instead of facial recognition the Directorate of Forensic Sciences used a technique called forensic gait analysis to match the walking pattern of the killer with that of the suspects (Mint, 2019).

3.1.2 Custodial use case of FRTs—a potential deterrent to third degree methods?

FRTs also have merit in terms of their potential influence on policing processes—specifically custodial ones due to better evidence. Use of force by the police against those in custody is well documented. The main reason behind the use of 'third-degree' methods in India is the short duration of custody.[3] The police are supposed to bring the suspect in front of the magistrate in under 24 hours which limits the time available for investigation. This is compounded by the fact that confessions made to them do not have evidentiary value, instilling systemic distrust in the police. However, Section 27 of the Indian Evidence Act allows material discovered as a result of a confession admissible in the court. FRT may, subject to acceptance of evidence, play a role addressing the need for quality evidence.

3.1.3 FRTs' larger potential as a law enforcement tool—towards a lower cost of crime and augmented police capacity?

These technologies can also serve as deterrents to crime. The Institute for Economics and Peace estimated the cost of violence in India in 2017 as 9% of its GDP.[4] While we don't have estimates on the direct impact of FRTs on the economic cost of violence, media reports suggest that these technologies have served as crime deterrents and reduced the incidence of crime. For example, in Surat, the 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. Vacancies and lack of capacity in policing are other issues that can be addressed by augmenting police resources with technological capability. We are aware that our argument rests on the performance of the technology itself and the ability of the police officers to use it effectively. The latter depends on many structural issues currently ailing policing in India.

[5] The New York Police Commissioner too echoed this with the line “No one can be arrested on the basis of the computer match alone” (New York Times, 2020).

[3] For a richer discussion on this, please see The Truth Machines: Policing, Violence, and Scientific Interrogations in India by Jinee Lokaneeta

[4] The cost includes expenditure and economic effect related to containing, preventing and dealing with the consequences of violence.

3.2 Widespread usage by law enforcement in India

While the above three are benefits of using FRTs, we do acknowledge the risks and implications of the technology falsely identifying and implicating someone.[5] Regardless, India has already moved forward with widespread deployment of FRTs. We have broadly classified their current applications under the three heads below:

1. CCTV cameras: Used by various states/cities to carry out real-time surveillance using facial recognition. In 2015, Surat became the first city in India to deploy real-time surveillance through facial recognition systems. Surat's system was used to convict 150 people in its first year of operation. The city police credit it with a 27% reduction in crime in the city of 5.5 million people (Gershgorn, 2020). Since then, many city police departments across India have piloted or deployed FRT.
2. Mobile applications: FaceTagr, an application used by police officers in Tamil Nadu, Andhra Pradesh and Puducherry, scans the offender's face and returns data about cases related to them in the database. Police departments in Uttar Pradesh, Uttarakhand and Rajasthan also use similar apps developed by various external vendors.
3. Databases: Both the above applications depend on a database. The Integrated People Information Hub set up in Hyderabad pulls information from dozens of places to build individual profiles of people. The database links CCTV footage, fingerprint data, call record details, voter ID, driving license, Aadhaar number and a crime number, offering a "360-degree view" of citizens.

Such widespread use calls for a serious analysis. FRTs must instead serve as a tool to aid and assist the police in investigations. These technologies are transformational only if the requisite safeguards are in place. Thus, before the intent of authorities and institutional readiness are analysed, we look at their technological readiness in the next section.

4. Technical aspects of FRTs

The accuracy rate of FRT has been called into question. Broadly, they are used for two purposes: verification[6] and identification[7] (Introna and Nissenbaum, 2010). The accuracy differs for both. We unpack the questions on the technical aspects of FRT that law enforcement agencies need to answer, in order to decide what uses can FRT be put to.

4.1 Choosing method of face detection and algorithm

FRTs work on pattern recognition algorithms which extract patterns from the data fed into the system

[6] Verification involves checking the identity of the person presenting credentials. The probe image is matched on a one-to-one basis with the gallery (reference database) which already contains the person's details.

[7] Identification involves matching the probe image — one-to-one — with the gallery to check who the individual is. The complication in this scenario is whether it is a closed set or an open set identification. Closed set ensures that we know that the individual is part of the gallery. Open-set means that there is a chance the individual is not part of the gallery. Thus, if the system rejects a match, it could mean one of two things: a) the system has made a mistake in the closed set scenario or b) in the open set scenario, it could mean either that the system has made a mistake or that the person is indeed not part of the system. Watchlist/tracking is an extension of the identification purpose, which is the most common use by law enforcement. It involves looking for a particular suspect and one-to-many matching of the suspect to everyone under the scanner.

and match it with stored data. There are various types of facial recognition algorithms that do this and each has a different approach to extracting the feature and matching it. The algorithm takes the 'probe' image (the image that one wants to match), detects the face and converts it to a format that is consistent with the ones in the reference database. It then extracts 'features' from the probe image and matches this to the reference database. There are four categories of face detection methods (Yan, Kriegman and Ahuja, 2002) and various algorithms (eigen-based, neural networks, distribution-based, etc) that can be used. Each algorithm has a different approach to extracting image information. This is the first thing for law enforcement agencies to clarify: which methods of face detection and feature extraction should be used for law enforcement purposes. Further, what are the limitations of each? A cost benefit analysis should be undertaken to reach a conclusion on algorithms being chosen.

4.2 Measuring performance of the algorithm

The key question is how will the performance of an algorithm be measured or evaluated? A lot of the facial recognition developers publish the accuracy rates as one of the metrics of the algorithm's performance. However, accuracy rate is one of the many metrics of performance. Accuracy rate is the number of correct classifications out of the total number of cases tested. This fails to capture one of the most important aspects, the ability to recognise, let us say, a criminal correctly. For example, in a dataset of 1,000 people with 20 criminals, as long as 980 of the non-criminals are recognised as non-criminals correctly, even if the model incorrectly classifies 20 of the criminals wrongly as non-criminal, the accuracy rate is still 98%. Hence there are other metrics to measure performance such as the number of false positives, false negatives. The threshold of the similarity score affects the number of false accepts and rejects of matches — in other words, type 1 and type 2 errors (Introna and Nissenbaum, 2010). If it is set too high, then a legitimate identity claim may be rejected. Conversely, if it is set too low, a false claim may be accepted. In the case of law enforcement, for instance, while identifying a criminal, the person may be in disguise, which in this case could be classified as a false reject. Thus, clarity on how such situations will be dealt with and checks to fool proof the technology is imperative before they are deployed. Other metrics of performance include precision, recall, F1-score, to name a few.

4.3 Quality of image

Since the performance of the facial recognition algorithm depends on the underlying image, the quality of the image plays an important role (Face Recognition Vendor Test, 2020). While matching the probe image with the database, a similarity score is generated for the match. This is accepted or rejected based on the threshold of acceptance which, in the case of law enforcement, will be high (Wood, 2018). The algorithm is therefore trained on various images until it is capable of generating a match with a reasonable level of accuracy. Lighting conditions, background, orientation of the face and camera distance are as important in these images as they are in actual use cases. All of these factors influence the accuracy of the match. Image quality is, in fact, perhaps the most significant factor for it. This is critical in the context of law enforcement since the ability to discern if an individual is indeed who they claim to be forms the basis of enquiry.

4.4 Evaluations

Depending on the purpose and the context of use, law enforcement has to run evaluations on the system and its algorithm before it is deployed for use. These evaluations must be conducted in settings as close to the situations in which the facial recognition system is expected to perform in real life. Moreover,

reporting the results of such evaluations will play a crucial role in understanding the pitfalls in the use of such technology and maintaining transparency. It will go a long way fostering trust and acceptance of the technology. Fussey and Murray (2019) published an independent report on the London Metropolitan Police's trial using live facial recognition technology. This kind of openness and willingness to evaluate play a huge role in informing the public about the strengths and pitfalls of the system and its users—the police.

We assert that evaluating FRTs on all these fronts is essential, particularly when the temptation to deploy them hastily in times of crises, such as now, may lead to their premature adoption for law and order as well. We turn to the issues with such deployment in the next section.

5. Concerns with FRT use in law enforcement

The Indian and many other legal systems rest on the tenet of 'innocent until proven guilty'. However, the act of constantly scanning and monitoring people stands in stark contradiction to this principle. This is a critical concern from a criminal justice point of view. Technology has the potential to provide the State with unfettered access to a person's data. This is particularly worrisome, especially given the inadequacy of legal safeguards[8] to cope with the increasing datafication of society and governance over the past two decades in India.

Concerns around facial recognition can be broadly classified as challenges within the current set up of law enforcement agencies — the capability of institutions to regulate such technology—and concerns with the technology itself — such as accuracy rates (part of which was discussed in the previous section).

5.1 Concerns with the law enforcement setup in India

5.1.1 Lack of unified approach in the deployment of technologies

State police forces do not operate in a unified way when it comes to surveillance in India (Kharbanda, 2015). According to the Seventh Schedule of the Constitution of India, 'Police' and 'Public Order' are state subjects. The legislative authority, allocation of powers and functions thus rest with the state government. Though the Bureau of Police Research and Development (BPR&D)—a Central body under the Union Ministry of Home Affairs—defines the range of functions as well as manuals that need to be prepared and maintained, every state has its own police act and manual.[9] Thus, a system to fully and effectively integrate facial recognition in and across each state, as well as state-specific laws, may be needed.

[8] The legal safeguards are continuously evolving at the time of writing this paper. It has been widely acknowledged that they aren't sufficient. Apart from the IT Act, 2000 and related SPDI Rules, NITI Aayog introduced a National Strategy on Artificial Intelligence. Added to this, the Personal Data Protection Bill is currently being debated in Parliament and a framework to govern Non-Personal Data has been introduced for public comments. The legal safeguards based on these documents are still to be legislated upon. In late 2019, a study by Comparitech placed India in the bottom 5 non-EU nations in protecting privacy of citizens, making the lack of these safeguards worrisome.

[9] For example, the BPR&D model police manual allows the police to carry out surveillance against 'bad characters', among others. The Bombay Police Manual (1959) does not define this term, leaving police officers with the discretion to interpret it. On the other hand, the Kerala State Police Manual (1969) defines bad characters to include dossier criminals, known depredators, suspects, ex-convicts and rowdies.

The absence of a uniform operational code in both use of the technology and the underlying processes allows for procedural inconsistencies. Consider the case of Hyderabad city police who are reported to have scanned facial data and fingerprints of random passersby *ultra vires* of the usual procedure (Barik, 2019). The police collected such data from people "suspected" of being criminals on the basis of their "intuition". While the procedure for legitimately collecting facial data is yet to be legally codified, collecting fingerprint data in this manner is clearly *ultra vires* the procedure outlined in the Prisoners Act, 1920. [10]

Such transgressions leave the government with the mammoth task of regulating each specific use case. While specialised state-specific bodies have a role to play, having a basic minimum unified approach sets a common threshold of requirements that must be met in the present and possibly in the future. The absence of a common, transparent threshold will damage the legitimacy of such technology, and therefore, public trust in it.

5.1.2 Lack of oversight regulations

1. Potential misuse of powers

The police have adopted unlawful surveillance procedures in the past. In 2019, the Central Bureau of Investigation (CBI) unlawfully intercepted phone calls of a businessman who allegedly offered bribes to bank employees to avail himself of credit. The Bombay High Court in *Vinit Kumar vs. Central Bureau Of Investigation, 2019* ruled that the action of the CBI was ultra vires of Section 5(2) of the Information Technology Act, which can be applied only in two circumstances: public emergency or public safety. While such unlawful uses of Call Detail Records (CDR) remain, there are plenty of cases where the use of such records have led to the solving of many criminal cases. CDR is one of the most important sources of evidence for police officers during investigation.

These risks continue to remain in the context of FRTs where the police will have access to immutable biometric data. A draft version of the PDP Bill tabled by the Justice Srikrishna committee in 2018 precluded the State from accessing such data without an individual's consent; except where such access was authorised by parliamentary legislation. However, in the final version of the Bill tabled before the Parliament in 2019, these clauses were amended (Agrawal, 2020). Section 35 of the amended PDP Bill allows the Central government to exempt any government agency from the provisions of the Act (including the "offences" chapter) for purposes of public order, national security, etc. Section 36 exempts "law enforcement and investigation" proceedings from certain provisions pertaining to "obligations of data fiduciary"; "grounds for processing personal data without consent"; sensitive data of children; rights of data principle; transparency and accountability measures. These amendments give "virtual carte blanche to the government to exempt any or all of its agencies to access personal and non-personal data of individuals and other entities on the mere declaration that there exist circumstances such as national security reasons, criminal investigations etc." in the words of Justice Srikrishna.

2. Role of private entities

Many of the cameras that are set up by private organisations for security purposes are also being used by the police for purposes of investigation, making it important to regulate the role of private organisations

[10] According to this Act, the police are authorised to take fingerprints of convicted persons sentenced to rigorous imprisonment for a period exceeding a year, persons arrested but not convicted for an offence which is punishable with rigorous imprisonment for a term upwards of one year or habitual offenders. In other words, fingerprints can be taken where an arrest has been recorded (Barik, 2019).

in setting up the necessary infrastructure for surveillance. According to the Public Safety (Measures) Enforcement Act, 2013 in Telangana, CCTV cameras have to be installed by private establishments that are frequented by a large number of people with a likelihood of public gathering of 100 people or more at a time. Every owner running the establishment is expected to store video footage for a period of 30 days and provide the same as and when required by an Inspector of Police, having jurisdiction over the area or any other authority as may be notified by the Government. Further, they are expected to file returns certifying that measures are being adhered to, and that the relevant equipment is in working condition, once in every six months. While storage aspects are mentioned, various other requirements, which are in practice internationally are missing. For example, the legal requirement for informed consent for data collection. Are there mandatory signs put up notifying people that they are surveilled?

European countries such as Germany, UK, France and Sweden have extensive laws around installing CCTV cameras (Gras, 2004). In the UK, individuals and commercial enterprises installing CCTV cameras have certain guidelines to adhere to. Individuals need to inform their neighbours that they are installing a CCTV camera and put up a notice or a sign saying that the place is under surveillance. In cases where the CCTV camera captures private areas of the neighbour, one has to enable privacy masking, which blanks out sensitive areas in the recording. This is over and above the data management rules.

This is followed by the requirement of a privacy impact assessment. Commercial enterprises are required to carry out a privacy impact assessment, appoint a person in charge of the CCTV camera and publish the name and contact details of someone that people can raise queries/complaints with (Champion, 2020). Any private organisation can buy a CCTV camera and set it up for security purposes. In some cases, the footage even captures passersby in public spaces.

However, CCTV cameras remain an important source of evidence for law enforcement, particularly in managing traffic violations. Close to 700,000 and 1,400,000 e-challans were generated for traffic violations in Mumbai and Pune respectively over two years (Vyas, 2019). Thus in order for them to continue to be a valuable source of evidence, strict oversight regulations are essential.

5.1.3 Discriminatory surveillance

The Executive Magistrate and the police are legally empowered to implement surveillance measures to arrest suspected persons in order to maintain peace and prevent offences. The measures laid out in the BPR&D model police manual include tracking movements of individuals with a past record of criminal activity, maintaining a register of suspected offenders, maintaining a “bad character” roll of strangers with suspicious conduct or demeanour and surveilling of “bad characters”. However, what constitutes “bad character” is a subjective decision.

In the past, certain communities, such as the Hijras, were notified as bad or 'criminal' according to the Criminal Tribes Act, 1871. The police conducted discriminatory surveillance against them whereby they were confined to certain settlements, made to carry identity cards, register their fingerprints and give roll calls thrice a day. They were also the first suspects when a crime occured, and were detained by police for interrogation (Satish, 2011). Cases of custodial torture and sexual abuse agaisnt them were not uncommon.[11] Therefore, further enhancing the police's surveillance powers with FRTs is a concern.

[11] While the Act of 1871 was repealed in 1949, discrimination against Hijras continued. In a landmark 2009 case, Naz Foundation vs. Govt of NCT of Delhi and Ors, the Delhi High Court, while ruling that criminalising consensual homosexual sex between adults violated their fundamental rights, noted that “...attachment of criminality to the hijra community still continue[d]” (Shah, 2009).

In Uttar Pradesh, the police conducted aerial surveillance of homes located in CAA-NRC protest areas in January, 2020 (Tripathi, 2020). They justified this on the grounds of tracking movements of allegedly 'anti-social' elements. Reports indicate that subsequently, in February, the police detained 1,100 people for alleged links to violence during protests (Reuters, 2020). These people were identified using footage from drones. Similarly, it is reported that the Delhi police used facial recognition software to screen and filter law and order "miscreants" at a political rally in December, 2019 (Mazoomdaar, 2019). A police officer involved in the screening reported that "each attendee at the rally was caught on camera at the metal detector gate and the live feed from there was matched with the facial dataset within five seconds at the control room set up at the venue". It is reported that the facial dataset contained images collected from footage filmed at protest sites.

All of these cases point toward the concerns with respect to presumptive policing. These risks need to be highlighted and addressed before the widespread deployment of FRTs. Recently, the Telangana government announced the establishment of a police command and control centre to track footage from 100,000 CCTV cameras, putting "every inch of the state" on the police radar (Barik, 2020). Such widespread surveillance measures need to be preceded by and supported with adequate checks and balances, and police training and accountability systems. These are discussed in Section 6.

5.2 Concerns with the technologies used in FRTs

5.2.1 Performance

1. Uncontrolled environments

The purpose of FRT deployment and whether or not it is in a controlled environment have a huge bearing on its performance. Most of the technical examples and standards cited in this section are based on international evaluations due to the lack of evaluation procedures in India. Verification algorithms, when used to match people based on a clear reference image (like a passport photo or mugshot) have been known to achieve 99.97% accuracy scores based on standard assessments like National Institute of Standards and Technology's (NIST) Facial Recognition Vendor Test (FRVT). However, such controlled environments are rarely feasible when it comes to policing. NIST's Face in Video Evaluation (FIVE), 2017 tested accuracy in varied settings such as airport boarding gates and sports venues. The results show that the accuracy rate in a fairly controlled environment, such as the airport boarding gate, is as high as 94.4%. In a less controlled environment like a sporting venue, however, accuracy rates varied between 36% and 87%, depending on camera placement (Crumpler, 2020).

Most often, identification based on one-to-many matching in uncontrolled environments is precisely what law enforcement needs FRTs for. Variations in facial expressions, illumination, orientation and angle of the face are only some of the complications affecting the captured image's quality in such situations (Mohamed, Abou-Elsoud, and Eid, 2011). In India, we still do not have transparent independent evaluations of these technologies in the context of law enforcement making this a big technological concern.

2. Impersonation

Misrepresentations of one's identity are known as presentation attacks, which are in the form of

[12] The dataset is collected from the Internet, resulting in unconstrained face images similar to real world settings.

impersonation (acquiring the identity of another) or obfuscation (obscuring one's own identity). Examples involve the use of masks, corrective glasses, contact lenses, facial prosthetics, plastic surgery, heavy make-up, changes in hairstyles, etc. (Tsitiridis, Conde, Gomez Ayllon and Cabello, 2019). A Disguised Faces in the Wild (DFW) dataset was released in 2018 as part of the International Workshop held in conjunction with Conference on Computer Vision and Pattern Recognition. The dataset contained normal, disguised and impersonator facial images along with images with bridal make-up and plastic surgery. The results demonstrated high accuracy errors. When the tolerable false acceptance rates (i.e. the likelihood that the system incorrectly accepts a user who should have been rejected) were higher, systems were able to perform better. But at a zero tolerable false acceptance rate,FRTs were able to verify only 10% of the images correctly (Deng and Zafeririou, 2019; Singh, Chawla, Singh, Vatsa, and Chellappa, 2019). In other words, presentation attacks represent a major challenge to even sophisticated systems (Singh, Agarwal, Singh, Nagpal and Vatsa, 2020). How will inaccuracies be addressed in situations where criminals are in disguise or in cases where a recent image of the person is not available? How will the accuracy in those cases vary? These are important questions that need to be debated.

3. Use of masks

The COVID-19 pandemic has necessitated behavioural changes such as widespread adoption of face masks and protective gear that have exacerbated this obfuscation challenge. Protesters in Hong Kong used face masks to manipulate the FRT system, prompting the government to ban face masks. This indicates that the algorithms aren't robust enough to recognise masked faces (Ng, 2020). In mainland China, a facial recognition company, Hanwang Technology Ltd., has claimed that it can even identify people when they are wearing a mask with a recognition rate of 95%. However, this has a caveat. Identification was possible in an office setting with upto 50,000 faces drawn from Chinese police's identification database containing 1.2 billion people, but not built to work on such a huge database. (Yang, 2020).

As we adopt the use of face masks, “we are blocking access to a significant amount of data points that help us differentiate one person from another”, according to Eric Hess, senior director of product management at facial recognition company, SAFR (Ng, 2020). Hess argues that the “greatest amount of biometric data that uniquely sets us apart resides in the central portion of the face, just above the brow line all the way down to the chin”. While training datasets are now being developed to upgrade the algorithms, their robustness will need to be thoroughly verified (Ng, 2020).

4. Independent studies with poor accuracy

Unless enough evaluations of FRT performance are conducted, police deployment of such technologies across the world is bound to show poor performance. The Met police's FRT use in London, for instance, garnered worldwide attention. Pete Fussey, an expert on surveillance from Essex University, conducted the only independent review of the public trials and found it was accurate in just 19% of cases (Dodd, 2020). As per NIST's extensive tests and studies on the accuracy of 1:1 verification and 1:many identification, no FRT system has 100% accuracy (Jain, 2020).

Performance can be judged via the rate of false positives or false negatives, which leads to inclusion and exclusion errors, respectively. Exclusion errors will prove to be particularly costly when deployed in

[13] The United States Government Accountability Office has highlighted performance differences that exist for certain demographics and ways in which it can be mitigated. More on this can be found here: https://www.gao.gov/assets/710/708045.pdf

cases which require the identification of individuals on the most wanted/high risk watchlist. Further, the size of the database can overwhelm the processing capacity of algorithms (US Government Accountability Office, 2016). And the age of the database also matters (US Government Accountability Office, 2002). Time delays, sometimes even that of a year, between collecting and analysing probe images against a database may produce accuracy errors.

5.2.2 Inherent biases in the algorithms

Facial features which vary by race and gender have been proved to affect accuracy rates. MIT's Gender Shades project evaluated the accuracy of FRT products and found that all worked better on lighter skin than on darker skin tones. The error difference of IBM Watson's accuracy on gender was almost 34.4%.

Figure 1: Accuracy of various FRT softwares

Source: http://gendershades.org/overview.html

MIT Media Labs also tested technologies developed by Amazon, IBM and Microsoft and found that they misidentified female faces as male faces, and this was more pronounced when the skin colour was dark (Singer, 2020). In fact, Amazon's Rekognition made an erroneous prediction for 28 members of the US Congress. 40% of the false matches related to the 20% Congressmen and Congresswomen of colour. Buolamwini and Gebru (2018) reported similar inaccuracies and biases.

Such inaccuracies have prompted countries to revert to analog methods (Marda, 2019). For example, the Detroit Police publicly stated that it won't identify people solely on the basis of facial recognition technologies due to accuracy differences in identifying blacks versus whites (Harmon, 2019). In a diverse country like India, such technology will bring with it unique concerns. More than 55% of undertrials in India are either Dalit, Muslim or Tribals. If there is enough reason to believe that such technology can be inherently discriminatory, then its use should be limited (Saxena, 2016).

It is unclear why exactly these technologies misidentify individuals. Sometimes it is the base training data which is to blame—with biased and even bad image quality—and other times the law enforcement agencies' software is not updated with the latest algorithms (Valentino-DeVries, 2020, Heilweil, 2020). A recent study (Nagapal et al, 2019) found that much like the human neurological process, deep learning algorithms are also susceptible to “own-race” and “own-age” bias. More research to eliminate age and race biases in algorithms needs to be undertaken to develop fairer systems.

Besides racial and gender discrimination, misuse of FRTs could also lead to religious and caste based profiling. For instance, in China, reports indicate that police use FRTs to filter out Uighurs from the community and prefer algorithms that have the functionality of identifying Uighur/non-Uighur attributes. The technology is trained to identify specific community attributes using machine learning algorithms and databases of images that are labelled as Uighurs and non-Uighurs (Mozur, 2019). These concerns need to be thought about hard before bringing in mass deployment of FRTs (Joy, 2020).

6. The way forward: recommendations for using FRT

Considering the relatively unregulated nature of surveillance and inaccuracy of facial recognition technologies, we think there are a few measures that should be implemented before FRTs are mass-deployed. Some safeguards can rely on existing legal mechanisms and legislative frameworks—the Indian Evidence Act, the Criminal Procedure Code, Information Technology Act, Telegraph Act, Right to Information Act, Right to Privacy, etc. Others may require significantly ramping up capacity within the police and strengthening procedural safeguards before scaling up the technology.

We discuss five immediate safeguards and three long-term safeguards that should be implemented before FRTs are deployed en-masse.

6.1 Immediate Procedural Safeguards

6.1.1 Defining the scope of use

A white paper by the World Economic Forum, 2020, outlines 'A Framework for Responsible Limits on Facial Recognition'. This was developed as a part of the pilot phase of the working group which followed the four main steps captured in *Figure 2* below—Define, Design, Assess and Validate. The first step involved defining what constitutes responsible use of FRT by organising it around 11 main principles, which provide a good starting point.[14] The second step is on proportional use of FRT, which involves asking if FRT is tailored to solve the problem it intends to address. Third, incorporating privacy while designing the system at every stage of development and testing. The other important principles include accountability, performance, right for information, consent, notice and consent (when used in public places), right to accessibility, children's rights and finally, having an alternative option and human presence. While all of them may not be applicable in the Indian policing context, such working groups composed of various stakeholders should define principles suited to the law enforcement scenario that guide the scope of use.

Figure 2: A Framework for Responsible Limits on Facial Recognition

Source: World Economic Forum

[14] The first principle is addressing bias and discrimination. As we have discussed earlier, this is one of the major criticisms against facial recognition algorithms as recorded in many developed countries. While the kind of bias in India is unclear, it is imperative for organizations to take steps to ensure any biases are identified and resolved.

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. For example, in cases involving missing persons, should FRT be deployed? What warrants the use of FRT needs to be determined along with evaluations/pilots in similar contexts that show reasonable performance for the intended purpose.

Apart from such frameworks, scholars have recommended applications for which FRT can be used in India. For example, Thorat, Nayak and Dandale (2010) have suggested 11 different ways in which FRTs could be adapted and used in India.[15] Thus, the first step in use of FRT is clearly defining the scope of use. Defining use cases restricts the discretion available, particularly with the lack of functional police autonomy.[16] Amid concerns about performance and bias errors, the police should refrain from using FRT for real time identification until progress is made in applying such technologies around the world in similar settings.[17]

6.1.2 Due diligence in procurement of the technology

FRT use has raised concerns around discriminationatory surveillance on the basis of an individual's socioeconomic status, caste, gender, race, etc. Since FRTs depend largely on the base dataset, steps should be taken to ensure that the training dataset captures as many characteristics as possible to reflect reality. The algorithms are usually run on the training dataset which is then tested to see the performance of the algorithm. Training datasets need to capture the diversity of gender, age, colour, etc. that is seen in reality. This can be done by ensuring that the data does not suffer from disproportionate representation from certain sections of the society. These are essential features to understand at the stage of procurement.

Minimising the false negatives and the false positives is key to achieving effectiveness and reducing undue harassment of individuals (Parsheera, 2019). As we noted earlier, apart from the quality of the images, the algorithm underlying the FRT plays a huge role in accuracy rates. NIST has defined international standards to test for accuracy of such technologies and conditions under which they work better. The limitation must be identified at the due diligence stage.

6.1.3 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). A few guidelines must be codified

[15] These include using FRTs to prevent ATM fraud, identifying and verifying terrorists/criminals at airports, railway stations, aiding in the verification of passports, visas and driving licenses, and addressing the issue of duplicate voters, among others.

[16] The Second Administrative Reforms Commission's reports have explicitly noted that the police is often used to meet personal and political ends (Chaturvedi, 2017).

[17] CAA-NRC protests earlier in the year presented opportunities for the police to track people in crowds and public spaces using these real-time features. In fact 1,100 protestors were identified using FRTs according to the assertions of the Home Minister (India Today, 2020). However, until we have a complete understanding of the technology, the police must refrain from using such nascent features.

before the deployment of FRT.[18] Some indicative suggestions are below:

1. **Procurement:** The General Financial Rules, 1947, the Manual for Procurement of Goods, 2017 and the Delegation of Financial Powers Rules, 1978 are some of the legislations governing public procurement in India. Their objective is to ensure that government authorities with the financial powers of procuring goods in the public interest exercise transparency and act in a fair and equitable manner (Mara and Deshpande, 2020). The degree of transparency prescribed therein must be practised during the NCRB FRT tender process as well.

2. **Purpose and scope of use:** The handling and use of the technology refers to limiting the purpose for which FRT is deployed (6.1.4) and the scope for which it is used (6.1.1).

3. **Data management:** Secure data storage and operation are also essential. The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 issued by the Ministry Of Communications and Information Technology stipulate that body corporates or any individual on behalf of body corporate are required to have "a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies". Such guidelines must be extended to private entities falling outside the rubric of a body corporate that are working with law enforcement authorities to ensure secure management of biometric data.

4. **Training:** Personnel must be trained in the usage of technology, processes, existing laws and sensitisation about potential impact of privacy breaches in parallel. This is discussed in detail in section 6.2.1.

6.1.4 Enforcing purpose limitation

The outbreak of COVID-19 and the enforcement of the Epidemic Diseases Act, 1879, made control of the epidemic partially a law and order issue. Contact tracing became one of the early and important roles of the police.[19] In order to foster trust, the police must collect and use data only for its intended purpose. A clear policy of purpose limitation[20] — collecting of data for explicit and legitimate purposes — is required. The importance of clearly specifying and limiting the purpose for which data is collected and using it as intended will mitigate the risk of potential harm and misuse of the data (Matthan, Venkataraman, & Patri, 2018).

[18] This will be similar to the guidelines issued by the Ministry of Home Affairs, 2015 for interception of telephone calls, procedures for the lawful procurement of the technology, its handling and use, as well as the sharing, copying, storage and destruction of records, among others, must be codified upfront and adhered to from the outset.

[19] For example, in Telangana, FRT data of varying quality obtained through CCTV cameras became a tool for police to implement these orders (Bedi, 2020).

[20] Article 5(1)(b) of the GDPR gives more detail on the principle of purpose limitation and article 89(1) carves out exceptions for storing data compatible with the outlined purposes such as historical research or public interest.

This will require identifying the key data points that are relevant to the situation; collection must be limited to those parameters only. This relates back to the potential for indiscriminate surveillance and the current lack of regulatory oversight in the usage of technology.

In addition to specifying the purpose for which data is collected, a notice of its collection must be made prior to the act of collection (Article 29 Data Protection Working Party, 2013). For example, signage stating that information of a personal and sensitive nature is being collected in a particular area or sending a letter are ways to notify or keep the individual informed (Mathias and Kazia, 2016). These principles have also been outlined by the Justice AP Shah Committee (Xynou, 2015) and are in the current criminal code.[21]

As police adoption of FRT becomes more commonplace, it is likely that it will be used to detect and investigate crimes. The regulations relating to evidence gathering have already been extended to electronic evidence.[22] They must govern FRT as well (Bhatnagar & Shekhawat, 2020). The circumstances under which personal data is collected and whether such data is lawfully collected or not matters in defining the uses it can be put to.

6.1.5 Undertaking a data impact & proportionality assessment

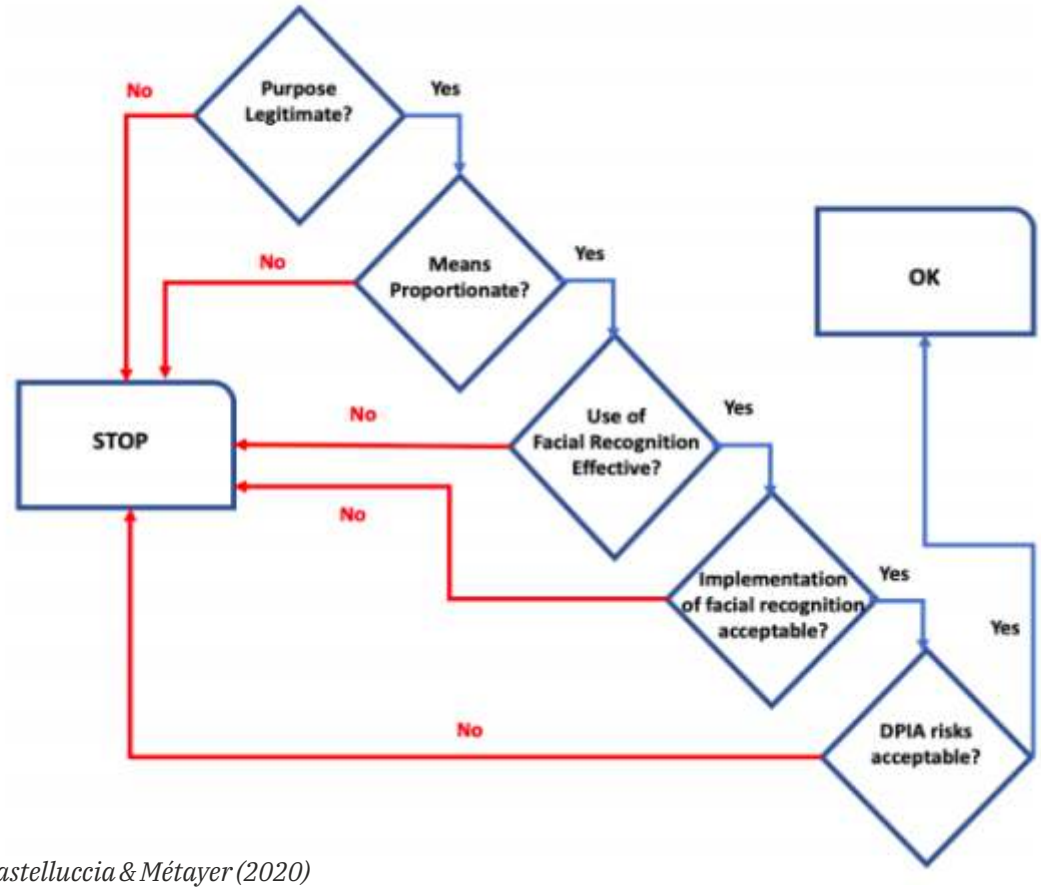
Understanding the impact of the use of FRT in a situation is important. Consider the rubric (Castelluccia and LeMétayer, 2020) presented as an example of the kind of safeguards that should be imposed. To illustrate, if someone needs to be identified for the purposes of national security, the answer to the question of the purpose being legitimate would be 'yes',[23] followed by an affirmative answer to the question of the means being proportionate. However, asking whether the use of FRT in itself is effective might lead to a 'no' which means it needs to be aborted.

[21] The Criminal Procedure Code, 1973 (CrPC) poses limitations on the gathering of evidence in a criminal investigation (Paliwala, 2019). Section 93 outlines the contours along which a search warrant may be issued (Bhatnagar & Shekhawat, 2020). For instance, sub-section 2 allows the court to limit the geographic scope of the search or inspection. Similarly, Section 165 of the CrPC provides guidelines for a search by a police officer and stipulates that the reasons for the search must be recorded in writing, which is then approved by a judicial authority (Deepthi, 2020).

[22] The amendment to the Indian Evidence Act, 1872 was an important breakthrough in this regard. With the introduction of Section 65A and 65B, the Act conferred legitimacy to previously inadmissible electronic evidence. Although recent cases (*Anvar P. V. vs. P. K. Basheer & Ors and Shafhi Mohammad vs. The State Of Himachal Pradesh*) highlight procedural uncertainties regarding the authenticating certificate for the electronic document and whether it is considered as primary or secondary evidence, the substantive validity of electronic evidence is not contended. Further, criminal/civil investigations are only strengthened with the help of CCTV footage of the crime scene (Ashby, 2017). Therefore, while navigating the labyrinth of the various types of evidence under the Act and their evidentiary value, it is imperative to limit FRT data as real, corroborative and circumstantial evidence in order to safeguard public interest (Sehgal, 2019).

[23] We recognize that this may not be 'yes' in all cases, but even in the cases it is yes, the use of FRT may not be automatically proportionate, thus underscoring the importance of the proportionality assessment.

Figure 3: Rubric for determining use of FRT



Source: Castelluccia & Métayer (2020)

Another example is the verification of individuals in government offices for attendance as proposed in Telangana (Sur, 2020). In case the purpose is viewed to be appropriate considering the outbreak of COVID-19 that has brought in the need for contactless methods of recording attendance. The means also seem to be proportional and the use of FRT in this case has proved to be effective. This brings us to the next step which involves determining if the implementation of such technology is acceptable. This squarely falls in the realm of consent and deliberation. Following this, a Data Protection Impact Assessment (DPIA) is recommended. It is one of the requirements of the Personal Data Protection Bill and a part of the Law Enforcement Directive for applications processing biometric data (Castelluccia and LeMétayer, 2020).

Finally, the four-pronged test put forth by the nine-judge bench of the Supreme Court in KS Puttaswamy vs. Union of India 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.

6.2 Long term solutions rely on police reforms and robust regulation

6.2.1 Police training and technology upgradation

We look at capacity building of the police force to handle FRTs responsibly. Thus, their training and technological upgradation become crucial.

1. Police training and capacity building

The largest proportion of the police is the constabulary in the field.[24] However, the constabulary's low entry-level qualification (completion of class 10 or 12 in many states) and inadequate training and preparation for their role are long-standing concerns, also noted by the Padmanabhaiah Committee. The Law Commission and the Second Administrative Reforms Commission also noted that officers lack the training and the expertise required to conduct professional investigations. They also have insufficient legal knowledge (on aspects like admissibility of evidence) and the forensic and cyber infrastructure available to them is both inadequate and outdated.

The lack of training is not limited to the constabulary alone. Since each of the State Police services has its own police academy for training, the lack of a unified approach for supervisory and senior police officers (excluding Indian Police Services (IPS) officers) is problematic here as well. FRT use requires functional knowledge of the underlying technology and the ability to discern false positives from false negatives (Introna and Nissenbaum, 2010). Apart from inspecting if it is indeed a false reject, it is imperative to understand that facial recognition systems can make errors. Specific training modules that help police personnel understand and identify such issues must be an integral part of the training programmes at the academies as a part of the curriculum. Automating and putting undue reliance on such facial recognition processes, without trained human oversight, can lead to disastrous outcomes. Additionally, training on capturing high quality images, use cases and sharing of information obtained from facial recognition searches, and time period after which the probe image should be deleted also needs to be factored in (Garvie, C., Bedoya, A., and Frankle, J., 2016).

2. Technological upgradation of the police

The Indian police also suffers from the lack of basic technology upgradation. The Status of Police in India, 2019 notes that on an average 70 police stations across 22 states did not have wireless devices, 214 police stations had no telephone and 24 had neither wireless nor telephone connectivity.

Figure 4: Facilities available at police stations

Facilities available at the station	Always	Sometimes	Never	No response
Functional computer	68	22	8	2
Functional CCTNS software	55	23	17	5
Forensic technology	27	20	42	9
Storage Facility for documents	67	20	11	2

All figures are in percentages. Figures are rounded off and might not add up to 100.

Question asked: How many times are the _____ facilities provided at your police station or jurisdiction–always, sometimes or never?

Source: Status of Police in India, 2019

42% of the personnel said that forensic technology is never available (Figure 4 above). A NITI Aayog paper by Jain and Gupta (2016) also mentions the importance of technology upgradation and states that the CCTNS system which was sanctioned in 2009 was still not fully implemented and functional across all states. Bihar and Rajasthan in particular lag in this implementation. The Comptroller and Auditor

[24] The police teeth to tail ratio, represented by comparing senior supervisory officers (Director General to Deputy Superintendent of Police) and immediate supervisory officers (Inspector to Assistant Sub-Inspector) with field personnel (Head Constable and Constable) for sanctioned strength of total police forces is 1:17:96 in 2019.

General's performance audit reviews of the modernisation of police show that the Police Telecommunications Network (PolNet) is still not properly functional. Effective use of FRTs, therefore, is a pipe dream if the police are not equipped with basic technological instruments to do its daily job.

6.2.2 Accountability of police and the role of Police Complaints Authority

Institutional checks and balances will play an important role in reigning in the discriminatory use of power. 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. The state-level PCA is empowered to look into complaints relating to death, grievous hurt and rape in custody filed against police officers of the rank of Superintendent of Police and above. In addition to these complaints, the district-level PCA is empowered to look into complaints of extortion, land/house grabbing and abuse of authority for officers up to the rank of Deputy Superintendent of Police.

Presently, 15 states and seven union territories have operational PCAs, according to a study conducted by Commonwealth Human Rights Initiative (CHRI), but only six states have them at both state and district levels. Another implementation issue has been with respect to the constitution of an independent panel to appoint the five PCA members. PCA membership includes a retired police officer from another state cadre, a member with 10 years of experience in the judiciary, a member representing civil society, and one officer with experience in public administration from another state. At least one of the members is to be a woman and not more than one member must be a retired police officer. The selection of these members is to be done by an independent panel. However, all 22 states and union territories have selected members to the PCA without setting up an independent panel (Venkatesan and Mathew, 2019). PCA operations are also marred with inefficiencies, according to the CHRI study. The study identifies the need for investigation staff, training and other resources for optimising the PCAs' oversight and accountability measures.

Setting up PCAs in the remaining states and taking measures to improve their functioning before large-scale deployment of FRTs is crucial—especially given past instances of ad hoc procedures, discrimination and inherent limitations with respect to accuracy and effectivness.

6.2.3 Regulation and independent oversight boards

Regulating and setting up independent oversight boards will require answering questions around how data is captured, how it is processed, how it is stored, how long it will be stored, what are the purposes for which it will be used, who will have access to it, safeguards to be put in place, role of the body in conducting impact evaluations of FRT and ensuring transparency of process. There are two factors that will play a key role here:

1. **Role of PDP Bill:** Separately, the PDP Bill 2019 does take cognisance of the need to have transparency and accountability measures. To this end, it prescribes constituting a 'Data Protection Authority' as a regulator to prevent misuse of personal data. Such an authority is to be constituted by the Central government upon the recommendation of a selection committee. Under the draft version of the Bill, submitted by the Srikrishna Committee in 2018, this selection committee consisted of: 1) Chief Justice of India or a judge of the Supreme Court nominated by him; 2) the cabinet secretary and 3) a reputed expert suggested by 1 and 2.

However, the 2019 Bill tabled before the Parliament amended this composition to include: 1) cabinet secretary; b) secretary to the Government of India in ministry dealing with legal affairs; c) secretary to the Government of India in ministry dealing with electronics and information technology. The revised composition is dominated by the executive compared to the earlier diverse composition comprising judicial, executive and expert members. Independent oversight in this context should involve some form of body that assesses the various principles—for example, the ones laid down by *Puttaswamy.*

2. **Regulatory independence:** The other important aspect to consider is the regulatory independence of this body. Take Aadhaar, for instance. Unique Identification Authority of India (UIDAI) is an example of a hybrid authority with the role of regulator and custodian of the database. It does not have the authority to decide which public services the Aadhaar database can be used for, nor the independence to freeze authentication when it feels it is unsafe. It merely acts as a data custodian that has failed to address public grievances (Padmanaban and Rastogi, 2019). Likewise, if the body created for FRTs is not independent, it will fail to build public trust in the technology and by extension the police. Means of grievance redressal are perhaps paramount for public trust when it comes to new technologies.

The incorporation of citizen oversight boards would be helpful in ensuring certain checks and balances through public pressure. The architects of the Constitution of India envisioned its citizens to be the real source of authority. Establishing this authority in the context of surveillance would contribute to public trust. Community control over police surveillance has been adopted by some cities in the US. Cambridge, for example, requires local police officers to seek the City Council's approval before surveillance technology is acquired, funded or used. This model also requires surveillance authorities to report on the data capabilities, storage and protection. Further, it requires authorities to report on how adverse impacts on civil rights and civil liberties will be prevented.

Conclusion

The use of FRTs may help the Indian government improve its core capabilities on policing, but there are legitimate concerns around it. The COVID-19 experience may well hasten deployment that does not take on board the issues with such technologies. We have delineated two such issues with FRT deployment in India in this paper. First, issues with the technology itself, and second, an institutional structure of policing that is poorly equipped to use FRTs to best effect. Thus, it is imperative for the government to take a step back and implement a few measures that can build robustness in the system to handle such technologies.

It must be noted that the legislative and legal framework is continuously evolving in India. Thus, deployment of these technologies, in any form, should be undertaken in a modular manner so as to easily make changes to the processes when the requisite laws are passed.

There are other important factors which were out of scope of this paper such as state-police relationships and political pressures which directly affect adoption and use of such technologies. We also think there are plenty of these discussions already being undertaken in different jurisdictions around the world and it may be useful to look at their nature to inform the laws and legislations in India. Both of these would be imperative in informing future research, bridging the knowledge gap.

Our solutions of intermediate measures and long-term measures were meant to codify a sequencing of reforms within the police so as to enable them to make use of facial recognition technologies in a responsible manner.

References

Agrawal, A., 2020. *Issues Around Surveillance In The Personal Data Protection Bill, 2019 | Medianama. [online] MediaNama.* Available at: <https://www.medianama.com/2020/01/223-nama-issues-surveillance-personal-data-protection-bill-2019/>.

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>.

Aristeidis, T., Cristina, C., Beatriz, G. and Enrique, C., 2019. *Bio-Inspired Presentation Attack Detection For Face Biometrics.* [online] Available at: <https://www.frontiersin.org/article/10.3389/fncom.2019.00034> [Accessed 23 July 2020].

Article 29 Data Protection Working Party, 2013. *Opinion 03/2013 on purpose limitation.* [online] Available at: <https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2013/wp203_en.pdf>

Ashby, M.P.J. The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis. Eur J Crim Policy Res 23, 441–459 (2017). https://doi.org/10.1007/s10610-017-9341-6

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., 2020. *NCRB Released Revised RFP For AFRS, Scraps CCTV Use.* [online] MediaNama. Available at: <https://www.medianama.com/2020/07/223-afrs-revised-tender-ncrb/>.

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/>.

Barik, S., 2020. 'Every Inch Of Telangana Will Be Under Surveillance,' Says State Government. [online] MediaNama. Available at: <https://www.medianama.com/2020/02/223-telangana-police-control-centre/>.

Barik, S., 2020. *NCRB drops CCTV integration clause from updated facial recognition tender, eases bid qualification criteria for vendors.* [online] MediaNama. Available at: <https://www.medianama.com/2020/07/223-afrs-revised-tender-ncrb/>.

Bedi, A., 2020. Geo-Mapping, CCTV Cameras, AI — How Telangana Police Is Using Tech To Enforce Covid Safety. [online] Available at: <https://theprint.in/india/geo-mapping-cctv-cameras-ai-how-telangana-police-is-using-tech-to-enforce-covid-safety/433856/>.

Bhandari V., Parsheera S., and Rahman F., 2018. *India's communication surveillance through the Puttaswamy lens.* [online] Available at: <https://blog.theleapjournal.org/2018/05/indias-communication-surveillance.html>.

Bhatnagar, A. and Shekhawat, M., 2020. *The Nuances Of Search And Seizure Of Electronic Evidence: What Are The Components Involved?.* [online] The Criminal Law Blog. Available at: <https://criminallawstudiesnluj.wordpress.com/2020/05/15/the-nuances-of-search-and-seizure-of-electronic-evidence-what-are-the-components-involved/>.

bprd.nic.in. 2017. [online] Available at:
<https://bprd.nic.in/WriteReadData/userfiles/file/databook2017.pdf>.

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

Bureau of Police Research and Development. Functions, Roles and Duties of Police in General. Available at: <https://bprd.nic.in/WriteReadData/userfiles/file/6798203243-Volume%202.pdf>

Buolamwini, J. and Gebru, T., 2018. *Gender Shades: Intersectional Accuracy Disparities In Commercial Gender Classification.* [online] gendershades.org. Available at: <http://gendershades.org/overview.html>.

Carlaw, S., 2020. *Impact On Biometrics Of Covid-19.* [online] https://www.sciencedirect.com/. Available at: <https://www.sciencedirect.com/science/article/pii/S0969476520300503>.

Castelluccia, C., Inria, D., Impact Analysis of Facial Recognition: Towards a Rigorous Methodology. 2020. ffhal-02480647f

Centre for Data Ethics and Innovation, 2020. *Snapshot Series: Facial Recognition Technology.* [online]. Available at: <https://www.politico.eu/wp-content/uploads/2020/05/Snapshot-Paper-Facial-Recognition-Technology.pdf>.

Champion, G., 2020. *CCTV And The GDPR – An Overview For Small Businesses - IT Governance UK Blog.* [online] IT Governance UK Blog. Available at: <https://www.itgovernance.co.uk/blog/cctv-and-the-gdpr-an-overview-for-small-businesses>.

Chaturvedi, A., 2017. Police Reforms In India. [online] PRS India. Available at:
<https://www.prsindia.org/policy/discussion-papers/police-reforms-india>.

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>.

Bureau of Police Research and Development, 2019. Data on Police Organisations.
<Available at: https://bprd.nic.in/WriteReadData/userfiles/file/202001301028101694907BPRDData 2019-19forweb-2.pdf>

DCAF Parliamentary Brief. *Safeguards in Electronic Surveillance.* [online] The Geneva Centre for the Democratic Control of Armed Forces (DCAF). Available at: <https://www.dcaf.ch/sites/default /files/publications/documents/Safeguards%20in%20Electronic%20Surveillance.pdf>.

Deepthi, B., 2020. *Authority Of Police To Search And Seize Under Crpc.* [online] Lawsisto.com. Available at: <https://lawsisto.com/legalnewsread/NDc0MA==/AUTHORITY-OF-POLICE-TO-SEARCH-AND-SEIZE-UNDER-CRPC>.

Deng, J. & Zafeririou,S, "ArcFace for Disguised Face Recognition," *2019 IEEE/CVF International Conference on Computer Vision Workshop (ICCVW)*, Seoul, Korea (South), 2019, pp. 485-493, doi: 10.1109/ICCVW.2019.00061.

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>.

dst.gov.in. 2020. *TDB Approves Technologies To Augment India's Efforts To Combat COVID 19* | Department Of Science & Technology. [online] Available at: <https://dst.gov.in/tdb-approves-technologies-augment-indias-efforts-combat-covid-19>.

Dudhwala F., 2020. *Facial recognition technology: A guide for the dazed and confused.* [online] Centre for Data Ethics and Innovation Blog. Available at: <https://cdei.blog.gov.uk/2020/06/01/facial-recognition-technology-a-guide-for-the-dazed-and-confused/>.

FBI Should Better Ensure Privacy and Accuracy. 2016. *Www.Gao.Gov.* [online] Available at: <https://perma.cc/ZA46-B3CG>.

ft.com. 2020. *How China Built Facial Recognition For People Wearing Masks.* [online] Available at: <https://www.ft.com/content/42415608-340c-4c0a-8c93-f22cdd4cc2d6>.

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>.

Garvie, C., Bedoya, A., and Frankle, J., 2016. *Unregulated Police Face Recognition In America. The Perpetual Line-up*. Available At: https://www.perpetuallineup.org/appendix/model-police-use-policy

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>.

Ghosh, I., 2020. *Mapped: The State Of Facial Recognition Around The World.* [online] Visual Capitalist. Available at: <https://www.visualcapitalist.com/facial-recognition-world-map/>.

Gras, M., 2004. *The Legal Regulation Of CCTV In Europe.* [online] Semantic Scholar. Available at: <https://pdfs.semanticscholar.org/f221/9331991593f259f7e11927d6809c0b8157c1.pdf>.

Grother, P., Ngan, M. and Hanaoka, K., 2020. [ebook] National Institute of Standards and Technology. Available at: <https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf>.

Hamann K., and Smith R., 2019. *Facial Recognition Technology: Where Will It Take Us?.* [online] American Bar Association. Available at: <https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/#:~:text=FRT%20has%20been%20used%20for,and%20terrorists%20from%20the%20event.>.

Harmon, A., 2019. *As Cameras Track Detroit'S Residents, A Debate Ensues Over Racial Bias.* [online] Nytimes.com. Available at: <https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html>.

Introna, L. and Nissenbaum, H., 2010. *Facial Recognition Technology A Survey Of Policy And Implementation Issues.* [online] Available at: <https://nissenbaum.tech.cornell.edu/papers/facial_recognition_report.pdf>.

India Today. 2020. Amit Shah on Delhi riots probe: 1100 people identified using face recognition tech, 300 came from UP. Available at: <https://www.indiatoday.in/india/story/face-identification-technique-amit-shah-on-delhi-riots-probe-1654523-2020-03-11>

Jain, A., 2020. *Problems With Facial Recognition Systems Operating In A Legal Vacuum.* [online] Internet Freedom Foundation. Available at: <https://internetfreedom.in/problems-with-facial-recognition-systems-operating-in-a-legal-vacuum/>.

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>.

Joy, S., 2020. *Majority Prisoners In Indian Jails Are Dalits, Muslims.* [online] Deccan Herald. Available at: <https://www.deccanherald.com/national/north-and-central/majority-prisoners-in-indian-jails-are-dalits-muslims-790478.html>.

keralaservice.org. 1969. *The Kerala Police Manual.* [online] Available at: <https://www.keralaservice.org/download/send/7-departmental-text-books/82-kerala-police-manual-1969-vol-i>.

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>.

Lawfilesext.leg.wa.gov. 2020. *Engrossed Substitute Senate Bill 6280.* [online] Available at: <http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Passed%20Legislature/6280-S.PL.pdf>.

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. *Why Police in India Use 'Third-Degree' Torture Methods for Interrogation.* The Wire. [online] Available at <https://thewire.in/books/police-torture-interrogation-jinee-lokaneeta-excerpt>

mahapolice.gov.in. 1959. *The Bombay Police Manual.* [online] Available at: <http://mahapolice.gov.in/files/acts_rules/69.pdf>.

Mara, P. and Deshpande, D., 2020. *Public Procurement 2020 | Procurement Rules And Trends In India | ICLG.* [online] International Comparative Legal Guides International Business Reports. Available at: <https://iclg.com/practice-areas/public-procurement-laws-and-regulations/2-procurement-rules-and-trends-in-india>.

Marda, V., 2019. *Indian Govt'S Approach To Facial Recognition Is Flawed & Driven By Faulty Assumptions.* [online] ThePrint. Available at: <https://theprint.in/opinion/indian-govt-approach-to-facial-recognition-flawed-driven-by-faulty-assumptions/327036/>.

Mathias, S. and Kazia, N., 2016. *Collection, Storage And Transfer Of Data In India.* [online] Lexology.com. Available at: <https://www.lexology.com/library/detail.aspx?g=00e56cb6-b0ea-46b7-ab1b-1d52de3646d0>.

Mathur, N. and Ahaskar, A., 2020. *Offices Ditch Fingers For Facial Recognition Tech.* [online] Livemint. Available at: <https://www.livemint.com/news/india/covid-19-impact-india-inc-switches-to-facial-recognition-for-staff-attendance-11585455083718.html>.

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

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/>.

meity.gov.in. 2011. [online] Available at: <https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf>.

mha.gov.in. 2015. [online] Available at: <https://www.mha.gov.in/MHA1/Par2017/pdfs/par2015-pdfs/rs-120815/2593.pdf>.

Mint. 2019. The new crime buster: Tracking gait technology. Available at: https://www.livemint.com/technology/tech-news/the-new-crime-buster-tracking-gait-technology-1549210184513.html

Mohamed, M.A., Abou-Elsoud, M.E., Eid, M.M., 2011. *Automated face recognition system: Multi-input databases.* International Conference on Computer Engineering & Systems (ICCES). Available at: https://www.researchgate.net/publication/239764744_Automated_face_recogntion_system_Multi-input_databases

Murugan, S., Dr. (2018, April 2). *Electronic Evidence: Collection, Preservation and Appreciation (Chennai, India, Vigilance and Anti Corruption, Tamil Nadu Police).* [online] Available at: http://www.nja.nic.in/Concluded_Programmes/2017-18/P-1077_PPTs/4.Electronic Evidence- Collection, Preservation and Appreciation.pdf

Nagpal, S., Singh, M., Singh, R., Vatsa, M. and Ratha, N. "Deep learning for face recognition: Pride or prejudiced?" arXiv preprint arXiv:1904.01219, June 2019

National Herald. 2020. *How Foolproof Is Amit Shah'S Facial Recognition Technology? IFF Raises Questions.* [online] Available at: <https://www.nationalheraldindia.com/india/how-foolproof-is-amit-shahs-facial-recognition-technology-iff-raises-questions>.

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/>.

Padmanabhan, A., and Rastogi, A., 2019. *Big Data.*

Paliwala, M., 2019. *Law of Evidence: An Overview of Different Kinds of Evidence* [online]. blog.ipleaders.in. Available at: <https://blog.ipleaders.in/different-kinds-of-evidence/>

Paliwala, M., 2019. *Search, Seizure and Production of Materials Under Criminal Law* [online]. blog.ipleaders.in. Available at: <https://blog.ipleaders.in/search-seizure-production-of-materials-under-criminal-law/#Search_by_a_police_officer_during_the_investigation>

Parsheera, S., 2020. *Facial Recognition Technologies In India: Why We Should Be Concerned.* [online] theleapjournal.org. Available at: <https://blog.theleapjournal.org/2020/01/facial-recognition-technologies-in.html>.

Peeters, B., 2020. *Facial Recognition At Brussels Airport: Face Down In The Mud. - CITIP Blog.* [online] CITIP blog. Available at: <https://www.law.kuleuven.be/citip/blog/facial-recognition-at-brussels-airport-face-down-in-the-mud/>.

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>.

Press Trust of India. 2018. *2 Percent Accuracy In Delhi Police Facial Recognition Software, Court Told.* [online] Available at: <https://www.ndtv.com/delhi-news/2-percent-accuracy-in-delhi-police-facial-recognition-software-court-told-1905242>.

Pritchett, L., Woolcock, M. and Andrews, M., 2011. *Capability Traps? The Mechanisms Of Persistent Implementation Failure.* [ebook] SSRN. Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1824519>.

Reuters, 2020. *Delhi, UP Police Use Facial Recognition Tech At Anti-CAA Protests, Others May Soon Catch Up.* [online] India Today. Available at: <https://www.indiatoday.in/india/story/delhi-up-police-use-facial-recognition-tech-at-anti-caa-protests-others-may-soon-catch-up-1647470-2020-02-18>.

Reuters, 2020. Even mask-wearers can be ID'd, China facial recognition firm says. Available at:<https://uk.reuters.com/article/us-health-coronavirus-facial-recognition/even-mask-wearers-can-be-idd-china-facial-recognition-firm-says-idUKKBN20W0WL>

Satish, M., 2011. *"Bad Characters, History Sheeters, Budding Goondas And Rowdies": Police Surveillance Files And Intelligence Databases In India.* [online] Manupatra. Available at: <http://docs.manupatra.in/newsline/articles/Upload/B06B8036-FE1B-42C0-AF68-0BF08990BF3E.pdf>.

Saxena, A., 2016. *India: More Than Half Of Undertrials Are Dalits, Muslims And Tribals.* [online] Aljazeera.com. Available at: <https://www.aljazeera.com/blogs/asia/2016/11/trial-india-dalits-muslims-tribals-161101150136542.html>].

Shah, A., 2009. *Naz Foundation Vs Government Of Nct Of Delhi.* [online] Indiankanoon.org. Available at: <https://indiankanoon.org/doc/100472805/>.

Shekhar, S., 2016. *Cops Part Of Nexus Stealing Call Records.* [online] India Today. Available at: <https://www.indiatoday.in/mail-today/story/delhi-police-call-records-snooping-328345-2016-07-10>.

Singer, N., 2020. *Amazon Is Pushing Facial Technology That A Study Says Could Be Biased.* [online] Nytimes.com. Available at: <https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html?module=inline>.

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.

Singh, M., Chawla, M., Singh, R., Vatsa, M., and Chellappa, R., 2019. *Disguised faces in the wild 2019.* Available at: https://openaccess.thecvf.com/content_ICCVW_2019/papers/DFW/Singh_Disguised_Faces_in_the_Wild_2019_ICCVW_2019_paper.pdf

Singh, J., 2020. *AI-Based Solution Amongst 6 COVID-19 Projects Receive Government Support.* [online] NDTV Gadgets 360. Available at: <https://gadgets.ndtv.com/science/news/technology-development-board-covid-19-coronavirus-tech-projects-approval-facial-recognition-2232056>.

South Western Railways, 2020. [online] Available at: <https://swr.indianrailways.gov.in/view_detail.jsp?lang=0&dcd=3370&id=0,4,268>.

Special Police Unit for Women & Children. *Electronic Evidence.* [online] Available at: <http://spuwac.com/index.php?option=com_content&view=article&id=72:electronic-evidence&catid=11:faqs&Itemid=93>.

Spuwac.com. n.d. *Electronic Evidence. [*online] Available at: <http://spuwac.com/index.php?option=com_content&view=article&id=72:electronic-evidence&catid=11:faqs&Itemid=93>

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>.

Status of Policing in India Report 2019, Common Cause & Lokniti – Centre for the Study Developing Societies. [online] Available at: <https://www.commoncause.in/uploadimage/page/Status_of_Policing_in_India_Report_2019_by_Common_Cause_and_CSDS.pdf>

Sur, A., 2020. *Facial Recognition Tech To Be The New Normal.* [online] The New Indian Express. Available at: <https://www.newindianexpress.com/cities/hyderabad/2020/apr/30/facial-recognition-tech-to-be-the-new-normal-2137146.html>.

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/>.

The New York Times. 2020. How the Police Use Facial Recognition, and Where It Falls Short. Available at: https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html

Thorat, S., Nayak, S. and Dandale, J., 2010. *Facial Recognition Technology: An Analysis With Scope In India.* [online] Arxiv.org. Available at: <https://arxiv.org/pdf/1005.4263.pdf>.

Tripathi, S., 2020. *UP Police'S Drone Surveillance: A Step Towards 'Orwellian' State?.* [online] TheQuint. Available at: <https://www.thequint.com/voices/opinion/uttar-pradesh-police-drone-surveillance-of-houses-right-to-privacy-security-law-constitution>.

Using Biometrics For Border Security. [online] Available at: <https://perma.cc/T9PL-KBBY>.

US Government Accountability Office. 2016. Face Recognition Technology: Fbi Should Better Ensure Privacy And Accuracy. Available at: <Https://Perma.Cc/Za46-b3cg>

US Government Accountability Office. 2002. Technology Assessment: Using Biometrics For Border Security. Available at: <Https://Perma.Cc/T9pl-kbby>

Vellon M., 2017. *12 Factors To Help You Evaluate Potential Technical Solutions.* [online] Forbes Technology Council. Available at: <https://www.forbes.com/sites/forbestechcouncil/2017/02/09/12-factors-to-help-you-evaluate-potential-technical-solutions/#5b1171f14f66>.

Venkatesan, V. and Mathew, S., 2019. *Police Reforms Still Largely Only On Paper.* [online] Frontline. Available at: <https://frontline.thehindu.com/dispatches/article28960801.ece>.

Von Grafenstein, M. (2018). *The Principle of Purpose Limitation in Data Protection Laws: The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation.* [online] Available at: <www.jstor.org/stable/j.ctv941v5w>.

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>

Wood, M., 2018. *Thoughts On Machine Learning Accuracy.* [online] AWS News Blog. Available at: <https://aws.amazon.com/blogs/aws/thoughts-on-machine-learning-accuracy/>

www3.weforum.org. 2020. *A Framework For Responsible Limits On Facial Recognition Use Case: Flow Management.* [online] Available at: <http://www3.weforum.org/docs/WEF_Framework_for_action_Facial_recognition_2020.pdf>.

Xynou, M., 2015. *Policy Recommendations For Surveillance Law In India And An Analysis Of Legal Provisions On Surveillance In India And The Necessary & Proportionate Principles.* [online] Cis-india.org. Available at: <https://cis-india.org/internet-governance/blog/policy-recommendations-for-surveillance-law-in-india-and-analysis-of-legal-provisions-on-surveillance-in-india-and-the-necessary-and-proportionate-principles.pdf>.

Yang, Y., 2020. *How China built facial recognition for people wearing masks.* [online] Financial Times. Available at <https://www.ft.com/content/42415608-340c-4c0a-8c93-f22cdd4cc2d6>

Yeung D., Balebako R., Gutierrez C. I., Chaykowsky M., 2020. *Face Recognition Technologies: Designing Systems that Protect Privacy and Prevent Bias.* [online] Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR4200/RR4226/RAND_RR4226.pdf

Acknowledgements

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 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.

datagovernance.org dgn@idfcinstitute.org

@datagovnetwork /datagovnetwork /datagovnetwork