Data Governance Network

November 2019

Working Paper 05

Adoption and regulation of facial recognition technologies in India: *Why and why not?*

Smriti Parsheera

NIPFP
National Institute
of Public Finance
and Policy

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

The National Institute of Public Finance and Policy (NIPFP) is a centre for research in public economics and policies. Founded in 1976, the institute undertakes research, policy advocacy and capacity building in a number of areas, including technology policy. Our work in this space has involved providing research and policy support to government agencies and contributing to the creation and dissemination of public knowledge in this field. Our current topics of interest include privacy and surveillance reform; digital identity; Internet governance and rights, and regulation of emerging technologies. We also focus on research that lies at the intersection of technology policy, regulatory governance and competition policy.

Disclaimer and Terms of Use

The analysis in this paper is based on research by the National Institute of Public Finance and Policy. The views expressed in this paper are not that of the National Institute of Public Finance and Policy or IDFC Limited or any of its affiliates.

Cover page credit: Cactus Communications

Paper design: Cactus Communications

Suggested Citation

Parsheera, S. (2019). *Adoption and regulation of facial recognition technologies in India: Why and why not?*. Data Governance Network Working Paper 05.

Supported by a grant from Omidyar Network

Abstract

The widespread adoption of facial recognition technologies by the public and private sectors, without any meaningful debate or regulation, raises a number of concerns. These concerns revolve around issues of transparency, privacy and civil liberties, accuracy and effectiveness, and evidence of biased outcomes. This paper outlines the various contexts in which the use of this technology is being discussed in India and the challenges that it presents on account of the lack of an informed policy debate and appropriate legal and procedural safeguards. It focuses, in particular, on the proposed National Automated Facial Recognition System and the many ways in which it falls short of satisfying the tests laid down by the Supreme Court in the *Puttaswamy* right to privacy case.

Table of Contents

1. Introduction

The march of technology has enabled us to do things at a scale, and with a level of efficiency, that might have seemed unfathomable until a few years ago. Access to millions of search results at our fingertips, sophisticated cameras in our mobile phones and virtually unlimited cloud storage space, are some of the many examples. The lived reality of these technological successes makes it easy to imagine that every challenge that we currently face can ultimately be solved with the right technological innovation, one that is just waiting to be discovered. However, this sort of "technological solutionism" comes with its own set of perils.

As observed by Evgeny Morozov, technology can indeed be a force of improvement but only if we are willing to "*genuinely interrogate what we are doing with it and what it is doing to us*" (Morozov, 2013). This paper seeks to explore these questions in the context of the adoption and regulation of facial recognition technologies (FRTs) in India.

FRTs refers to a set of technological tools that can be used for identifying or verifying human beings from photographs, videos or in real time. In the Handbook of Face Recognition Technology, Li and Jain (2011) note that face recognition has several advantages over other biometric identification techniques, such as fingerprint and iris scans – *"besides being natural and nonintrusive, the most important advantage of face is that it can be captured at a distance and in a covert manner"*. However, this also the exact reason why biometric data, in general, and facial data, in particular, poses unique and far-reaching challenges for the privacy of individuals and societies.

Research on FRTs has been going on for several decades, but recent advances in computer vision and machine learning have given it a new lease of life. Everyday uses of the technology include photo tagging suggestions on social media, biometric unlocking of mobile phones and photo filters on popular mobile apps. Then there are the slightly more "innovative" applications, such as the use of FRTs for monitoring the consumption of toilet paper in China's public restrooms (Lin, 2019); tracking attendance of congregates at churches (Pearson, 2015); and diagnosis of congenital and neuro-developmental disorders based on distinctive facial features (Dolgin, 2019).

The most pervasive, and worrying, use of FRTs, however, comes up in the context of its increasing deployment by government agencies, particularly for surveillance and law enforcement purposes. Evidence from around the world indicates that both democratic states as well as authoritarian regimes are equally drawn to the massive surveillance potential of FRTs. As per the AI Global Surveillance Index released by the Carnegie Endowment for International Peace, 85 percent of the countries that they studied (64 out of 75) were making use of facial recognition systems for surveillance purposes (Feldstein, 2019).[1]

In India, the National Crime Records Bureau (NCRB) recently invited bids for the creation of a National Automated Face Recognition System (NAFRS). This is meant to be a technological solution to facilitate criminal identification and verification by the police. This comes on top of existing accounts about the use of FRTs in cities like Chennai, Amritsar, Surat and Hyderabad for matching real-time closed circuit television (CCTV) footage with criminal databases and analysing facial data captured through smart glasses (Murali, 2018). In addition to the law enforcement related applications, other contexts in which FRTs are being talked about in India include biometric authentication though Aadhaar, attendance in schools and colleges, and check-in processes at airports.

The rapid deployment of FRTs, without accompanying guidelines or legal frameworks, raises a number of questions. These concerns revolve around the lack of transparency around facial recognition systems; their implications for privacy and civil liberties; and evidence of bias and discrimination in their outcomes. Equally, we also need to the question the accuracy and effectiveness of facial recognition systems. Namely, their ability to achieve what they claim to do, and their suitability for the specific context in which the technology is sought to be deployed. While all these concerns hold true for the use of FRTs by the government as well as private entities, the imbalance of power between the citizen and the state and the likely consequences from the abuse of that power make this a particularly worrying problem in the context of law enforcement uses.

[1] The index uses a four-part scheme to classify countries based on their political regimes. The four categories along with some examples are as follows – *Closed Autocracy* (Bahrain, China and Saudi Arabia); *Electoral Autocracy* (Algeria, Egypt and Mayalsia); *Electoral Democracy* (Argentina, India and Netherlands); and *Liberal Democracy* (Australia, Mexico, the United Kingdom (UK) and the United States of America (USA)).

With further advancements in the technology and the discovery of newer use-cases, the adoption of FRTs can only be expected to rise further. At the same time, increasing adoption will also exacerbate many of the concerns. The challenge therefore lies in being able to assess the tradeoffs between the drawbacks and advantages of adopting FRTs in different contexts. This sort of thinking is necessary for assessing whether, and under what circumstances, should this technology be adopted.

Drawing from this background, the rest of the paper is organised as follows. In the first section we explain the meaning of FRTs, the key developments that have contributed to its growth in recent years, and some of the main functions and use cases. This is followed, in the second section, by an identification of some of the prominent use cases that are being discussed in the Indian context. Next, we explore the main challenges posed by FRTs, highlighting issues of transparency, threats to civil liberties, accuracy and reliability, bias and discrimination and challenges of the overall ecosystem in which the technology is sought to be placed. The fourth section contains a discussion about the potential models of regulation and the roles and incentives of different stakeholders in that process. This is followed, in the fifth chapter, by more specific discussions around the principles that should guide the use of FRTs by law enforcement agencies, with a focus on the proposed NAFRS project in India. The last section concludes.

2. What are facial recognition technologies?

Automated facial recognition is a form of biometric analysis that allows for the identification or verification of an individual based on patterns derived from their facial characteristics and features. While there are a range of facial recognition techniques, prevalent models rely on using an image to create a mathematical representation of a person's face, which can then be compared against the representations captured in an existing database or gallery of photographs to find likely matches (Moosa, 2019; Introna & Nissenbaum, 2010).

In the following section we explain the difference between the processes of 'verification' and 'identification' using FRTs. We then go on to discuss another type of categorisation, based on whether or not the application of the FRTs system is taking place in a cooperative setting.

2.1. Classification of FRTs

The first step in any facial recognition system is that of *detection* of a human face in an image. In fact, there are several use cases where facial detection can serve as an end in itself, without the need for identifying specific individuals. Examples of this include auto focus function of a camera or online tools for trying virtual makeup or eyeglasses (Future of Privacy Forum, 2018). The detection process is followed by *feature extraction,* to pick out the specific features that define a person's face and distinguish it from that of others. This may include features like the length of the jaw line, spacing between the eyes, dimensions of the nose, mouth and ears, etc (Raj & Niar, 2017).

Finally, there is the step of *recognition,* which results in the verification or identification of an individual (Lu, Zhou, & Yu, 2003). Also referred to as *1:1 verification* and *1:many* identification, the former seeks to test whether a person is who she claims to be while the latter tries to identify a specific person from a pool of unknown persons (Future of Privacy Forum, 2018).

Introna and Nissenbaum (2010) explain that the verification function is often used in situations where an individual already has a relationship with the institution conducting the probe due to which her credentials are already in the system. Matching a person against an image corresponding to their identification number in a company's employment database or dataset of students enrolled in an educational institution, are some examples. 1:many identification, on the other hand, is more complicated and also more prone to errors, given the larger set of unknowns in the system. For instance, trying to identify a person based on CCTV footage is complicated because of the conditions in which such images are captured as well as the uncertainty regarding whether that person is actually present in the database that is being used for matching.

Another logic that can be used for classifying FRTs is based on the extent to which the person on whom the technology is being applied co-operates with the deployment process (Li & Jain, 2011). The attendance example referred to above relates to a *co-operative user scenario* where the students or employees can typically be expected to co-operate with the institution both at the time of capturing their images for creating the gallery database as well as subsequent matching of their face against that database. In contrast, the process of identifying suspected criminals using CCTV footage is most likely to occur in a *non-cooperative user scenario*, where the person is not directly facing the camera and the lighting, angle, etc. are also uncontrolled.

As per facial recognition scientists, the problem of 1:1 verification using FRTs in a cooperative setting is a "*reasonably well-solved problem*". In fact they assert that automated face recognition surpasses the performance of human recognition in "*constrained situations*", where factors like lighting, pose, facial wear, facial expression, etc., can be controlled for (Li & Jain, 2011). However, as we discuss in the subsequent sections, the real world application of FRTs go much beyond situations of controlled environments and the resulting implications go much beyond the concerns of inaccurate results.

Before venturing into a more detailed exploration of these issues, we discuss some of the key developments that have contributed to the advances in FRTs, and which make this an opportune moment to discuss the adoption and regulation of this technology.

2.2. Why discuss this now?

While research on face recognition has been going on for several decades, there has been a significant spike in interest around FRTs in the last few years. This holds true for research, development and adoption of the technology as well as academic and policy debates highlighting the concerns around its usage.

The growing popularity of this field is illustrated by the increasing number of use cases; emergence of multiple academic and research conferences on the subject and the availability of reliable tools for systematic evaluation of the technology (Lu et al., 2003).[2] Increase in

[2] For instance, the National Institute of Standards and Technology (NIST) in the United States has created an open system for measuring the performance of facial recognition algorithms using parameters such as accuracy, speed, memory consumption, and resilience (NIST, 2019).

the number of patents for FRTs in the last few years is another useful indicator.[3] All of these developments have contributed to, or perhaps been fueled by, greater commercial interest in the technology and increased adoption by government agencies.

At the same time, concerns around the unchecked use of FRTs are also growing. Visuals of protesters in Hong Kong taking down smart lamp posts and surveillance cameras, while having their faces covered by masks and umbrellas, are symbolic of the growing resistance towards state surveillance through FRTs. This push back against FRTs is supported by a rich body of work from researchers, civil society organisations as well as some technology companies highlighting the need for appropriate regulatory and oversight mechanisms in this field. We discuss these perspectives in subsequent sections of the paper.

Following are some of the infrastructural pillars that have enabled the increased research in, and adoption of, FRTs.

1. **Availability of digital images**

   A facial recognition system basically relies on the availability of three types of data sets – the *training set* that is used to develop and train the algorithm; the *gallery set* with images of known individuals, against which the matching process is undertaken; and the *probe image,* which is sought to be recognised (Phillips & Newton, 2002). In the last decade or so we have seen a massive increase in the availability of digital facial images that can be used for each of these purposes. A part of this can be attributed to the increase in Internet penetration coupled with the rapid proliferation of cameras in devices like mobile phones.

   In 2013, Facebook announced that it had over 250 billion photos on its site, with an average of about 350 million images being added each day (Wagner, 2013). While, data of this nature is not always accessible to the public (although it could be used by Facebook for training its own systems), individual settings often allow these images to become accessible. This is also true for images available on blogs, news reports, photo hosting sites, etc., which are generally searchable through search engines.

[3] China has emerged as the global leader in patents for FRTs. By 2017, it had more than 900 published patents in facial recognition, up from about 200 in 2012 (CB Insights, 2018).

The digitisation of government processes and collection of digital images for the issuance of identification documents, like passports, voter IDs, Aadhaar cards, tax identity card, etc, has allowed for the creation of similar databases in the hands of state agencies. The images collected in these processes can sometimes also become accessible to other stakeholders through initiatives such as the Indian government's bulk data sharing policy for vehicle registration certificates and driver licenses (Ministry of Road Transport and Highways, 2019). While the policy does not specify whether the photographs of drivers are included in the shared datasets, the reference to sharing of the "complete data" indicates that this is likely to be the case.

In addition, a number of private institutions also tend to put out image datasets that can be utilised for training and testing of face recognition algorithms. There are often tailored for training algorithms under specific conditions. For instance, there are databases that offer images of the same person clicked over a period of time (Colour FERET database) or in different poses and illumination conditions (Multi-PIE database). Similarly, one can also access images sourced from uncontrolled indoor environments (SCface database) to train a facial recognition system that is meant to be deployed in such situations (Grgic & Delac, 2019).

Finally, images may also be put out in the public domain as a means of 'data philanthropy'. For instance, IBM was recently in the news for providing researchers access to a dataset of close to a million images that were put out by the photo hosting site Flickr, without the knowledge or consent of the uploaders (Solon, 2019).

2. **Widespread deployment of CCTV cameras**

Governments all over the world are actively involved in the deployment of CCTV cameras in public spaces like roads, parks, airports and railway stations. The link between increasing coverage of CCTV cameras and their current or future integration with FRTs is a crucial one. As noted by Senior and Pankanti (2011), access to automated identification systems changes the nature of the

CCTV surveillance system from a labour-intensive, manual, process to one that is conducive for effortless and ubiquitous monitoring.

CCTV footage may be used for drawing out probe images of suspected individuals or, in case of live facial recognition systems, for matching images of passersby against a designated 'watchlist'. China's Skynet project, which the state media claims to be the "world's biggest surveillance network", is an oft quoted example of a mass surveillance system using CCTV cameras (Shen, 2018). The country is now rolling out an even larger video surveillance system, which goes by the name of *"Xueliang"*, or the Sharp Eyes Project.[4] This is accompanied by requirements that authorities should promote *"modern technologies such as data mining, face recognition, license plate recognition, intelligent warning systems"* using the video surveillance systems (Rollet, 2018).[5]

Despite the frequent use of Chinese examples, evidence from the around the world shows that all sorts of government regimes, including liberal democracies, are equally charmed by the security and surveillance potential of large scale CCTV deployments. Much of this work is taking place under initiatives to build smart cities or as urban safety measures.

In Delhi, the government is currently in the process of setting up about 300,000 CCTV cameras, in addition to the 250,000 cameras already being operated by the Delhi police. One of the stated objectives of this project is to secure the safety of Delhi's "sisters and mothers" (Jeelani, 2019), i.e., to enhance public safety of women. This illustrates a problematic link between use of surveillance technologies as a tool for delivering gender justice. In reality, such technologies often end up having a disproportionate negative impact on women and other marginalised groups.[6]

[4] The project finds its origin in a 2015 mandate by the Chinese National Development and Reform Commission that by 2020 there should be no blind spots in the coverage of the country's public areas.

[5] China has also gained notoriety for the export of its surveillance technology to other countries like Mongolia, Zimbabwe and Ecuador. See Romaniuk and Burgers (2018).

[6] For instance, see Keyes (2018) for a discussion on the impact of automatic gender recognition systems on the transgender community.

In addition to the deployment by state agencies, we are also seeing increased adoption of CCTV by private users in places like shops, offices and housing complexes.[7] While data from private systems is not directly available to government agencies in the same way that their own systems are, laws in India tend to confer government agencies with very wide ranging powers of access to any available information. In Delhi, the draft rules for regulation of CCTV proposed that that every operator of a CCTV system installed in a public place must report the existence of such a system to the Delhi Police. Further, the information collected through the system would have to be made available to authorised government agencies for prevention, detection, investigation, prosecution and punishment of offences.[8]

On one hand, this sort of regulation can act as a check on the installation of undisclosed cameras in public places. On the other, it only adds to the knowledge of law enforcement agencies on data sources that they can access and use for the deployment of face recognition and other analytical tools.

3. **Computation and processing capacity**

   Running FRTs on a large scale requires significant computational and processing capabilities. The proliferation of off-the-shelf facial analytics solutions, many of which allow for convenient processing of large volumes of data at affordable rates, have made this technology more accessible to a broad range of users. Examples of some of the prominent cloud-based facial recognition tools include Amazon's Rekognition and Microsoft's Azure toolkit, which allow users to easily deploy facial recognition services on an index of face images put together by the user.

2.3. Key functions and use cases

FRTs are being adopted in a broad range of a contexts. One useful way to classify these use cases is based on the underlying functions that are sought to be performed. Given

[7] Many of these systems do not follow basic protocols like setting secure passwords, which has allowed operators like Insecam and EarthCam to create an online directory of live feeds of security cameras from around the world.

[8] Rule 4, Draft Delhi Rules for Regulation of CCTV Camera Systems in NCT of Delhi, 2018.

below is a non-exhaustive list of four main types of functions with examples of their applications (Senior & Bolle, 2002a; Huang, Xiong, & Zhang, 2011; NEC, 2019).

1. **Identification and access controls**

   This is the most basic function of a facial recognition system, where a person's face is used the basis for authenticating their identity and/or verifying whether they are entitled to access certain systems. The identification function would, for instance, include use cases like checking a person's identity for purposes like voter identification, nation ID registration, driving licenses, marking attendance, etc. The access control function builds on top of face identification to check whether a person is an authorised user for a specific purpose. The applications that pursue this function include biometric unlocking of mobile devices, guarding entry to restricted areas, authorising withdrawals from ATM machines and verifying if a person is a legitimate beneficiary of a government scheme (Senior & Bolle, 2002a).

2. **Security and surveillance**

   This function relates to the pursuit of enhanced security covering a broad range of applications, some of which may also overlap with the access control function discussed above. For instance, the use of FRTs for verification of passengers and immigration checks at airports is a form of access control that also seeks to serve the function of enhanced security.[9]

   Much of the surveillance related use of FRTs also derives its logic from the goal of providing higher security. This is based on the expectation that crime rates will reduce as potential offenders become aware that they are being watched and can easily be identified using the system. Emperical studies have, however, shown that while technologies like CCTV have helped in reducing specific types of crimes (like car thefts), there have been no observable effect in reduction of violent crimes (Piza, Welsh, Farrington, & Thomas, 2019).

[9] The Customs and Border Protection Biometric Exit Program in the United States is anticipated to have *"the ability to scan the faces of 97 percent of commercial air passengers departing the United States by 2023"* (Funk, 2019).

3. **Law enforcement**

   The main use of FRTs in the context of law enforcement relates to the ability to search and identify suspected individuals quickly, even with incomplete information about their identity (Huang et al., 2011). For instance, CCTV footage from cameras located in the vicinity of a site of crime is routinely checked to identify and trace the movements of the suspect. Similarly, cameras located at traffic signals can be used for identifying drivers who commit traffic violations. Other reported applications in the field may include searching for missing persons, checking human trafficking and detecting the use of false ID documents.

4. **Business efficiency**

   Finally, face recognition also serves a number of commercial and business efficiency related functions. This includes adoption by photo storage and sharing platforms for the tagging of individuals; ability of retail and hospitality sectors to identify their customers or dynamically generating services and content suited for their profiles (NEC, 2019). For instance, digital signage systems can calculate a gazer's age and gender and accordingly change the advertisement on the screen. Facial detection and analysis also serves as the building block for other applications like emotion or sentiment analysis which have many uses in the marketing and entertainment industries.

3. Applications in the Indian context

As in other parts of the world, there are several instances of facial recognition systems being deployed by private as well as government agencies in India. Before getting into a detailed discussion of these use cases, it is important to highlight two important factors. First, all of the current deployments of FRTs in India are taking place in the absence of a robust data protection law. While the current Information Technology Act, 2000 and the rules under it classify biometric data as "sensitive personal data", laying down conditions for its collection, disclosure and sharing, the scope and implementation of the law remains grossly inadequate. Moreover, the obligations under the present law are applicable only to “body corporates”, hence excluding most instances where government agencies interact with biometric facial data. Second, in each of the cases listed below, the adoption of FRTs, or the decision to do so, has been announced without any prior discussion or consultation about the broader implications of the projects.

Despite these serious limitations, the use of FRTs is being discussed in many contexts, including the following.

1. **National Automated Face Recognition System**

   In June, 2019, the NCRB, which is the body responsible for managing information on crime and criminals in India, issued a tender inviting bids for the setting up of the NAFRS (NCRB, 2019). Notably, the issuance of the tender document was not preceded by any public debate or consultation regarding the adoption of such a system. Further, in a right to information request filed by the Internet Freedom Foundation, the NCRB disclosed that the issuance of the tender was also not preceded by any inter-ministerial meetings or discussions.

   As per the tender document, the NAFRS is meant to be used for the identification and verification of persons using *“digital images, photos, digital sketches, video frames and video sources”*. The purposes for which it is to be deployed include identification of criminals, missing children and persons, unidentified dead bodies and unknown children and persons who have been traced but whose identity cannot be determined.

   The tender also identifies a number of sources that would be used for generating probe and gallery images. The former would, for instance, include sources like video feeds obtained from CCTV cameras installed by the police as well as by other private or public organisations. The gallery database would in turn be based on photographs from very wide range of sources, including the country’s 74 million plus passport holders (Manish, 2018); over 1.2 million persons whose ten finger prints are available with the Central Finger Print Bureau (NCRB, 2018); and more than 1,700 missing children listed on the Ministry of Women and Child

Development's tracking portal (Khoya-Paya, 2019). More importantly, the list of proposed data sources also contains a sweeping category for *"any other image database available with police / other entity"*, which implies that virtually each and every database in the country could potentially be linked with this system.

Further, the tender provides that in case of states that have already initiated their own face recognition programmes for law enforcement purposes, those systems would also be linked with the NAFRS. Reported instances of such systems include the Punjab Artificial Intelligence System, which allows photographs of suspects to be matched against pictures of convicted persons housed in jails across the state of Punjab (Sathe, 2018). Surat, Chennai, Hyderabad, Vijaywada and Mumbai are some of the other cities where law enforcement authorities are reportedly using FRTs, or have done so on specific occasions in the past (Vidyut, 2018).

2. Aadhaar authentication and KYC

The Aadhaar enrollment process has ensured that the government already has a database with the photographs of over 1.2 billion individuals. The purposes for which this information may be used is regulated by the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (Aadhaar Act). While identifying these purposes, the Aadhaar Act draws a distinction between the treatment of "biometric information" and "core biometric information", with photographs being included in the former category.[10]

The law affords a higher degree of protection to core biometric information (fingerprints and iris scans) by restricting it from being shared with any person or used for any purpose other than generation of Aadhaar and authentication under the Aadhaar Act.[11] Photographs and demographic information, on the other hand, are permitted to be shared in accordance with the law, which would include purposes like e-know your customer (KYC) and now offline

[10] Core biometric information is defined in Section 2(j) of the Aadhaar Act to mean finger print, Iris scan, or such other biological attribute of an individual as may be specified by regulations.

[11] Section 29(1), Aadhaar Act.

Aadhaar verification.[12] The original version of the Aadhaar Act also laid down a restriction on publicly displaying or publishing a person's Aadhaar number or their core biometric information. The recent 2019 amendments to the Aadhaar Act have, however, replaced the reference to "core biometrics" with "demographic information or photograph". Accordingly, it is no longer permissible to create a public database of the photographs that are collected in connection with the enrollment, authentication or verification processes under the Aadhaar Act.

In January, 2018, the Unique Identification Authority of India (UIDAI) had announced that it would allow the use of facial recognition as one of the modes of authentication under the Aadhaar Act. This decision came at the height of the challenge before the Supreme Court regarding the constitutional validity of Aadhaar, on grounds that included privacy concerns as well as exclusion of legitimate beneficiaries. The notification stated that the use of FRTs in Aadhaar was meant to allow for "inclusive authentication" as several residents who had enrolled for Aadhaar were facing difficulties in completing the authentication using fingerprints and iris scans (UIDAI, 2018).[13] Through subsequent circulars the UIDAI mandated telecom service providers to start undertaking face authentication of their subscribers.[14]

The Supreme Court's verdict in the *Puttaswamy* Aadhaar case[15] and the subsequent amendments to the Aadhaar Act, have however drawn a distinction between the use of Aadhaar authentication for the delivery of government welfare benefits and other purposes such as KYC verifications. Pursuant to these developments, it is no longer possible to mandate face authentication for KYC processes conducted by

[12] The concept of offline verification was introduced through the Aadhaar and Other Laws (Amendment) Ordinance, 2019 that was in effect from March–July, 2019. It has now been replaced by the Aadhaar and Other Laws (Amendment) Bill, 2019 that has been approved by both houses of Parliament.

[13] Response to Lok Sabha Unstarred Question No. 857, To be answered on 7 February 2018. This response also stated that various security aspects used in the authentication ecosystem, like encryption, use of registered devices, biometric locking / unlocking, etc., would also be applicable to face authentication.

[14] UIDAI, Implementation of face authentication, Circular No. 11 of 2018, 17 August, 2018, https://uidai.gov.in/images/resource/Face_Auth_Circular_11_18082018.pdf. For this purpose, a photograph of the person's face would have to be captured and provided to the UIDAI for authentication or e-KYC, along with fingerprint / iris based authentication. In addition, the service provider would have to independently verify whether the image collected during the KYC process matched with the one available in the UIDAI's records.

[15] Justice KS Puttaswamy (Retd.) and Anr v. Union of India and Ors (2018).

entities like banks and telecom companies, although the law also does not prevent these entities from adopting such systems on their own. Face authentication can however still be mandated as a form of authentication for the receipt of a subsidy, benefit or service from the government. In this context, the UIDAI had previously (before the Supreme Court verdict) clarified that the use of facial recognition would only be possible in combination with other modes of authentication like finger/iris or one time password (OTP) as a second factor of authentication.

The amended Aadhaar Act has now introduced the concept of an offline identity verification system. This allows a person to have their Aadhaar-linked photograph and demographic information captured in a extensible Markup Language (XML) file that would be digitally signed by the UIDAI. This information can then be used by the individual for the purposes of KYC verification. As per the UIDAI, this offline e-KYC data can be shared with the agency carrying out the KYC, in either a digital (XML / PDF) or printed (QR code) format. This verification process can be accompanied by mobile number based OTP validation or *"face validation by capturing face and matching against the photo within the e-KYC XML"* (UIDAI, 2019). This suggests that entities conducting KYC verification are left with the discretion to deploy manual or automated facial recognition techniques at their end.

3. **Digital KYC**

In parallel with these developments, there has also been a push towards the adoption of non-Aadhaar based digital KYC processes. This is meant to allow for the satisfaction of regulatory KYC norms without having to incur the high costs of physical KYC verification. As per industry body NASSCOM, one of the reasons for this push in the fintech industry comes from the ineffectiveness of the XML based offline Aadhaar verification method, which was reported to have failure rates as high as 57 percent (K. Gupta, 2019).

In April, 2019, the Department of Telecommunications (DoT) permitted the use of an alternate digital KYC for issuing new mobile connections to subscribers (DoT, 2019). More recently, the rules under the Prevention of Money Laundering Act, 2002, have been amended to allow for digital KYC.[16] Both under the DoT notification and the PMLA rules, the verification can be done only by means of a live photograph (printed or video-graphed photos are not allowed) and has to be accompanied by the GPS coordinates, time stamp and other specified details. Another key element of the process is that the authorised representative of the service provider has to verify that the live photograph of the customer matches with the photo available on their identity/ address proof documents.

While imposing the requirement of verification of the photographs the rules do not specify whether this can be done only through a manual verification or can an automated verification process using FRTs also be deployed? This suggests that the agency conducting the KYC process can use its discretion to make use of FRTs in the process provided that the ultimate responsibility is borne by the authorised individual, in accordance with the rules.[17] It therefore remains to be seen whether the new digital KYC processes will lead to a greater rush for adoption of automated face recognition or would most businesses choose to rely on manual face verification by their employees?

4. **Consumer applications and devices**

Consumers in India end up interacting face recognition systems in various capacities. We have already discussed the scale at which digital images are being added on to the Internet, particularly on social media platforms like Facebook. With over 270 million Facebook users in India, the country constitutes its largest market in terms of user base (Statista, 2019). It is therefore reasonable to assume that Indian users are making a sizeable contribution to Facebook's continuously expanding image database, on which FRTs are being deployed.

[16] Annexure 1 – Digital KYC Process, Prevention of Money-laundering (Maintenance of Records) Third Amendment Rules, 2019.

[17] There are already third party services like Signzy that assist banks and financial service provides in the customer onboarding process by deploying FRTs for conduction KYC checks.

Another emerging use case comes from the availability of biometric unlocking features on mobile devices, more commonly through fingerprint recognition but also increasingly through face recognition. As per Cisco's Visual Networking Index, about 27 percent of the Indian population was using smartphones in 2017 and this figure was expected to go up to 60 percent by 2022 (Bhattacharya, 2018). Several of these smartphones already offer the facial unlocking function but it has not yet become a mass market product, both on account of affordability issues and the emerging nature of the application.[18]

In a country with a per capita income of about 10,000 Indian Rupees per month, it is logical to expect that many of the first time users of smartphones will opt for entry-level to mid-range devices.[19] These devices cannot match more advanced and secure FRTs, like the infrared based technology being used by Apple on its Face ID system.

The relevance of the differential facial security standards available on different smartphones is brought to light by a recent study conducted by Dutch consumer forum, Consumentenbond. The researchers tested 60 smartphones with a face recognition feature and found that 26 of them were vulnerable to a "photo hack". This meant that the device could be unlocked by putting up a photograph of the phone's owner in front of the camera (Kulche, 2019).[20]

In another independent test, even some of the devices that passed the photo hack were found to be vulnerable to a more sophisticated technique of using a 3D printed model of the registered owner's head as an unlocking mechanism (Brewster, 2018). These studies illustrate how, given the user profile and characteristics of the Indian

[18] A search for the term "mobile with face unlock" on Amazon's global and Indian sites provided 574 and 45 results, respectively. The cheapest option with this feature in India was listed for about 4,000 Indian Rupees, which is about 56 US Dollars.

[19] As per a study released by Counterpoint Research, Chinese smartphone makers had captured over 65 percent of the Indian market by March, 2019 (N. Sharma, 2019).

[20] The list of devices that failed the test included those manufactured by brands like Alcatel, ASUS, Huawei, LG, Motorola, Nokia, Samsung, Sony Xperia and Xiaomi. However, many of these companies also had other models, presumably slightly higher end ones, that could not be unlocked with the photograph. This was also the case with the Apple and OnePlus devices that were put to test.

market, reliance on facial unlocking techniques on low-end mobile phones could create increased security vulnerabilities for consumers.

5. **Airport check-in and security**

   In 2018, the Ministry of Civil Aviation launched a project referred to as "Digi Yatra". It is a facial biometric boarding system to be used for automated processing at airports, *"right from the terminal entry gate, check-in/bag drop, security check and boarding gates"* (MoCA, 2019).[21] Testing under the project, which is currently voluntary, has already begun at Hyderabad, Bengaluru and Delhi airports. The process involves online pre-registration by the passenger, which may also be done at the airport kiosk, followed by activation and verification using a government issued identification document.

   As per the scheme documents, the platform will initially provide a 1:1 verification, but this will subsequently be upgraded to a 1:many system, in a phased manner. The policy lays down certain privacy and security related measures that will be adopted to secure users' data. One of the elements of this process is that the biometric data will be removed from the system after completion of boarding and departure from the airport. However, the system operator would have the ability to change this setting based on security requirements, on a need basis. The policy also provides for periodic audits of the biometric system to ensure adherence with prescribed data protection standards.

6. **Attendance systems**

   Another oft-cited use of face recognition is for creating automated attendance systems. Adopters of this technology range from companies like Tech Mahindra, which is using FRTs to mark the attendance of its employees, to multiple applications in the education sector. For example, Delhi's Indian Institute of Technology has a home-grown solution called Timble that is used to mark student

[21] As per the policy, the Digi Yatra Platform is to be built as a joint venture between the Airports Authority of India (AAI) and the five major airport operators in the country. It also refers to the work of a Technical Working Committee consisting of representatives from major Indian airports and the AAI.

attendance (PTI, 2017). Proposals are also underway to roll out similar systems to mark the attendance of young school going students in Tamil Nadu's government schools (India Today, 2018) and for all government teachers in the state of Gujarat (R. Sharma, 2019).

These use cases are very similar to the facts that came up before the Swedish Data Protection Authority in its first fine under the General Data Protection Regulation (EDPB, 2019). The Authority struck down the use of FRTs by a school in northern Sweden to keep track of students' attendance. It was found that the school had processed sensitive biometric data unlawfully and failed to conduct an adequate impact assessment exercise prior to the deployment of the project. Notably, the school has based the processing of the facial data on the consent obtained from the students and parents but it was held that consent could not be a valid legal basis in this situation, given the clear imbalance between the data subject and the controller.

The Delhi High Court is currently hearing a petition against the government's decision to install CCTV cameras in all government run and aided schools in Delhi.[22] The petitioners in this case have submitted that the use of CCTVs is not backed by any detailed study on the impact of the move of the right to privacy of teachers and students, its psychological implications on them and the maintenance of the security of the collected data (Mahajan, 2019). Although the matter is still pending, the Delhi High Court already seems to have formed the view that there is no special right to privacy in class rooms since *"the picture and videos of students have already been captured by CCTV on the road, inside the campus and in the corridor of the school"* (PTI, 2019b).

While this case does not relate to the adoption of FRTs, the observations of the court do indicate a worrying trend of how the widespread adoption of a particular technology, in this case CCTV cameras, can become a ground for its legitimisation and further adoption even in contexts where it might otherwise not have been deemed acceptable.

[22] The matter of Daniel George v. Government of NCT of Delhi (2017) is currently being heard by the Delhi High Court while a similar challenge in Amber Tickoo v. Government of NCT of Delhi (2017) matter was dismissed by the Supreme Court.

In each of the cases discussed above, the adoption of FRTs would generate some benefits. For instance, facial detection might allow intelligence and law enforcement agencies to utilise their limited resources in an efficient manner. This could be used to generate investigation leads, which can then be manually pursued, or to assist in the identification of 'wanted' persons in a large gathering. Another benefit that has been pointed out is that computerised recognition can help in overcoming the errors of human memory and judgement, which could impair the veracity of eyewitness accounts in criminal proceedings (Bromby, 2002).[23]

The use of FRTs could also help in reducing the time and cost of carrying out physical verifications, as seen in the use case relating to digital KYC processes. Under certain circumstances, it could also help in reducing unwarranted exclusions in the delivery of government benefits. For instance, if it is made available as one of several biometric authentication solutions available to a person, particularly when facing difficulties in the use of other mechanisms like fingerprints or iris scan.

These benefits of increased efficiency, security, convenience or accountability, however, need to be weighed carefully against the many concerns posed by the use of FRTs, which have been identified and discussed in the next section.

4. What are the key concerns?

The primary focus of most of the technical research on face recognition has been on improving the accuracy and efficiency of these systems. In other words, to minimise the false negatives and false positives. While both these metrics are useful indicators for evaluating the effectiveness of a system, their actual relevance has to be seen in light of the context in which FRTs are being deployed. For instance, when it comes to a system like Aadhaar, the challenge is to minimise both the false negatives – to avoid exclusion of legitimate beneficiaries – as well as false positives – to prevent misidentification, which would amount to a failure of the authentication process.

[23] Bromby (2002), however, clarifies that even with these benefits, computerised facial recognition systems must only be seen as decision support tools rather than decision-making tools.

A false negative, where the algorithm is not able to identify a person who is supposed to be in a system can lead to unwarranted exclusion and inconvenience. False positives, on the other hand, can be equally, if not more worrying. This is particularly true for situations where facial recognition is being used for surveillance and law enforcement purposes. For instance, the use of facial recognition wrongly identified a student at Brown University as one of the terror suspects in the Easter bombings that took place in Sri Lanka (Fox, 2019). While in this case the error was immediately corrected by the Sri Lankan Police, this may not always be the case. False identification using FRTs can therefore subject individuals to unwarranted investigation, embarrassment and harassment (Marda, 2019).

Yet, even if a facial recognition system were able to achieve perfect accuracy, this does not take away from the fact that the adoption of FRTs poses a number of serious implications from a privacy and civil liberties perspective. These concerns are further compounded by the lack of transparency around the adoption of the technology and likelihood of its disproportionate impact on vulnerable and disadvantaged groups. In this section, we highlight some of the main concerns arising from the use of FRTs, from a legal, ethical and societal perspective, which often tend to be ignored in the more techno-centric debates around FRTs.

4.1. Transparency

Individuals, researchers and the public often do not have access to any meaningful information about the adoption of FRTs in various contexts. This includes the lack of basic information about when, or the specific purposes for which, the technologies are being deployed. Similarly, we know very little about the criteria used for the selection of the technology partner, the security protocols that are in place and the accuracy of the results. Further, to what extent is data that is collected for one purpose being used for FRTs in other contexts?

Transparency about the use of FRTs becomes all the more important when it is used in the context of criminal investigations. One of the basic components of the principle of natural justice is that a person accused of an offence should have access to the information that is proposed to be used against her and the right to cross-examine it. Civil rights groups in the United States have raised these issues in an amicus brief filed before the Florida Supreme Court in the case of *Willie Allen Lynch v. State of Florida.* The case relates to an appeal filed by a person against his conviction for illegal sale of drugs based on the results of a facial recognition algorithm. The accused was the first among a list of probable matches identified by the algorithm with a "one star of confidence" that it had generated the correct match.

Since facial recognition systems typically deal with the personally identifiable information of individuals, some transparency requirements do flow from applicable data protection laws. Recognising the criticality of biometric data, most data protection frameworks treat biometric data as a form of "sensitive personal data".

In Europe, the General Data Protection Regulation prohibits the processing of biometric data (using technical means that allows the unique identification or authentication of a natural person) except under certain specific conditions, which include requiring the explicit consent of the data subject. The law, however, allows member states to introduce further conditions or limitations to these provisions. Whitener and Aragon (2019) note that this has already led to the relaxation of the norms for state agencies in the context of surveillance related functions. For instance, Netherlands has provided a carve-out for biometric data that is necessary for authentication or security purposes and Croatia has created an exemption for surveillance security systems.

In India also, the provisions under the Information Technology, Act, 2000 and the rules under it, classify biometric data as a type of sensitive personal data. This is useful given that the protections that are currently available under Indian law, including for the collection, disclosure and sharing of personal information, are applicable only to sensitive personal data. However, as noted earlier, these obligations are only applicable to "body corporates" and hence do not apply to the government's interactions with biometric facial data.

The current move towards the adoption of a comprehensive data protection law in the country proposes to continue this classification of biometric data as a form of sensitive personal data, allowing it a higher degree of protection compared to other types of data. The draft bill provides that unless the processing of such data is mandated by the law or required to be done in emergency situations, the processing has to be preceded by informed and specific consent from the user.[24] Further, the draft bill also calls for transparency regarding data processing practices and data protection impact assessments by significant data fiduciaries who undertake large scale processing of biometric data.[25]

As and when a comprehensive data protection law comes into place that should determine a basic level of protection, transparency and usage restrictions for the use of facial biometrics. However, there are certain limitations on the kind and degree of transparency that can be achieved through data protection laws. Firstly, the focus of data protection laws is on informing the individual about the ways in which their facial data may be collected and used. This is supposed to give the individual the option to opt out of the system in case she disagrees with such processing. While the effectiveness of this choice remains questionable in all contexts, this is especially true in cases of data processing by the government.

Secondly, data protection provisions are not likely to lead to the kind of transparency that we need from the developers or vendors (as opposed to the adopters or users) of facial recognition systems. This includes information about the underlying model, training data that was used, accuracy rates and other granular information which would make it possible to independently test the accuracy, reliability and biases in the system. We therefore need to look beyond data protection laws to find meaningful ways of ensuring transparency and public disclosure on the part of the developers and vendors of facial recognition systems.

[24] Section 18, Draft Personal Data Protection Bill, 2018.
[25] Sections 30 and 33, Draft Personal Data Protection Bill, 2018.

4.2. Privacy and civil liberties

The unchecked use of FRTs poses a real and immediate threat to privacy and other civil liberties. In this context, Lynch (2018) notes that the main issue with biometrics is that they are unique to each of us and cannot be changed. These risks are even higher in case of facial recognition as in most cases a person's face is exposed at all times, which makes it much more difficult to prevent the collection of one facial images. One of the most worrying use cases from a privacy perspective is the pervasive use of CCTV cameras along with FRTs, which can allow for almost real-time tracking of a person, or at least create the perception of such tracking, which is sufficiently harmful in itself. Besides CCTV cameras the increasing use of devices like smart glasses and body cameras by policing agencies also raise similar concerns.

China's massive network of CCTV cameras and the deployment of FRTs on top of that is one of the most cited examples of a FRT-driven surveillance state. The technology is being used for purposes ranging from profiling of Uighur Muslims in the country's western region to identifying jaywalkers in the Shenzhen region. However, it is important to note that many democratic regimes are also drawn to the massive surveillance potential of FRTs, albeit with a slightly higher degree of checks and balances and greater push back from civil society.

In the United States, roughly one in every two American adults have had their photos searched by a law enforcement agency (Garvie, Bedoya, & Frankle, 2016). In Australia, the federal government is implementing a programme called 'Capability' to enable extensive sharing of images across federal and state databases for the deployment of FRTs (Belot, 2018). In Germany, the police has been using videos and images from police records, train stations and a publicly-sourced database to identify rioters and protesters (Monroy, 2019). Closer to home, the NCRB has invited bids for the creation of the NAFRS, which, as discussed earlier, could potentially have access to any image data base in the country.

In addition to the privacy concerns posed by these systems, they also create a chilling effect on the liberty, movement and speech rights of individuals. The deployment of

FRTs in situations of protests and large public gatherings affects a person's right to association and expression and the ability to express dissent without fears of persecution and backlash. The rise of surveillance technologies combined with FRTs also has worrying implications for the use of face coverings by protesters.

One way in which demonstrators often deal with concerns of targeting and harassment by authorities is by using masks, scarves and other protective gear to conceal their identity. The use of these defensive mechanisms is, however, being rested by state agencies through various "anti-mask" initiatives. These may come in the form of direct restrictions on the use of masks or indirect measures like imposing restrictions on trade and commerce of protective gadgets in times of protest. For instance, in the ongoing protests in Hong Kong protesters have been seen to be deploying instruments like gas masks, helmets, umbrellas and goggles to hide their faces from the gaze of surveillance cameras. In response, the state resorted to measures to restrict the sale and importation of items that may be regarded as "resistance tools" (Quackenbush, 2019) followed by the more recent adoption of an anti-mask law.

In Sri Lanka also, the April, 2019 bombings led the government to issue a notification banning all face coverings, like *burqas,* helmets or masks, that could hinder identification for the purposes of national security (Waldrop, 2019). Many other parts of the world, including several countries in Europe and a number of states in the Unites States, also have anti-mask laws.[26]

As FRTs become pervasive it can only be expected that more and more people will choose to resort to available anti-surveillance techniques, which will, in turn, invite retaliatory actions from the state. This will not only affect the rights of those who choose to mask themselves for civil and political reasons but will also have a disproportionate impact on many others who may adopt facial coverings for various religious, cultural or other reasons.

[26] Some of these laws were brought to control the actions of specific groups like the Ku Klux Klan, controlling public gatherings that have the potential to become violent or preventing the use of masks while committing a crime (Daly, 2017).

For instance, Daly (2017) notes how the French government's broadly worded restrictions on religious face covering are broad enough to also apply to those who cover their faces in political protests.[27] Similarly, people may choose to cover their faces for a variety of other unconnected reasons like to protect themselves from the heat, cold or air pollution. Any sweeping restrictions on face coverings could therefore end up affecting the rights of a very broad spectrum of individuals.

Although surveillance and law enforcement seem to be the most ubiquitous and vexing use cases of FRTs, certainly from a privacy perspective, the widespread commercial deployment of the technology also poses its fair share of concerns. A person's face serves as a unique identifier which can be used for pooling together information about them from multiple online sources. This takes away their liberty to share information about themselves in some contexts but remain anonymous in others. For instance, Acquisti, Gross, and Stutzman (2014) demonstrate how it is easily possible to connect images from an online dating site, where individuals put up their pictures but might want to protect their identities (by using pseudonyms), with publicly available profiles on social networking sites.[28] It has also been noted that the use of FRTs by platforms like Facebook alters the characteristics of a photograph into biometric data while at the same time taking away the user's control over the further transmission of that data (Welinder, 2012).

Another talked about commercial application of FRTs is in the retail sector, for in-store tracking of customers and display of relevant marketing content to them. In this context, CDT (2012) notes that although current systems of digital advertising tend not to personally identify the consumers, future applications of FRTs could well be geared at delivering tailored content based on individual profiles. In effect, this would build an "*offline version of the behavioral advertising that currently occurs online*". The level of identifiability required by such systems will of course vary as per the specific use

[27] In 2014, the European Court of Human Rights passed a decision in S.A.S. v. France allowing the French government to ban the use of facial coverings in public places on the ground that restricting such covering was more conducive to the process of socialisation and "living together" in society.

[28] The researchers were also able to link unidentified subjects with images available on websites like Facebook and Linkedin and then apply data mining techniques to generate a detailed profile about the originally unidentified faces.

case. For instance, automated checkouts and payments using FRTs logically require a higher degree of identifiability compared to generation of marketing materials based just on characteristics such as the user's gender or age.

4.3. Accuracy and reliability

It has been a well acknowledged problem in the field of facial recognition that the results of the system are only as good as the quality of the images that are being run through it. Differences in the conditions of the images being compared can therefore easily lead to errors in facial recognition (Senior & Bolle, 2002b). This can occur for a number of reasons, such as *physical changes* in the facial expression, age, personal appearance (makeup, glasses, facial hair); *acquisition geometry changes* linked to the angle of the face or the presentation of the profile; and *imaging changes* on account of the variations in lighting, camera variations and other characteristics of the image (Senior & Bolle, 2002b; Lu et al., 2003; Li & Jain, 2011).

Researches have pointed out that these problems are less likely to affect the results of 3D facial recognition systems. 3D systems are capable of functioning well even under dim lights and with variant facial positions and expressions, situations which have typically posed a challenge for 2D systems (Zhou & Xiao, 2018). However, as of now, most use cases of FRTs continue to be built on 2D systems and therefore the concerns discussed here are likely to remain relevant in the near future.

This is also reflected in international standards on the use of face image data for biometric applications, like the ones adopted by the International Organization for Standardization and the International Electrotechnical Commission. These standards provide detailed specifications regarding data formats, scene constraints (lighting, pose, expression, etc.), photographic properties (positioning, camera focus, etc.) and digital image attributes (image resolution, image size, etc.) (ISO/IEC, 2011). In situations where such conditions can be mandated and controlled, as seen in the case of passport photographs for visa processing, the gallery database would consist of a higher quality of images and thus be more suitable for being processed through a facial recognition system. This is also the case for other cooperative situations like image databases of employees or students, which may be used for the purpose of 1:1 verification.

The larger challenge, however, arises in context of real world applications of FRTs in non-cooperative settings, particularly when a 1:many identification process is being carried out. For instance, images collected from a CCTV camera would invariably be captured in different lighting and camera angles and with differing facial expressions and appearance than the ones contained in the gallery database. Moreover, there could also be situations where both the gallery database and the probe image are collected in a non-cooperative setting, which makes the results even more prone to errors.

Accuracy rates are also found to be lower in contexts where real-time biometric processing of video imagery is involved. In a study conducted to assess the live facial recognition system being tested by the London Metropolitan Police,[29] Fussey and Murray (2019) found that out of the 46 potential matches identified by the system only 8 matches could eventually be verified correctly, indicating a success rate of about 19 percent.[30]

Besides the variations in the gallery and probe images, the training data that is used for developing the facial recognition system also plays a major role in determining its effectiveness. Buolamwin and Gebru (2018) have demonstrated how the commercially available facial recognition tools offered by leading companies like Microsoft, IBM and Face++ reported much higher error rates for persons with darker skin tones. The study found that darker-skinned females were the most misclassified group – with error rates of up to 34.7 percent – while the maximum error rate for lighter-skinned males was just 0.8 percent. This difference arose primarily on account of the under-representation of data belonging to darker skinned persons in the dataset that was used for training

[29] The system involves the deployment of live cameras using which the images of passersby are streamed directly to the live facial recognition system database, which contains a 'watch list' of offenders.

[30] Of the remaining matches made by the automated system, 16 were judged as being "non-credible" by the adjudicating officers and 14 were verified as incorrect matches following an identity check.

the algorithms. In a follow up study, Raji and Buolamwin (2019) included two more companies – Amazon and Kairos, with similar results.[31]

Although studies like these have questioned the effectiveness of FRTs in real world scenarios, technical evaluations show that there have been significant leaps in FRTs in the last five years. As per NIST's findings from its Face Recognition Vendor Testing Program, there have been massive gains in accuracy in the results of the 2018 tests compared to the ones in 2013.[32] NIST attributes these gains to the "*integration, or complete replacement, of older facial recognition techniques with those based on deep convolutional neural networks*" (Grother, Ngan, & Hanaoka, 2019).

While reporting that the best performing algorithms offer "*close to perfect recognition*", the NIST study also points to the need to place these findings in the right context. First, the report clarifies that the results are applicable only in the context of mugshot images searched in mugshot galleries – the primary gallery used for the tests comprised of 26.6 million portrait photos from well-controlled settings. Second, there were significant variations in the results among different algorithms and developers, with recognition error rates in a particular scenario ranging from *"a few tenths of one percent up to beyond fifty percent"*.

These factors could partially explain the gap between lab tested accuracy levels and the actual performance of FRTs that are currently in use. At the same time, it is also likely that the algorithms submitted to NIST for review may be more advanced than the ones that are commercially being deployed. The study itself suggests that this may be the case and advises end-users of FRTs to "*establish whether installed algorithms predate the development of the prototypes evaluated here and inquire with suppliers on availability of the latest versions*" (Grother et al., 2019).

[31] They reported error rates of 31.37 percent and 22.50 for darker females, compared to overall error rates of 8.66 percent and 6.60 percent, for Amazon and Kairos, respectively.

[32] These results are based on the 1:many identification evaluation of 127 algorithms conducted by NIST on two-dimensional images.

4.4. Bias and discrimination

India is a multi-racial, multi-ethnic, society, which is also reflected in the diversity of physiological characteristics seen across the country. We already have studies that point to the significant differences between the facial features of people from North India and South India (Prasanna et al., 2013) and the differing abilities of humans and machines to classify Indian faces into these groups (Kattia & Aruna, 2018). The actual diversity of Indian faces, however, extends much beyond the broad north / south based regional variations.

O'Toole (2011) notes that just as humans display an "other race effect" – where they are able to better recognise faces belonging to the same race as them – this is also the case with facial recognition algorithms. Based on data from NIST's 2006 vendor test, researchers grouped together the algorithms submitted from East Asia, Europe, and North America to find that each algorithm displayed more accurate results for faces from the same region, possibly due to the nature and volume of the training data that was being used. Based on these results the researchers suggested that since many facial recognition algorithms are often applied to diverse user sets it is important to ensure that "stability over demographics" should be considered as one of the factors for determining its robustness (Phillips, Jiang, Narvekar, Ayyard, & O'Toole, 2011). This factor becomes particularly important given the scale at which facial recognition tools developed in certain jurisdictions, like China, are being widely deployed by users across the world on populations with very different facial characteristics.

It is also important to highlight that most of the research around algorithmic bias and discrimination has emanated in the US context and the focus has mainly been on issues of race (or skin color) and gender. The accuracy problems of FRTs in these contexts are often attributed to the use of biased data sets, which end up generating results that are detrimental to particular demographic groups. This was the case in the mis-characterisation of faces of females with darker skin tones (Buolamwin & Gebru, 2018; Raji & Buolamwin, 2019). Similarly, there is also evidence to show that the problem of false matches generally tends to be higher in case of people of color. A study done by the American Civil Liberties Union using Amazon Rekognition found 28 false matches while comparing the pictures of members of the United States Congress against a database of 25,000 publicly available arrest photos. Interestingly, nearly 40 percent of the false matches in the test were of people of color, even though they constitute only about 20 percent of the total members in the Congress (Snow, 2018).

Research of this nature has helped in shining the light on issues of bias in FRTs. It can also become the basis for bringing about improvements to the algorithms in question. For instance, in their follow up work on the Gender Shades study, Raji and Buolamwin (2019) found that all the three systems covered in their original study (Microsoft, IBM, Face++) displayed a reduction in the error rates for female faces as well as darker faces. While this seems like a positive development, it has been pointed out that ensuring better demographic representation in data sets does not do much to solve the larger issues of injustice in the institutional contexts within which facial recognition is being employed (Hoffmann, 2019). Others, like Keyes (2018), challenge the very premise of deploying automated gender recognition systems, which tend to reflect the traditional models of gender as being binary, physiologically based, and immutable. This works to the specific detriment of cerain groups, like transgendered persons, who may not fit into the traditionally defined gender constructs.[33]

This begs the question whether having facial recognition algorithms that are better at identifying individuals within more specifically defined classes necessarily lead to fairer outcomes? Or would it become an even more potent tool for targeted mis-treatment and discrimination? Individuals should ideally not have to be subjected to the either the bias and discrimination caused by poor accuracy rates or face the consequences of highly accurate, reliable, effective and potentially ominous facial recognition systems (Parsheera et al., 2019). This represents the moral dilemma of facial recognition, one that will only worsen with further advances in the technology.

[33] An examination of 58 papers on the subject of automatic gender recognition showed that 94.8 percent of the papers treated gender as binary (male/ female or man/ woman); 72.4 percent treated it as being immutable (that which cannot be altered post-assignment); and 60.3 percent treated it is as physiological (based on externally-visible structure of a person's body) (Keyes, 2018).

4.5. Limitations of the supporting ecosystem

Another important factor, particularly in the Indian context, is the relevance of the surrounding ecosystem within which the face recognition technology is sought to be introduced. For instance, the mandatory use of FRTs for marking attendance in rural schools would have to account for real world factors like power outages, network down time, availability of devices and power structures within the local community. While these issues go beyond the technical capabilities of FRTs, or even the legal and ethical implications around them, it would be dangerous to adopt such technological solutions without understanding this context. Similar concerns have also come up in the context of biometric authentication using Aadhaar, and would continue to remain relevant if mandatory facial recognition were to be deployed in future, either for Aadhaar authentication or KYC verification.

Moreover, the idea of using facial recognition in the context of Aadhaar came up, at least in the public domain, only after a large chunk of the population had already been enrolled. This makes it important to verify whether the photographs that were collected during enrolment process are of adequate quality to deliver reliable results going forward. The adoption of FRTs for Aadhaar authentication, whether on a voluntary or mandatory basis, or any other use of Aadhaar images for facial recognition purposes, will therefore have to be preceded by extensive trials. Such trials will have to be representative in character, accounting for factors like gender, age, race, geographic location and existence of persons with disabilities in the population. Further, the methodology and results of any such tests will need to be put out in the public domain for necessary verification and scrutiny of the systems.

In addition to the concerns of accuracy and error rates as well as the implications for individual rights and civil liberties, the facial recognition market is also characterised by several market failures.

Firstly, there is the issue of *negative externalities* arising on account of the transaction between the adopters and developers of FRTs, which has significant implications for the rights and liberties of third parties, often without their knowledge or consent.

Secondly, there is a high degree of *information asymmetry* between developers, adopters and persons who are subjected to the system, whether as part of the training data set, as gallery images or as the probe subject. This is closely linked with the transparency concerns that were discussed earlier.

Thirdly, it can also be argued that since FRTs serve to facilitate the provision of enhanced security by the state, which is a *public good,* there is in fact a case for policy interventions to encourage further research and development in this field.

The co-existence of these factors poses difficult questions about what should be the appropriate frameworks to balance the complex tradeoffs between the security, efficiency and other benefits of FRTs and the many concerns posed by the use of this technology.

5. What could be the possible interventions?

The different belief systems surrounding the use of FRTs have led to a range of proposals on whether and how this technology should be regulated. At one end of this spectrum are those who call for an absolute ban on FRTs, noting that it poses an extraordinary danger, far in excess of other forms of surveillance and self-regulation measures are not going to be sufficient to address these concerns (Hartzog, 2018). In particular, such bans or restrictions are being called for in the context of government use of facial recognition systems. At the same time there are some organisations, like the Ada Lovelace Institute, that are advocating for a broader, but voluntary, moratorium on all future public and private sector deployment of FRTs (Kind, 2019).

Many other stakeholders have suggested that the concerns posed by FRTs need to be regulated, at this stage, through ethical frameworks that will comprehensively address issues such as, privacy, security, accuracy, transparency, bias, etc. In a handful of cases, the need for legislative interventions to ensure such outcomes has also been proposed.[34]

[34] For instance, organisations like the Electronic Frontier Foundation have called for government actions to *"limit unnecessary data collection; instill proper protections on data collection, transfer, and search; ensure accountability; mandate independent oversight; require appropriate legal process before collection and use; and define clear rules for data sharing at all levels"* (Lynch, 2018).

At the other extreme of the spectrum is the perspective that the growth of emerging technologies like facial recognition should not be stifled though premature regulation. Proponents of this view would argue that future innovations in FRTs, both in terms of improved accuracy as well as the development of privacy protecting measures, will be able to address most of the concerns without the need for any form of stricter regulation at this stage.

However, in practical terms, a “no regulation” framework may not really be feasible as there seems to be growing convergence on the need for some sort of intervention to balance the benefits and challenges of facial recognition systems. This is also reflected in the global move towards enhanced data protection, with biometric data being one of the protected categories, and the widespread adoption of national strategies for artificial intelligence. Many of these strategy documents speak of the need for ethical and responsible development of Al-based systems.

Finally, it would also be relevant to track the role of technological innovations that can act as a counter measure to check the increasing use of FRTs. Examples of this include eye glasses with infrared-blocking lenses (Reflectacles, 2019) and solutions like D-ID, which use image modification techniques that can make images resistant to facial recognition systems (D-ID, 2019). However, so far, these can be regarded as fringe solutions that cannot really match the speed and scale of adoption of FRTs.

5.1. Stakeholders and their roles

The future advancements in FRTs as well as the policies surrounding them are likely to shaped by the complex interactions between a range of different actors and the belief systems within which they operate. We identify below some of the key stakeholders that are involved in this process, while also recognising that not all of these actors can, or will, have an equal say in such decisions.

1. Developers or vendors of FRTs, generally private corporations like Microsoft, Visionlabs, Amazon, NEC, etc. At the same time, we are also seeing seeing several collaborations between technology companies and universities to collectively engage in research on FRTs.

2. Adopters of FRTs, which may be governments agencies as well as private actors. In both these cases the technology can be used for surveillance or non-surveillance related purposes.
3. Researchers, academics and civil society organisations engaged in evaluating the performance of FRTs and its legal and ethical implications. Employees and shareholders of some of the large players in the FRTs space have also lent their voices to this debate, in particular, by rallying against the sale of FRTs to government agencies for surveillance purposes.
4. Individuals whose data is used for training of facial recognition systems and on whom the technologies are actually being deployed.
5. Government agencies and courts that will ultimately be responsible for deciding the policy or legal interventions that may be required in this space, taking into account the costs and benefits of using FRTs in different contexts.

Of these, the first two groups, namely the developers and adopters of FRTs, are primarily responsible for driving the conversation about new functions and applications of facial recognition systems. We therefore need to begin by asking whether these stakeholders have the ability, as well as incentives, to assess the complex tradeoffs that are involved in the process?

To some extent, the answer may lie in the pressure being exerted by researchers and civil society organisations in demonstrating the pitfalls of indiscriminate adoption of FRTs. This is accompanied by demands for more stringent and external forms of regulation. This bears reputational implications for the developers of the technology as well as commercial ones, particularly when studies point to the gaps in the accuracy or effectiveness of the system. At the same time, the fear of regulatory and compliance burdens can also serve as a significant motivator for the adoption of self-regulatory codes and practices.

Any move towards the regulation of FRTs will also be shaped by the complex interactions between the government and the private sector in the development and use of facial recognition systems. Speaking in the context of collection and use of personal data, Schneier refers to the *"public/private surveillance partnership"*. While it may be reasonable for the government to limit the circumstances under which corporations can collect and use personal data, the fact that the government is able to use that very data for its own surveillance purposes, creates a disincentive for bringing laws that limit data collection (Schneier, 2013).

Applied to the FRTs context, we see that policy decisions of one sort, i.e. government deployment and procurement of FRTs, are leading to private investments in, and technical advancements of, the technology. At the same time, its widespread deployment, accompanied by reports of harm being caused to individuals, is leading to strengthened calls for regulatory interventions in this space. Adopting a firm regulatory stance will eventually end up curtailing the government's own powers and surveillance capabilities, making it harder to expect such a decision.

Finally, when it come to the role of individuals, in most cases they neither have the information nor the ability to question the deployment of FRTs. Data protection frameworks try to offer some semblance of individual control over decisions about personal data, through requirements of notice and consent, and "explicit consent" in case of biometric data. However, the effectiveness of these measures in the context of FRTs, particularly when it comes to government use of data, remains questionable. The representation of individual interests in the debates surrounding FRTs can therefore be expected to be left largely to the mercy of governments, advocacy groups and courts.

5.2. Models of regulation

At the heart of the discussion on choosing an appropriate model for regulation of FRTs lies the tussle between the benefits of permission-less innovation and the challenges of recognising and controlling its significant adverse implications. As noted in the introduction to this section, the approaches that are currently being discussed in this regard can broadly be classified into two categories. The first approach is one where the responsibility of developing and adhering to ethical principles for facial recognition would be left primarily to the industry – the developers and users of the technology. The second approach is one that would involve some sort of external oversight and regulatory restrictions on the use of FRTs, generally through some form of legislative intervention. This maybe in the form of banning specific use cases, a full fledged mechanism for independent regulatory oversight or a co-regulatory model with participation of the industry as well as the regulator.

As per the AI Ethics Guidelines Global Inventory complied by Algorithm Watch, most of the current discussions around ethical deployment of artificial intelligence focus on voluntary commitments, with only three or four examples that suggest an oversight or enforcement mechanism (Algorithm Watch, 2019).

The self-regulatory approaches generally require that the providers of facial recognition systems should assess the ethical considerations emanating from the use of the technology, including decisions on who to supply to and in what contexts. For instance, in December, 2018, Microsoft announced the adoption of a set of six principles – fairness, transparency, accountability, non-discrimination, notice and consent, and lawful surveillance – which would guide its work on facial recognition (Microsoft, 2018).[35] Following this, the company has reportedly refused to supply FRTs to government agencies on two occasions where it was believed that the technology could be used to carry out blanket surveillance or impede the freedom of assembly (Kraus, 2019).

In some cases, calls for self regulation by developers of FRTs have been initiated by their own shareholders and employees. Notably, a group of Amazon's shareholders had put together a proposal seeking a prohibition on the sale of FRTs to government agencies on the grounds that it threatens civil liberties and creates scope for discrimination against minority groups.[36] The resolution was ultimately rejected by the company's

[35] To be clear, Microsoft has expressed the view that these voluntary principles are not an end in themselves and need to be accompanied by a legislative framework that will inform the baseline regulation on facial recognition. Similar to Microsoft, Amazon has also recommended the need for a legislative framework to govern face recognition. The difference, however, is that its proposals are geared mainly towards ensuring responsible use, particularly by government users, rather than controlling the conduct of the developers of the technology.

[36] Amazon's board, however, opposed the proposal on the ground that new technology should not be banned or condemned because of its potential misuse and the focus should instead be on properly regulating its usage. See Notice of 2019 Annual General Meeting, 11 April, 2019, https://ir.aboutamazon.com/static-files/35fa4e12-78bd-40bc-a700-59eea3dbd23b.

shareholders along with another proposal that demanded an independent human and civil rights review into the use of the technology (Whittaker, 2019).

There have also been some government and industry level initiatives to nudge users towards the ethical deployment of FRTs on a voluntary basis. In 2016, the National Telecommunications and Information Administration in the United States came out with its recommendations on privacy best practices for the use of facial recognition for commercial purposes. The recommendations speak of the transparency that should be offered to consumers regarding the use of the technology, adequate security and quality standards as well as mechanisms for resolution and redress.

Similar guidelines have also been adopted in specific sub-sectors. For instance, CDT (2012) refers to the initiatives of the Digital Signage Federation and the Point of Purchase Advertising International in the United States for adoption of desirable privacy standards in the digital signage sector. These voluntary standards contain requirements like opt-in consent for collecting any directly identifiable information, prohibition on collecting facial recognition information on minors (under 13) and providing notice of data collection, even if it only consists of "anonymous" data. While noting these developments, CDT (2012) also acknowledges that the effectiveness of these standards is affected both by their voluntary character and the fact that digital industry currently forms only a small part of the broader commercial ecosystem for FRTs.

Moving to the second approach of external oversight mechanisms, we note that FRTs are already being regulated to some extent in countries that have data protection laws, which tend to treat biometric data as a form of sensitive personal data. This is the case under the European GDPR as well as the proposed data protection bill in India, both of which apply to the processing of personal data by private parties as well as state agencies. The version of the draft bill prepared by the Justice Srikrishna committee, in fact, goes on to suggest that the government would have the power to ban the use of certain forms of biometric data, except as permitted by law. However, there is no guidance on the actors against whom, and the circumstances in which, this power could be used.

In contrast to the proposals in India and the law in Europe, the biometric protection laws that have been adopted by states like Illinois, Texas and Washington in the United States are applicable only to private entities.[37] However, there have been other specific instruments, like the amendment to the Administrative Code in San Francisco, which have imposed restrictions the use of FRTs by government agencies in the United States.[38] As we discuss in the next section, a closer look at the San Francisco ordinance reveals that although it has imposed a general ban on the use of such technology by the city's departments, it is still possible for it to be used for investigative or prosecutorial functions, in certain contexts.

Looking beyond the realm of privacy and data protection, the calls for regulation of FRTs are also being driven by considerations like the need to ensure greater transparency by technology companies, so as to enable independent testing of accuracy and unfair bias (Smith, 2018). Information of this sort is necessary for there to be independent checks on the functioning of facial recognition systems and to facilitate more localised studies, such as the the use and impact of particular FRTs in the Indian context.

6. Surveillance and law enforcement: *When could it be necessary and proportionate?*

While intelligence and law enforcement agencies view FRTs as an indispensable tool for furthering security and law enforcement objectives, much of the conversation around the regulation of FRTs is also focused on these use cases. The challenges to privacy and civil liberties from the use of FRTs in these contexts and the potential for its disproportionate impact on vulnerable groups has led to calls for banning, or at

[37] Recently, there has also been a move to bring about a national level law called the "Commercial Facial Recognition Privacy Act of 2019" that would restrict any private collection, use and sharing of facial recognition data without adequate notice and affirmative consent. The bill also seeks to prohibit the use of such data to discriminate against a person in violation of a law or to repurpose the data for a different purpose. While an official version of the bill has not yet been published, an unofficial version is available online at https://www.scribd.com/document/401931553/The-Commercial-Facial-Recognition-Privacy-Act.

[38] Chapter 19B, Administrative Code – Acquisition of Surveillance Technology, https://sfgov.legistar.com/View.ashx?M=F&ID=7206781&GUID=38D37061-4D87-4A94-9AB3-CB113656159A. It has been reported that this move is also being followed by some other cities in the United States, like Somerville and Oakland (Metz, 2019).

least severely restricting, its adoption for surveillance purposes. The decision of the city of San Francisco in May, 2019 to ban the use of facial recognition by government agencies has become one of the most widely discussed examples of such a position, leading to calls for similar restrictions in many other parts of the world.

The ordinance adopted by San Francisco makes it unlawful for any city department to directly obtain, retain, access, or use any FRTs or any information obtained from them. The term "department" is defined fairly broadly to include any official, department, board, commission or other entity in the city but *does not include* the District Attorney or the Sheriff while performing their investigation or prosecution functions. In such cases, the agencies will have to certify why the acquisition of a specific technology is necessary for their functions. Further, in order to ensure transparency, that certification will be required to become a part of the public record. Similarly, federally-regulated facilities at the airport or port, are also excluded from the scope of the restrictions.

This offers an interesting example of a model where government use of FRTs is barred for general surveillance purposes (as well as all other non-surveillance uses like allowing entry to public buildings, delivering benefits transfers, etc.) but can still be used in situations where it can be shown to be necessary for investigative and law enforcement purposes.

The challenge for each country then becomes that of determining what are the tests based on which it would be determined whether the use of FRTs for surveillance or law enforcement purposes can be regarded as being "necessary" in a particular context? What should be the appropriate procedural safeguards in such situations?

In India's case, the legitimacy of any state-led intervention involving the use of FRTs will necessarily have to pass muster under the tests laid down by the Supreme Court in the case of *K. S. Puttaswamy v. Union of India.* This was followed by the decision in the Aadhaar case where we saw the application of these tests in the context of biometric technologies. In addition there are a set of challenges to the constitutional validity of the surveillance architecture in India that are currently pending before the Supreme Court.

The manner in which future courts may examine the validity of a framework like the NCRB's proposed face recognition system is therefore very likely to be influenced by the application of the *Puttaswamy* tests in these related contexts.

In addition to the jurisprudence from India, the judicial developments and checks and balances on the use of FRTs being discussed in other parts of the world would also serve as a useful reference point for courts and policymakers in India.

In December, 2018, the Hamburg Data Protection Commissioner passed an order against the use of FRTs by the Hamburg police for identification of rioters who participated in the G20 protests in the city. The data being used by the police for this purpose included videos and images of persons in public spaces, like stations, using its own databases as well as a crowd-sourced collection of data. The Data Protection Commissioner found that there was no legal basis for the processing of the personal data of thousands of uninvolved persons against whom there was no specific suspicion of being involved in the riots. Accordingly, the Commissioner directed the deletion of the reference database and the information contained in it (Hamburg Data Protection Commissioner, 2018). The interior authority of the city of Hamburg had challenged this order before an administrative court, which has recently been granted by the court.

The UK High Court also looked into the legality and proportionality of a live facial recognition system but arrived at a decision which is very different from that of the Hamburg Commissioner. We discuss the court's order in the case of *R (Bridges) v. Chief Constable of South Wales Police and Ors (2019),* and its implications, in the following sections.

6.1. FRTs through the *Puttaswamy* lens

In August, 2017, the Supreme Court of India delivered a landmark verdict in the *Puttaswamy* case affirming that privacy constitutes a fundamental right under the Indian Constitution.[39] The court held that even though this right is not explicitly mentioned in

[39] Justice KS Puttaswamy (Retd.) and Anr v. Union of India and Ors (2017).

the Constitution, it derives its fundamental status from its interplay with a number of other constitutional rights. This includes the right to life and personal liberty (Article 21), right to equality (Articles 14 to 18) and freedoms of speech, expression, movement, association, etc. (Article 19). While doing so, the court also established that even though privacy is not an absolute right, any interference in an individual's privacy by the state, should be done only in a manner that is *"fair, just and reasonable"*.

The judges then went on to explain what it would mean to be fair, just and reasonable in the context of privacy, laying down the following tests: (i) *legality* – the intervention should be supported by a law; (ii) *legitimate goal* – it should pursue a legitimate state aim; and (iii) *proportionality* – there should be a rational nexus between the objects and the means adopted to achieve them. Further, it was also observed that there need to be appropriate procedural guarantees to check against the abuse of state power.[40]

The scope of the proportionality test was further clarified by the Supreme Court in the Aadhaar case. The majority decision in the case reiterated that in addition to the requirement of there being a legitimate goal and a rational nexus between the adopted means and that goal, there are some specific tests of proportionality that must be satisfied. Proportionality requires that the intervention in question should be able to satisfy the requirements of *necessity* – there being no less restrictive but equally effective alternative and *balancing* – no disproportionate impact on the right holder. Drawing from the work of Bilchitz (2014), the Supreme Court noted that the right approach would be to first consider the range of possible alternatives available to the government to achieve the desired goal; assess the effectiveness of each measure individually, followed by the impact of the respective measures on the rights that are at stake. Based on this assessment it would be determined whether there could be an alternative, less restrictive, remedy.

The legitimacy of the facial recognition system proposed under the NCRB tender has already being questioned on these grounds. In a legal notice sent by the

[40] See Bhandari, Kak, Parsheera, and Rahman (2017) for a more detailed discussion on the tests applied by the different Judges in this case.

Internet Freedom Foundation to the NCRB and the Ministry of Home Affairs the organisation has pointed to the lack of any statutory basis for the creation of such a system (A. Gupta, 2019). This violates the first test laid down by the Supreme Court in the *Puttaswamy case*. Further, the notice also challenges the proposed system on the grounds that it allows images of individuals to be collected without their knowledge and consent; is susceptible to misidentification and discriminatory profiling; and lacks proportionality safeguards and oversight mechanisms. In the event that the government still proceeds with the system in its current form this is likely to become an important precedent for the application of the legality and proportionality tests in the context of FRTs.

Notably, one of the arguments put forth by the government in the Aadhaar litigation was that a person's face is a widely accepted form of identification and we routinely provide facial photographs for purposes like issuance of driving licenses, passports, school admissions, etc. Based on this, the state argued that there can be no "reasonable expectation of privacy" in facial photographs. The court rejected this argument while noting that when any demographic or biometric data is being collected and stored by state agencies, it merits a closer examination using the proportionality tests. At the same time, the court also conceded that the fact that certain information about individuals is available in the public domain could be a relevant factor while undertaking the balancing exercise in the proportionality analysis.

In the context of FRTs, it would be pertinent to note that the processing of a facial image to develop an individual's unique facial pattern, and the ability for that data to be stored and processed later, gives facial recognition a character which is very different from putting one's face or photos in the public domain. Therefore, the argument of people's faces being available in the public domain should in any case not be regarded as a valid mitigating factor in case of deployment of FRTs for law enforcement purposes.

Following are some of the other factors that would be relevant while examining the NAFRS proposal through the *Puttaswamy* lens.

1. **Lack of legal basis**

   The mechanism proposed under the NCRB tender is in *prima facie* violation of the first test of legality as the system being proposed under it does not have any statutory basis. Neither is it created under any rules or regulations, which might in turn have a statutory backing. This is in direct contrast to situations where there exists a statutory basis for access to personal data. This includes provisions on interception of telephonic messages and data under the Telegraph Act and the Information Technology Act, respectively or collection of fingerprints under the Identification of Prisoners Act.

   In the Aadhaar case, we saw the Supreme Court strike down certain requirements of mandatory linking of Aadhaar precisely for the reason that such actions did not have a legal basis. This was the case with the administrative circular on mandatory verification of SIM card ownership as well as the linkage with various scholarship schemes by bodies such as the Central Board of Secondary Education and the University Grants Commission. The lack of any enabling legal provision in the case of NAFRS would therefore be the first barrier to its legitimate adoption.

   Even if the government were to subsequently enact such a law, or argue that the basis for adoption of FRTs flows from general investigation powers under criminal law, the design and implementation of NAFRS would of course still have to pass muster under the other layers of the *Puttaswamy* tests.

2. **Violation of proportionality standards**

   The stated objectives of the NAFRS, which include the identification of criminals, missing children and adults and unidentified dead bodies, all lie well within the bounds of legitimate state objectives. Therefore, it would be reasonable to expect that any court in India will not find it hard to agree that the proposed NAFRS satisfies the second *Puttaswamy* test. It is however going to be much harder to justify how the deployment of FRTs over large segments of the population, without their consent, can be regarded to be a proportionate response for meeting the desired goals.

While rejecting the justification of countering black money as the basis for mandatory linkage of Aadhaar with bank accounts, the majority verdict in the Aadhaar case had noted that imposing such a restriction on the entire population, without any evidence of wrong doing on their part, would constitute a disproportionate response. In the words of the court, *"[u]nder the garb of prevention of money laundering or black money, there cannot be such a sweeping provision which targets every resident of the country as a suspicious person*". Such a "presumption of criminality" would be treated as being disproportionate and arbitrary.[41]

The same logic would also apply to the deployment of FRTs on innocent citizens, without there being any reasonable suspicion of them being involved in any illegal activity. As noted by Peter Schaar, the former German Data Protection Commissioner, such uses of FRTs "*render innocent people suspects for a time, create a need for justification on their part and make further checks by the authorities unavoidable*" (Introna & Nissenbaum, 2010).

The lack of any data minimisation norms or mechanisms to ensure purpose limitation, will also make it harder for the state to justify the reasonableness of the selected mechanism. For instance, there are no effective limitations on the sources of images that can be legitimately used by the system, the gravity of offences that might qualify for its use, or checks against any further mission creep in the purposes for which the NAFRS may be used.

3. **Effectiveness of the intervention**

   Another factor that should go into a proportionality analysis of the NCRB's proposed facial recognition system is an examination of the effectiveness of the selected mechanism to achieve the intended objectives. This is a precondition to understanding the *necessity* of the intervention. As discussed earlier, there are several challenges with the accuracy and reliability of FRTs. The results would

[41] Para 430, Justice KS Puttaswamy (Retd.) and Anr v. Union of India and Ors (2018).

therefore be affected by variations in the environment and lighting conditions and the challenges of using images gathered from non-cooperative settings.

Further, some of the specific functions of the NCRB's proposed system, like application of NAFRS for identification of missing children and unidentified bodies, are widely-recognised as "unsolved problems" of FRTs. Research on FRTs has shown that even in case of facial recognition algorithms that otherwise perform very well, age related factors and facial injuries are among the main reasons that lead to poorer results (Grother et al., 2019).

Unidentified bodies are often found with injuries or in a condition where disfiguration or decomposition has taken place. This will make it harder to undertake reliable automated recognition using such images. Similarly, the use of FRTs for identification of missing children also poses unique issues due to the likely age difference that exists between probe and gallery images accompanied by the inability to obtain an updated facial image to update the gallery dataset (Park & Jain, 2011). This challenge is also reflected in the standard operating procedure adopted by the South Wales Police in UK in the context of its live facial recognition system. The procedure notes that children under the age of 18 will not normally feature in a watchlist due to *"the reduced accuracy of the system when considering immature faces"*.[42]

At the same time, we already have a precedent of a situation where the application of FRTs by the Delhi Police is reported to have resulted in the identification of close to 3,000 missing children. This action was taken by the police pursuant to a direction issued by the Delhi High Court in April, 2018. The identification was done by matching the images of missing children with a database of photographs of over 45,000 children living in various children's homes (PTI, 2018b).[43]

Subsequent developments have, however, found the Delhi High Court questioning the police for the lack of further results in use FRTs to find missing children. Most recently, the police was directed to submit details of the number of missing children

[42] R (Bridges) v. Chief Constable of South Wales Police and Ors (2019).

[43] The recognition technology for this purpose was provided by the software developer, Vision Box, free of cost for a period of one year subject to the condition that it would be used only for tracing missing children (PTI, 2018a).

who had been identified using the technology and the status of their restoration with their families. These observations were made by the Court pursuant to the submissions made by the Ministry of Women and Child Development about the poor performance of the facial recognition software, including, in some cases, its inability to distinguish between boys and girls (PTI, 2019a).

This seems to suggest that a targetted intervention, like matching faces of missing children with a gallery of images of children living in children's homes in an identified region, might be able to deliver more effective results compared to the general application of FRTs on a broader segment of the population. However, in the absence of data protection norms, even such targeted use cases leave us with several unanswered questions. For instance, what happens to the data of the children who were part of this exercise but whose data did not match with the missing children? Will their data be retained and used for other purposes, including future investigations in criminal cases?

This discussion circles back to the core issue of proportionality in the use of FRTs. The limited accuracy and reliability of FRTs, combined with serious privacy concerns, make it harder to justify the deployment of the technology on wide segments of the general population.

4. **Procedural safeguards**

   The issues highlighted above are further compounded by the lack of appropriate checks and balances in the deployment of FRTs by state agencies in India. As also acknowledged by the Justice Srikrishna Committee, "*[m]uch intelligence-gathering does not happen under the remit of the law, there is little meaningful oversight that is outside the executive, and there is a vacuum in checks and balances to prevent the untrammeled rise of a surveillance society*" (Justice Srikrishna Committee, 2018). The lack of prior judicial approval and other forms of oversight have led to excessive executive control over what personal data may be accessed, by whom and under what circumstances?[44]

[44] See Bailey, Bhandari, Parsheera, and Rahman (2018) for a discussion on the present legal framework around data access by surveillance and law enforcement agencies in India and challenges with the same.

In this context it would also be relevant to refer to the observations made by the Supreme Court in the context of sharing of Aadhaar related data with enforcement agencies. The majority decision noted that although the disclosure of information in the interest of national security cannot be faulted with, the power to make such decisions should preferably be vested in the hands of a judicial officer.

6.2. Differentiating *R (Bridges) v. South Wales Police*

In September, 2019, a Divisional Bench of the UK High Court delivered its decision in a challenge brought against the live automated facial recognition system being tested by the South Wales Police. The system under challenge allows the police to extract facial biometric data from live CCTV feeds and compare that against a designated watchlist of persons. The claimant challenged the adoption of this system for violation of various UK laws, including requirements under human rights, data protection and equality laws. Upon examination of the issues, the court rejected the case on all the grounds, holding that the two instances in which the system had been tested so far satisfied the requirements under applicable laws.[45]

While the decision represents a worrying precedent that could be seen as strengthening the case for application of FRTs by law enforcement agencies, it is critical to examine some of the key factors that the court took into account while coming to its conclusions. A discussion of this nature is particularly relevant in the Indian context due to the lack of similar safeguards in our system.

Firstly, the UK decision noted that the system in question did infringe on the right to privacy of individuals under Article 8(1) of the European Convention on Human Rights but this infringement satisfied the conditions of lawfulness and fairness. Hence, it constituted a valid basis for interference in the right to privacy. In coming to this conclusion, the court referred to the many legal controls contained in the primary law as well in statutory codes of practice and the standard operating procedures published by the South Wales Police. In particular, these provisions included legal

[45] R (Bridges) v. Chief Constable of South Wales Police and Ors (2019).

obligations relating to the protection of personal data under the Data Protection Act, 2018 and its predecessor law of 1998; and the requirements relating to regulation of CCTV and other surveillance camera technology under the Protection of Freedoms Act, 2012 and the role of the Surveillance Camera Commissioner established under that law. As discussed above, we do not have similar legal protections and oversight mechanisms in India.

Secondly, the UK court relied on the fact that that the deployment of the live facial recognition system by the police was not meant to done in a covert manner. In fact, the standard operating procedures issued by the South Wales Police specifically noted that the face recognition tool would only be used overtly with clear signage to indicate its deployment. In the absence of a legal framework or similar operating procedures in India, we do not have similar guarantees about the FRTs not be used by law enforcement agencies in a covert manner. In this context it would also be important to draw a distinction between situations where the deployment of CCTV cameras might be brought to the attention of the public and those where footage from those cameras could be used for automated facial recognition. In the UK scenario information about both these events was required to be legally provided to the public, which is not the case in India.

Thirdly, it is important to note that the facial recognition system being adopted by the South Wales Police is still at a trial stage. Yet, its adoption has been preceded by documentation such as an initial "Equality Impact Assessment"[46], standard operating procedures and deployment reports to be created in advance of any deployment of the system. Further, the court also relied on the fact that the use of the system by the South Wales Police had been the subject of an independent academic analysis by Cardiff University's Police Science Institute.

[46] The mere existence of such an assessment is however not a sufficient ground to believe that the potential for bias and discrimination in the system had been properly accounted for. For instance, the claimant's submission in this case was that the assessment had failed to account for the higher rates of false positive matches for females and black and minority ethnic faces.

Similar trials of live facial recognition systems are also being carried out in other parts of the UK. Notably, the trials being conducted by the London Metropolitian Police have been the subject matter of an independent review by researchers at the University of Essex Human Rights Centre (Fussey & Murray, 2019) and independent ethical assessment by the London Policing Ethics Panel (Shale, Bowman, Singh, & Wenar, 2019).

The recommendations made by the London Ethics Panel include the suggestion that, given the intrusive nature of the technology, its use should be limited to managing only the more serious offences. Accordingly, the watch list of people whose images are fed into the system should correspond to the seriousness of the offences or expected harm. The panel also emphasised the importance of conducting proper trials before adopting such new technologies and publishing the trial data and evaluations to enable public scrutiny and evaluation.

We clearly do not have parallels of any similar systems of impact assessment or independent review being adopted for facial recognition systems in India. This holds true for existing uses of FRTs by state police authorities for tracking criminals or locating missing children as well as the proposed use in the NAFRS context. Any reliance on the UK decision by courts in India would therefore have to take into account these key differences in the legal and institutional context of the two countries.

As noted in the Cardiff University's report, while automated facial recognition can facilitate efficient policing and enhance public safety, there are also "profound challenges that accompany the adoption of this approach" (Davies, Innes, & Dawson, 2018). These factors include the black boxed nature of the algorithm, increased likelihood of false positives for certain face types, and difficulties in gauging the crime prevention effects of such a system. The same factors are equally relevant in the Indian context. However, the concerns around deployment of FRTs by law enforcement agencies in India are further heightened in our context due to the absence of statutory safeguards, impact assessments and independent oversight and review mechanisms.

6.3. Lessons for FRT adoption in India

The discussions in the preceding sections make it clear that in so far as having a appropriate legal framework is concerned, we are a fair distance away from being able to legitimately adopt FRTs for surveillance and law enforcement purposes. This holds true both in terms of there being no specific legislative authorisation for the use of FRTs by the police and intelligence agencies as well as the lack of a comprehensive data protection law.

Needless to say, any thinking about the need for such a legal framework to authorise the use of FRTs will have to be preceded by a transparent and consultative process. This will require the government to present a clear articulation of the objectives that it seeks to achieve, assessment of the various alternatives and an explanation of why the use of FRTs might constitute a necessary and proportionate response. Stakeholders and the public should be given a meaningful opportunity to provide their inputs on the proposals with an obligation on the government to respond to the suggestions and concerns.

Assuming that following such a process, the government still decides to proceed with the adoption of FRTs for law enforcement purposes, the design of the system will have to incorporate certain necessary checks and balances. The following are some of the suggested provisions that should form part of the primary law. This will, of course, also have to be accompanied by other, more specific, requirements to be contained in binding and enforceable standard operating procedures.

Firstly, the law should narrowly define the boundaries surrounding the use of the facial recognition system, namely the purposes for which it may be used and the persons who images may be used for the probe and gallery databases. One of the ways of achieving this narrow tailoring could be by providing that the use of FRTs would be permissible only pursuant to a judicial order and only in case of investigation of serious offences.[47] For instance, such uses may be limited to cases that relate to cognizable and non-bailable offences.

[47] On a similar note, Microsoft's proposed framework for regulation of FRTs suggests that law enforcement agencies should be permitted to use facial recognition for ongoing surveillance of specified individuals in public spaces only pursuant to a court order or where there is an emergency situation involving danger or death or physical injury (Smith, 2018).

The sources that can be used for the gallery database should also be limited to specific categories of persons instead of being extended to any member of the public, as suggested by the NCRB's tender. For instance, the law may provide that only persons who have previously been convicted, accused or suspected of a offence can be included in the search database. The law may, however, also authorise a judicial authority to sanction the use of any other source of images for matching purposes, if so justified in the facts and circumstances of the case.

Secondly, in situations where FRTs are sought to be used for a specific use case, like finding missing children, the selection of the gallery dataset should be done in a manner that is suited to the needs of that objective. An example of this could be the use of facial recognition for matching the faces of missing children with unidentified children living in children's homes. However, any such use should also be constrained by strict provisions relating to safety and storage of the collected data and limitations on its future uses for other facial recognition tests or for any other purpose.

Thirdly, the law needs to provide for appropriate procedural safeguards and independent oversight mechanisms. In addition to the requirement of judicial review of the decision to adopt FRTs, there should be mechanisms for independent analysis and verification of the performance of FRTs from a legal, technical and ethical perspective. Transparency about the trial process that should precede the deployment of the system, the process of vendor selection, and other accuracy and performance parameters would be some of the essential components of this process.

Finally, the design of the system should provide for a mechanism to track the usage of the facial recognition system. This would include maintaining logs about each application of the system, the results generated in the process, the individuals responsible for assessing those results and the decision taken by them, and the ultimate consequences of the action. This sort of mechanism would be useful for auditing purposes and to ensure accountability of the individuals who are responsible for applying the automated face recognition system.

7. Conclusion

The growing use of facial recognition systems is being prompted by motives like enhanced security, convenience and efficiency across multiple use cases. Yet, their unchecked use, particularly by government agencies, poses a number of serious challenges around privacy, transparency, accuracy, bias and lack of adequate accountability mechanisms. This situation raises some difficult questions. On one hand, there is the imminent threat that widespread deployment of FRTs poses to individual and community rights, which might be impossible to rectify in future. On the other, is the concern that while some of the potential benefits of facial recognition systems are currently known, others may come to light only as the technology evolves further. Would it then be appropriate to stifle future innovation by banning the use of a technology that is still in a nascent stage of development?

Clearly, neither one of these extremes, of total prohibition or rampant unchecked deployment, is a suitable one. The challenge therefore lies in finding an appropriate mix of policy tools for a solution that lies somewhere in between these extremes. Based on currently available knowledge, a suggested option would be to find ways to isolate the most "troubling" use cases of FRTs – such as, its large scale use by government agencies for surveillance and law enforcement purposes – from some of the more targeted ones. We therefore need to develop appropriate standards for each of these situations, starting with the minimum basic requirement of having a comprehensive data protection framework.

As and when India adopts a data protection law, that would determine a basic level of protection for the use of facial biometrics by private parties and the state. This would include requirements relating to explicit consent, transparency obligations, purpose limitation and other usage restrictions. However, a data protection framework will not in itself be able to secure the degree the accountability that we need from the range of stakeholders participating in the implementation of FRTs.

For instance, provisions under a data protection law are not likely to compel the developers and vendors of facial recognition systems to ensure transparency about their underlying models, training data that was used, false positive and negative rates and other more granular information. Yet, information of this sort is necessary for there to be any independent checks and analysis on the accuracy, reliability and biases in the systems and to facilitate more India-centric studies on the use and impact of FRTs. We therefore need to look beyond data protection laws to find meaningful ways of ensuring transparency and public disclosure on the development and use of facial recognition systems.

When it comes to deployment of FRTs by state agencies, that will necessarily have to satisfy the tests laid down by the Supreme Court in the *Puttaswamy* case. This will be the case irrespective of whether the technology is to be used for implementing a national level automated facial recognition system for law enforcement purposes or marking attendance of students and teachers in government schools. Further, the adoption of any such measure should be preceded by a transparent and consultative process that would compel the government to closely examine the pros and cons of the intended move.

Focusing, in particular, on the NCRB's tender, we demonstrate how the proposed design of the facial recognition system falls grossly short of satisfying the constitutional safeguards. In short, the system lacks legal authorisation; it does not constitute a necessary and proportionate intervention to meet the desired objectives; and there is a complete absence of procedural safeguards to ensure fair and reasonable application.

Before law enforcement bodies in India can make use of FRTs, the Parliament will have to authorise the same through an appropriate legal framework. Some of the basic checks and balances of such a framework would include, narrow tailoring of the purposes for which the system may be deployed and the persons who images may be used for the probe and gallery databases; prior judicial approval for the use of the system; and inbuilt mechanisms for independent analysis and verification of the system's performance.

As a final note, while the paper highlights several challenges with the current accuracy and reliability of facial recognition systems, it is likely that technology will eventually evolve to a state that can overcome many of these concerns. This makes it necessary to reiterate that satisfactory performance of FRTs is only a necessary, but not sufficient, pre-condition for the deployment of such systems. Its use has to be supported, in all cases, by a robust framework for gauging the suitability and proportionality of using FRTs in any given context. At the same time, we also need broader, inter-disciplinary, studies that look beyond individual use cases to evolve a deeper understanding of how personalities and societies are likely to be reshaped under the ubiquitous gaze of facial recognition systems.

References

Acquisti, A., Gross, R., & Stutzman, F. (2014). Face recognition and privacy in the age of augmented reality. *Journal of Privacy and Confidentiality,* 6(2).

Algorithm Watch. (2019). Ai ethics guidelines global inventory. Retrieved from https://algorithmwatch.org/en/project/ai-ethics-guidelines-global-inventory/

Amber Tickoo v. Government of NCT of Delhi. (2017). Supreme Court of India, W.P.(C) No. 570/2019 (pending case).

Bailey, R., Bhandari, V., Parsheera, S., & Rahman, F. (2018, August). Use of personal data by intelligence and law enforcement agencies. Macro/Finance Group, NIPFP. Retrieved from http://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf

Belot, H. (2018). Government's facial recognition scheme could be abused, lawyers warn. Retrieved from https://www.abc.net.au/news/2018-05-03/facial-recognition-scheme-could-be-abused-law-council/9723494

Bhandari, V., Kak, A., Parsheera, S., & Rahman, F. (2017, September). An analysis of puttaswamy: the supreme court's privacy verdict. Retrieved from https://bit.ly/2Mxb3Pi

Bhattacharya, A. (2018). The number of smartphone users in india will more than double in four years. Retrieved from https://qz.com/india/1483368/indias-smartphone-internet-usage-will-surge-by-2022-cisco-says/

Bilchitz, D. (2014). Necessity and proportionality: towards a balanced approach? In L. Lazarus, C. McCrudden, & N. Bowles (Eds.), *Reasoning rights.* Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2320437

Brewster, T. (2018). We 3d printed our heads to bypass facial recognition security and it worked. Retrieved from https://www.forbes.com/video/5978671815001/#4cccb6e22461

Bromby, M. (2002). To be taken at face value? computerised identification. *Information & Communication Technology Law,* 11(1). Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1561523

Buolamwin, J. & Gebru, T. (2018). Gender shades: intersectional accuracy disparities in commercial gender classification. Retrieved from http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

CB Insights. (2018). China: facial recognition capital of the world. Retrieved from https://www.cbinsights.com/research/china-facial-recognition-capital-of-the-world/

CDT. (2012). Seeing is id'ing: facial recognition & privacy. Retrieved from https://cdt.org/files/pdfs/Facial_Recognition_and_Privacy-Center_for_Democracy_and_Technology-January_2012.pdf

Daly, A. (2017). Covering up: american and european legal approaches to public facial anonymity after s.a.s. v france. In T. Timan, B. C. Newell, & B.-J. Koops (Eds.), *Privacy in public space: conceptual and regulatory challenges.* Elgar Law Technology and Society.

Daniel George v. Government of NCT of Delhi. (2017). Delhi High Court, WP (Civ). No. 7083/2018 (pending case).

Davies, B., Innes, M., & Dawson, A. (2018). An evaluation of south wales police's use of automated facial recognition. Retrieved from https://www.statewatch.org/news/2018/nov/uk-south-wales-police-facial-recognition-cardiff-uni-eval-11-18.pdf

D-ID. (2019). D-id product overview. Retrieved from https://www.deidentification.co/wp-content/uploads/2019/03/D-ID-Product-Overview.pdf

Dolgin, E. (2019). Ai face-scanning app spots signs of rare genetic disorders. Retrieved from https://www.nature.com/articles/d41586-019-00027-x

DoT. (2019). Instruction for alternate digital kyc process for issuing new mobile connections to subscriber. Retrieved from http://dot.gov.in/sites/default/files/Digital%5C%20KYC%5C%20instructions_03042019.PDF

EDPB. (2019). Facial recognition in school renders sweden's first gdpr fine. Retrieved from https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en

Feldstein, S. (2019, September). The global expansion of ai surveillance. Retrieved from https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

Fox, J. C. (2019). Brown university student mistakenly identified as sri lanka bombing suspect. Retrieved from https://www.bostonglobe.com/metro/2019/04/28/brown-student-mistaken-identified-sri-lanka-bombings-suspect/0hP2YwyYi4qrCEdxKZCpZM/story.html

Funk, A. (2019). I opted out of facial recognition at the airport – it wasn't easy. Retrieved from https://www.wired.com/story/opt-out-of-facial-recognition-at-the-airport/

Fussey, P. & Murray, D. (2019). Independent report on the london metropolitan police service's trial of live facial recognition technology. Retrieved from https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf

Future of Privacy Forum. (2018). Understanding facial detection, characterization and recognition technologies. Retrieved from https://fpf.org/wp-content/uploads/2018/09/FPF_FaceRecognitionPoster_R5.pdf

Garvie, C., Bedoya, A., & Frankle, J. (2016). The perpetual lineup. Retrieved from https://www.perpetuallineup.org/%5C#introduction

Grgic, M. & Delac, K. (2019). Databases. Retrieved from http://www.face-rec.org/databases/

Grother, P., Ngan, M., & Hanaoka, K. (2019). Ongoing face recognition vendor test (frvt) part 2: identification. Retrieved from https://doi.org/10.6028/NIST.IR.8238

Gupta, A. (2019). Legal notice to recall the request for proposal for "automated facial recognition sysytem". Retrieved from https://drive.google.com/file/d/1XNeqiyjCF0KWbiZB5mRUCtVyyxU2wj2v/view

Gupta, K. (2019). Nasscom's suggestions to address the kyc challenges faced by prepaid payment instruments. Retrieved from https://community.nasscom.in/communities/policy-advocacy/nasscoms-suggestions-to-address-the-kyc-challenges-faced-by-prepaid-payment-instruments-ppis.html

Hamburg Data Protection Commissioner. (2018, December). Order on the use of the facial recognition software "videmo 360" by the hamburg police to investigate criminal offenses in connection with the g20 summit in hamburg. Retrieved from https://datenschutz-hamburg.de/assets/pdf/Anordnung_HmbBfDI_2018-12-18.pdf

Hartzog, W. (2018). Facial recognition is the perfect tool for oppression. Retrieved from https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66

Hoffmann, A. L. (2019). Where fairness fails: data, algorithms, and thelimits of anti discrimination discourse. *Information, Communication & Society,* 22(7). Retrieved from https://doi.org/10.1080/1369118X.2019.1573912

Huang, T., Xiong, Z., & Zhang, Z. (2011). Face recognition applications. In S. Z. Li & A. K. Jain (Eds.), *Handbook of face recognition* (Second).

India Today. (2018). Tamil nadu schools to launch facial recognition app to replace attendance registers. Retrieved from https://www.indiatoday.in/education-today/news/story/tamil-nadu-schools-facial-recognition-app-attendance-registers-artificial-intelligence-divd-1406813-2018-12-11

Introna, L. D. & Nissenbaum, H. (2010). Facial recognition technology: a survey of policy and implementation issues. Retrieved from https://www.researchgate.net/publication/228275071

ISO/IEC. (2011). 19794-5:2011 – information technology – biometric data interchange formats – part 5: face image data. International Organization for Standardization and International Electrotechnical Commission. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:19794:-5:ed-2:v1:en

Jeelani, G. (2019). Big brother's watching you: aap govt's mega project to install about 3 lakh cctv cameras. Retrieved from https://www.indiatoday.in/mail-today/story/big-brother-s-watching-you-aap-govt-s-mega-project-to-install-about-3-lakh-cctv-cameras-1571748-2019-07-21

Justice KS Puttaswamy (Retd.) and Anr v. Union of India and Ors. (2017). Supreme Court of India, WP (Civ). No. 494/2012.

Justice KS Puttaswamy (Retd.) and Anr v. Union of India and Ors. (2018). Supreme Court of India, WP (Civ). No. 494/2012. Retrieved from https://www.sci.gov.in/supreme-court/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

Justice Srikrishna Committee. (2018, July). A free and fair digital economy: protecting privacy, empowering indians. Report of the Committee of Experts under the Chairmanship of Justice B. N. Srikrishna. Retrieved from http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

Kattia, H. & Aruna, S. (2018). Are you from north or south india? a hard race classification task reveals systematic representational differences between humans and machines. Retrieved from https://arxiv.org/pdf/1703.07595.pdf

Keyes, O. (2018). The misgendering machines: trans/hci implications of automatic gender recognition. Retrieved from https://dl.acm.org/citation.cfm?id=3274357

Khoya-Paya. (2019). Facial recognition system helps trace 3,000 missing children in 4 days. Retrieved from http://khoyapaya.gov.in/mpp/dashboard

Kind, C. (2019). Biometrics and facial recognition technology – where next? Retrieved from https://www.adalovelaceinstitute.org/biometrics-and-facial-recognition-technology-where-next/

Kraus, R. (2019). Microsoft refused to sell facial recognition tech to law enforcement. Retrieved from https://me.mashable.com/tech/4207/microsoft-refused-to-sell-facial-recognition-tech-to-law-enforcement

Kulche, P. (2019). Facial recognition on smartphone is not always safe. Retrieved from https://www.consumentenbond.nl/veilig-internetten/gezichtsherkenning-te-hacken

Li, S. Z. & Jain, A. K. (2011). Introduction. In S. Z. Li & A. K. Jain (Eds.), *Handbook of face recognition* (Second).

Lin, J. (2019). The curious case of toilet paper and facial recognition. Retrieved from https://uxdesign.cc/the-curious-case-of-toilet-paper-and-facial-recognition-c204c701fd0f

Lu, Y., Zhou, J., & Yu, S. (2003). A survey of face detection, extraction and submission. *Computing and Informatics, 22.*

Lynch, J. (2018). Face off: law enforcement use of facial recognition technology. Retrieved from https://www.eff.org/wp/law-enforcement-use-face-recognition

Mahajan, S. (2019). Do cctv cameras in classrooms violate right to privacy? supreme court to decide. Retrieved from https://barandbench.com/cctv-cameras-classrooms-right-privacy-supreme-court-notice-delhi-govt/

Manish, S. (2018). India's passport revolution: how millions of citizens got the blue book. Retrieved from https://www.business-standard.com/article/economy-policy/india-s-passport-revolution-how-millions-of-citizens-got-the-blue-book-118073100814_1.html

Marda, V. (2019). Facial recognition is an invasive and inefficient tool. Retrieved from https://www.thehindu.com/opinion/op-ed/facial-recognition-is-an-invasive-and-inefficient-tool/article28629051.ece

Metz, R. (2019). Beyond san francisco, more cities are saying no to facial recognition. Retrieved from https://edition.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html

Microsoft. (2018). Six principles for developing and deploying facial recognition technology. Retrieved from https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2018/12/MSFT-Principles-on-Facial-Recognition.pdf

Ministry of Road Transport and Highways. (2019). Bulk data sharing policy & procedure. Retrieved from https://parivahan.gov.in/parivahan/sites/default/files/NOTIFICATION%26ADVISORY/8March%202019.pdf

MoCA. (2019). Digi yatra: reimagining air travel in india. Retrieved from http://civilaviation.gov.in/sites/default/files/Digi%5C%20Yatra%5C%20Policy%2009%5C%5C%20Aug%5C%2018.pdf

Monroy, M. (2019). Face recognition after g20: police in hamburg laughs at data protection commissioner. Retrieved from https://digit.site36.net/2019/09/19/face-recognition-after-g20-police-in-hamburg-laughs-at-data-protection-commissioner/

Moosa, A. (2019). A comprehensive guide to facial recognition algorithms. Retrieved from https://www.baseapp.com/computer-vision/a-comprehensive-guide-to-facial-recognition-algorithms/

Morozov, E. (2013). *To save everything click here: the folly of technological solutionism.* Public Affairs.

Murali, A. (2018). The big eye: the tech is all ready for mass surveillance in india. Retrieved from https://factordaily.com/face-recognition-mass-surveillance-in-india/

NCRB. (2018). Finger print analysis and criminal tracing system. Retrieved from http://ncrb.gov.in/BureauDivisions/CFPB/facts.aspx

NCRB. (2019). Request for proposal to procure national automated facial recognition system. Retrieved from http://ncrb.gov.in/TENDERS/AFRS/RFPNAFRS.pdf

NEC. (2019). Face recognition. Retrieved from https://www.nec.com/en/global/solutions/safety/face_recognition/PDF/NeoFace_Watch_Brochure.pdf

NIST. (2019). Frvt 1:n identification. Retrieved from https://www.nist.gov/programs-projects/frvt-1n-identification

O'Toole, A. (2011). Face recognition by humans and machines. In S. Z. Li & A. K. Jain (Eds.), *Handbook of face recognition* (Second).

Park, U. & Jain, A. K. (2011). Face aging modeling. In S. Z. Li & A. K. Jain (Eds.), *Handbook of face recognition* (Second).

Parsheera, S., Catania, P., Cording, S., Cortiz, D., Donna, M., Lee, K., & van Wijngaarden, A. (2019). Fairness and non-discrimination. In C. Morgan (Ed.), *Responsible ai: a global policy framework,* (1st ed.). ITechLaw.

Pearson, J. (2015). Churches are using facial recognition to track members, this startup says. Retrieved from https://www.vice.com/emus/article/z4mdv5/churches-are-using-facial-recognition-to-track-members-this-startup-says

Phillips, P. J., Jiang, F., Narvekar, A., Ayyard, J., & O'Toole, A. (2011). An other-race effect for face recognitionalgorithms. *ACM Transactions on Applied Perception,* 8(2). Retrieved from https://dl.acm.org/citation.cfm?id=1870082

Phillips, P. J. & Newton, E. M. (2002). Meta-analysis of face recognition algorithms. *Proceedings of the Fifth IEEE International Conference on Automatic Face and Gesture Recognition.* Retrieved from https://ieeexplore.ieee.org/document/1004160

Piza, E. L., Welsh, B. C., Farrington, D. P., & Thomas, A. L. (2019). Cctv surveillance for crime prevention: a 40-year systematic review with meta-analysis. *Criminology & PublicPolicy, 18.* Retrieved from https://doi.org/10.1111/1745-9133.12419

Prasanna, L., Bhosale, S., D'Souza, A., Mamatha, H., Thomas, R., & Sachin, K. (2013). Facial indices of north and south indian adults: reliability in stature estimation and sexual dimorphism. *Journal of Clinial & Diagnostic Work,* 7(8). Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3782890/

PTI. (2017). Attendance woes? iit delhi resorts to beacons, smart phones. Retrieved from https://www.indiatoday.in/pti-feed/story/attendance-woes-iit-delhi-resorts-to-beacons-smart-phones-911199-2017-04-19

PTI. (2018a). Delhi police tells high court it requires more information from centre on missing children. Retrieved from https://www.firstpost.com/india/delhi-police-tells-high-court-it-requires-more-information-from-centre-on-missing-children-4443161.html

PTI. (2018b). Facial recognition system helps trace 3,000 missing children in 4 days. Retrieved from http://timesofindia.indiatimes.com/articleshow/63870129.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

PTI. (2019a). Police facial recognition software glitchy: centre. Retrieved from https://www.thehindu.com/news/cities/Delhi/police-facial-recognition-software-glitchy-centre/article29237850.ece

PTI. (2019b). "what special privacy": delhi court over opposition to classroom cctvs. Retrieved from https://www.ndtv.com/delhi-news/what-special-privacy-delhi-high-court-over-opposition-to-classroom-cctvs-2079009

Quackenbush, C. (2019). A run on gas masks: hong kong protesters circumvent crackdown on protective gear. Retrieved from https://www.washingtonpost.com/world/asia_pacific/a-run-on-gas-masks-hong-kong-protesters-circumvent-crackdown-on-protective-gear/2019/08/15/2c543030-be57-11e9-b873-63ace636af08_story.html?noredirect=on

R (Bridges) v. Chief Constable of South Wales Police and Ors. (2019). High Court of Justice (Queen's Bench Division), [2019] EWHC 2341 (Admin).

Raj, S. N. & Niar, V. (2017). Comparison study of algorithms used for feature extraction in facial recognition. *International Journal of Computer Science and Information Technologies,* 8(2). Retrieved from http://ijcsit.com/docs/Volume%208/vol8issue2/ijcsit2017080205.pdf

Raji, I. D. & Buolamwin, J. (2019). Actionable auditing: investigating the impact of publicly naming biased performance results ofcommercial ai products. Retrieved from http://www.aies-conference.com/wp-content/uploads/2019/01/AIES-19_paper_223.pdf

Reflectacles. (2019). Irpair. Retrieved from https://www.reflectacles.com/irpair

Rollet, C. (2018). China public video surveillance guide: from skynet to sharp eyes. Retrieved from https://ipvm.com/reports/sharpeyes

Romaniuk, S. N. & Burgers, T. (2018). How china's ai technology exports are seeding surveillance societies globally. Retrieved from https://thediplomat.com/2018/10/how-chinas-ai-technology-exports-are-seeding-surveillance-societies-globally/

Sathe, G. (2018). Cops in india are using artificial intelligence that can identify you in a crowd. Retrieved from https://www.huffingtonpost.in/2018/08/15/facial-recognition-ai-is-shaking-up-criminals-in-punjab-but-should-you-worry-too_a-23502796/

Schneier, B. (2013). The public/private surveillance partnership. Retrieved from https://www.schneier.com/blog/archives/2013/08/the_publicpriva_1.html

Senior, A. W. & Bolle, R. M. (2002a). Face recognition and its application. In D. D. Zhang (Ed.), *Biometric solutions: for authentication in an e-world.* Retrieved from http://andrewsenior.com/papers/SeniorB02FaceChap.pdf

Senior, A. W. & Bolle, R. M. (2002b). Face recognition and its application. In D. D. Zhang (Ed.), *Biometric solutions: for authentication in an e-world.* Springer Science and Business Media. Retrieved from http://andrewsenior.com/papers/SeniorB02FaceChap. pdf

Senior, A. W. & Pankanti, S. (2011). Privacy protection and face recognition. In S. Z. Li & A. K. Jain (Eds.), *Handbook of face recognition* (Second).

Shale, S., Bowman, D., Singh, P., & Wenar, L. (2019). Final report on live facial recognition. Retrieved from http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lfr_final_report_-_may_2019.pdf

Sharma, N. (2019). Indian smartphone brands are crumbling under pressure from chinese players. Retrieved from https://qz.com/india/1623686/indian-smartphone-brand-intex-may-die-due-to-chinas-xiaomi-oppo/

Sharma, R. (2019). Facial-recognition attendance system: it is fool-proof, has no scope for manipulation, says gujarat's education secretary. Retrieved from https://indianexpress.com/article/education/facial-recognition-attendance-system-it-is-fool-proof-has-no-scope-for-manipulation-says-education-secretary-5925570/

Shen, X. (2018). What is skynet? Retrieved from https://www.abacusnews.com/who-what/skynet-chinas-massive-video-surveillance-network/article/2166938

Smith, B. (2018). Facial recognition: it's time for action. Retrieved from https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/

Snow, J. (2018). Amazon's face recognition falsely matched 28 members of congress with mugshots. Retrieved from https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

Solon, O. (2019). Facial recognition's 'dirty little secret': millions of online photos scraped without consent. Retrieved from https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921

Statista. (2019). Leading countries based on number of facebook users as of july 2019 (in millions). Retrieved from https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/

UIDAI. (2018). Implementation of face authentication. Retrieved from https://uidai.gov.in/images/resource/Uidai_circular_Face_authentication_15012018.pdf

UIDAI. (2019). Aadhaar paperless offline e-kyc. Retrieved from https://uidai.gov.in/ecosystem/authentication-devices-documents/about-aadhaar-paperless-offline-e-kyc.html

Vidyut. (2018). Police surveillance: arbitrary, unchecked and growing. Retrieved from https://aamjanata.com/digital-india/police-surveillance-arbitrary-unchecked-growing/.

Wagner, K. (2013). Facebook has a quarter of a trillion user photos. Retrieved from https://mashable.com/2013/09/16/facebook-photo-uploads/

Waldrop, T. (2019). Sri lanka bans all face coverings for 'public protection' after bomb attacks. Retrieved from https://edition.cnn.com/2019/04/29/asia/sri-lanka-face-coverings-ban/index.html

Welinder, Y. (2012). A face tells more than a thousand posts: developing face recognition privacy in social networks. *Harvard Journal of Law & Technolog,* 26(1).

Whitener, M. & Aragon, R. (2019). How should we regulate facial-recognition technology? Retrieved from https://iapp.org/news/a/how-should-we-regulate-facial-recognition-technology/

Whittaker, Z. (2019). Amazon shareholders reject facial recognition sale ban to governments. Retrieved from https://techcrunch.com/2019/05/22/amazon-reject-facial-recognition-proposals/

Zhou, S. & Xiao, S. (2018). 3d face recognition: a survey. Retrieved from https://doi.org/10.1186/s13673-018-0157-2

Acknowledgements

The author would like to thank Ajay Shah, Ambuj Sagar, Apar Gupta, Christopher Slobogin, Elizabeth Coombs, Salil Tripathi, an anonymous peer reviewer and all participants at the Data Governance Network roundtable held in New Delhi on 4 September, 2019 for valuable inputs and comments. All errors are her own.

About the Author

The author is a Fellow at the National Institute of Public Finance and Policy.

🌐 datagovernance.org ✉ dgn@idfcinstitute.org

@datagovnetwork /datagovnetwork /datagovnetwork