DGN Policy Brief 05
January 2020
Data Governance Network

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

Smriti Parsheera

The widespread adoption of facial recognition technologies (FRTs) by the public and private sectors, without any meaningful debate or regulation, raises a number of concerns. Any adoption of this technology has to be preceded by a meaningful suitability and proportionality analysis, taking into account the concerns of accuracy, reliability, privacy, transparency and bias as well as the need for appropriate procedural safeguards.

1. Introduction

Automated facial recognition is a form of biometric analysis that can be used for identifying or verifying human beings from photographs, videos or in real time. A typical deployment involves the creation of a mathematical representation of a person's face, which can then be used for comparison against a gallery of existing images.

Given the intrinsic link between a person's face and their identity, the widespread adoption of FRTs without any real checks and balances raises a number of concerns. These concerns revolve around the lack of transparency around the use of facial recognition systems; their implications for privacy and civil liberties; and evidence of bias and dis- crimination 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.

All of this holds true for the use of FRTs by the government as well as private entities. However, the imbalance of power between the citizen and the state and the likely consequences from its abuse make it particularly relevant to question the use of FRTs for law enforcement purposes. An analysis of the state's use of FRTs also becomes necessary in light of the Supreme Court's verdict in the Puttaswamy right to privacy decision.
Applications in the Indian context

2. Application in the Indian context

Some of the known commercial uses of FRTs include photo tagging suggestions on social media, biometric unlocking of mobile phones and digital signage systems that display customised advertising based on the gazer's profile. Be- sides its increasing commercial deployment, government interest in FRTs is also growing, specifically in the context of surveillance and law enforcement related uses. The following are some of the notable discussions around the use of facial recognition systems in the Indian context.

National Automated Face Recognition System – In June, 2019, the National Crime Records Bureau (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 National Automated Face Recognition System (NAFRS) (NCRB, 2019). The purposes for which the system is proposed to be used include identification of criminals, missing children and persons and unidentified dead bodies.

The sources of probe and gallery images will include im- ages held by passport authorities, the Central Finger Print Bureau and the government's missing children tracking portal. However, this list also contains a sweeping category for "any other image database available with police / other entity". This seems to suggest that virtually each and every data- base in the country could potentially be linked with this system.

Aadhaar authentication and KYC – 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, to be used in combination with other modes of authentication (UIDAI, 2018). Through subsequent circulars the UIDAI mandated telecom service providers to start under- taking face authentication of their subscribers.

Pursuant to the Supreme Court's verdict in the *Puttaswamy* Aadhaar case, it is no longer possible for the government to mandate Aadhaar based face authentication by private entities like banks and telecom companies. The amended Aadhaar Act has, however, introduced the concept of an offline identity verification system using an eXtensible Markup Language (XML) file. This can be accompanied by "*face validation by capturing face and matching against the photo within the e-KYC XML*" (UIDAI, 2019). This suggests that businesses would have the discretion to conduct such validation through manual or automated facial recognition techniques.

Consumer applications and devices – India has over 270 million Facebook users, which makes it a significant contributor to the company's massive deployment of FRTs for tagging of photos that are uploaded on its platform. The use of face recognition for biometric unlocking on mobile devices is another emerging use case. Given the user profile and characteristics of the Indian market, reliance on facial unlocking techniques on low-end mobile phones could create increased security vulnerabilities for consumers. A recent study found that 24 out of the 60 tested smartphones could be unlocked by putting the phone owner's in front of the camera (Kulche, 2019). In another test, many devices were found to be vulnerable to a more sophisticated technique of unlocking using a 3D model of the owner's head (Brewster, 2018).

Airport check-in and security – In 2018, the Ministry of Civil Aviation launched the "Digi Yatra" project that pro- poses to create a facial biometrics based boarding system at airports (MoCA, 2019). Testing under the project, which is currently voluntary, has been going on at the Hyderabad, Bengaluru and Delhi airports. 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.

Attendance systems – Another oft-cited use of face recognition is for creating automated attendance systems. For ex- ample, Delhi's Indian Institute of Technology has a home-grown solution called Timble that is used to mark student 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 (Sharma, 2019).

In a related fact situation under the General Data Protection Regulation (GDPR), the Swedish Data Protection Authority struck down the adoption of FRTs by a school in northern Sweden. The Authority observed that obtaining the con- sent of the students or their parents could not be a valid legal basis for such processing, given the clear imbalance between the data subject and the controller (EDPB, 2019).

In each of the use cases discussed above, the use of FRTs can be traced to the pursuit of goals like increased efficiency, security, convenience or accountability. However, there has been no systematic evaluation of the costs and benefits of using FRTs in any of these contexts. The adoption of the technology has also not been preceded by any public discussions or consultations. Moreover, all of these developments are taking place in the absence of a robust data protection law in the country.

While the current Information Technology Act, 2000 and the rules under it classify biometric data as "sensitive personal data", the scope and implementation of the law re- mains grossly inadequate. Further, the obligations under the present law are applicable only to "body corporates", hence excluding most instances where government agencies interact with biometric facial data.

3. What are the key policy concerns?

The primary focus of most of the technical research on face recognition has been on improving the accuracy and efficiency of the technology. 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, false negatives in a system like Aadhaar would lead to the exclusion of legitimate beneficiaries while a false positive in the surveillance and law enforcement context can 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 still poses a number of serious concerns, from a legal, ethical and societal perspective.

Transparency – There is a lack of meaningful information about when, or the specific purposes for which, FRTs are being deployed; sources of training data and gallery images; criteria for the selection of the technology partner; applicable privacy and security protocols and accuracy rates. Information of this sort is necessary to ensure that the principles of natural justice are followed in criminal investigations (Trivedi & Wessler, 2019). More broadly, better transparency would also enable independent testing and audit of facial recognition systems (Smith, 2018).

Data protection laws like the GDPR and the draft personal data bill in India seek to provide a basic level of notice and transparency to enable the exercise of meaningful choice by individuals. The effectiveness of this choice, however, remains questionable in all contexts, particularly in cases of data processing by the government. Moreover, data protection provisions are also 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 FRTs.

Privacy and civil liberties – The unchecked use of FRTs poses a real and immediate threat to privacy and other civil liberties. The main issue with biometrics is that they are unique to each of us and cannot be changed. A person's face, in particular, is exposed at all times, which makes it much more difficult to prevent the collection of one facial images (Lynch, 2018).

In addition, widespread use of FRTs can also create a chilling effect on the liberty, movement and speech rights of individuals. Visuals of masked protesters in Hong Kong taking down smart lamp posts and surveillance cameras are symbolic of this tussle between the state's use of surveillance technologies and counter-measures being resorted to by protesters. As governments chose to respond to such situations with "anti-mask initiatives" this would affect not only the rights of protesters' but also those who may adopt facial coverings for various religious, cultural or practical reasons.

The widespread commercial deployment of the technology also poses several privacy concerns. For instance, it has been noted that the use of FRTs by platforms like Face- book 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). Researchers have also shown how a person's face can easily be used as a personal identifier for pooling together information about them from multiple online sources – like dating websites and social media portals – where the per- son might want to reveal their true identity in one context but remain anonymous in others (Acquisti, Gross, & Stutz- man, 2014).

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. Results of FRTs are therefore prone to errors on account of differences in the conditions of the images being compared, in terms of appearance, ex- pression age, lighting, camera angle, etc. (Senior & Bolle, 2002; Lu, Zhou, & Yu, 2003; Li & Jain, 2011). This is particularly true in cases where the technology is applied in non- cooperative settings, for instance, using images gathered from a closed circuit television (CCTV) camera or for real- time biometric processing. For instance, a study on the live facial recognition system being tested

by the London Metropolitan Police 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 (Fussey & Murray, 2019).

Having said that, it is important to acknowledge that there have been significant leaps in the technical capabilities of FRTs in recent years. For instance, many of the technical issues listed above are less likely to affect the results of 3D facial recognition systems compared to the more pre- valent 2D systems (Zhou & Xiao, 2018). As per the National Institute of Standards and Technology (NIST), the "*best performing algorithms*" in its 2018 Face Recognition Vendor Testing Program have shown significant improvements over the 2015 test results and can now offer "*close to perfect recognition*". Yet, there still remain significant vari- ations 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*" (Grother, Ngan, & Hanaoka, 2019). Satisfactory performance of FRTs is, however, only a necessary, but not sufficient, pre-condition for the deployment of such systems.

Bias and discrimination – The training data being used by FRTs 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++ showed much higher error rates for women with darker skin tones. This difference arose primarily on account of the under- representation of data belonging to this group in the training dataset. Similarly, a study done by the American Civil Liberties Union using Amazon Rekognition found that nearly 40 percent of the false face matches between members of the US Congress and a database of arrested persons were of people of color. In contrast, only about 20 percent of the Congress members actually belonged to this demographic group (Snow, 2018). While most of this research has emanated in the US context, it is easy to draw some parallels with the challenges that would arise in the deployment of similar systems in India's multi-racial, multi-ethic set up.

Research of this nature is valuable in that it can serve as the basis for making appropriate fixes to the training data and algorithms. However, it has been rightly 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). For instance, Keyes (2018) challenges 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 certain groups, like transgendered persons, who may not fit into the traditionally defined gender constructs.

Limitations of the supporting ecosystem – Another import- ant factor, particularly in the Indian context, is the relevance of the surrounding ecosystem within which FRTs are 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 the context of Aadhaar.

4. What are the debates around regulation?

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 these concerns cannot be addressed through self-regulation (Hartzog, 2018). In particular, such bans or restrictions are being called for in the context of government use of facial recognition systems. Some organisations are, however, advocating

for a broader, but voluntary, moratorium on all future public and private sector deployment of FRTs (Kind, 2019).

However, the more dominant narrative, at present, revolves around the formulation of ethical frameworks to address is- sues such as, privacy, security, accuracy, transparency and bias in the use of FRTs. Within this, there are variations where the responsibility of developing and adhering to eth- ical principles is proposed to be left primarily to the developers and users of the technology or where the government plays a more active role in setting out these principles and monitoring their compliance.

At the other extreme of the spectrum lies the view that the growth of emerging technologies like facial recognition should not be stifled though premature regulation. How- ever, in practical terms, a "no regulation" framework may not really be feasible as there seems to be growing con- vergence 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 (AI). Many of these strategy documents speak of the need for ethical and responsible development of AI-based systems. Notably, any move towards the regulation of FRTs will be shaped by the complex interactions between the government and the private sector in the development and use of facial recognition. With governments themselves being major consumers of FRTs, they have a key role to play in the adoption and technical advancements of the techno- logy. Calls for strengthened regulatory interventions in this space will therefore end up curtailing the government's own powers and surveillance capabilities, making it harder to expect such a decision.

In terms of regulatory and judicial precedents, so far there have only been a handful of developments around the use of FRTs. One of these relates to the ban on the use of FRTs by the city of San Francisco. Notably, the definition of department in the San Francisco ordinance excludes the District Attorney or the Sheriff while performing their investigation or prosecution functions. While the understanding on the ground seems to be that all government agencies are barred from using FRTs, the text of the law suggests that there may be a possibility for particular agencies to resort to the use of FRTs under necessary circumstances. Similar bans have been adopted in a few other municipal laws in addition to which a few states in the US have also adopted specific laws to ban the use of FRTs in body cameras worn by police officials. There have also been two notable cases on the use of FRTs for law enforcement. The first case stems from an order passed by the Hamburg Data Protection Commissioner that is currently under challenge before an administrative court in Germany. In its order the Hamburg Commissioner had directed the deletion of a database created by the po- lice for the identification of rioters who participated in the G20 protests in the city. As per the Commissioner, the system involved the processing of the personal data of thou- sands of uninvolved persons against whom there was no specific suspicion of being involved in the riots. The Commissioner noted that there was no legal basis for such pro- cessing (Hamburg Data Protection Commissioner, 2018).

The other case relates to the decision of a divisional bench of the UK High Court in R (Bridges) v. Chief Constable of South Wales Police and Ors (2019). In this case the court upheld the validity of a live facial recognition system being tested by the South Wales Police. The system allowed the police to extract facial biometric data from live CCTV feeds and compare that against a designated watchlist of persons. The claimant argued that the adoption of this system violated UK's human rights, data protection and equality laws. The court, however, rejected these claims, holding that the two instances in which the system had so far been tested satisfied the requirements under applicable laws.

While the decision represents a worrying precedent that could be seen as strengthening the application of FRTs by law enforcement agencies, it is critical to note that the decision of the UK court was based on the existence of various statutory safeguards, impact assessments and independent oversight and review mechanisms under UK laws. As we discuss below, we do not have any similar safeguards in our system. This

holds true for existing uses of FRTs by state police authorities as well as the proposed use under the NAFRS tender.

5. 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. The court held that even though privacy is not an absolute right, any state interference in the right to privacy can only be done in a manner that is "*fair, just and reasonable*". This requires that any restriction on privacy should satisfy 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, there need to be appropriate procedural guarantees to check against the abuse of state power (See Bhandari, Kak, Parsheera, and Rahman (2017)). The scope of the proportionality test was further clarified by the Supreme Court in the Aadhaar case to include the requirements of *necessity* – there being no less restrictive but equally effective alternative and *balancing* – no disproportionate impact on the right holder.

The legitimacy of the facial recognition system proposed under the NCRB tender has already being questioned in a notice sent by the Internet Freedom Foundation to the NCRB and the Ministry of Home Affairs (Gupta, 2019). The notice points to the lack of any statutory basis for the creation of such a system. It also challenges the fact that proposed system 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 this context, following are some of the key factors to be considered while examining the NAFRS proposal through the *Puttaswamy* lens.

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 does not have any statutory basis. Neither is it created under any rules or regulations, which might in turn have a statutory backing. In the Aadhaar case, we saw the Supreme Court strike down requirements of mandatory linking of Aadhaar for SIM card verification and certain scholarship schemes precisely for the reason that such actions did not have a legal basis.

Violation of proportionality standards – The stated objectives of the NAFRS include the identification of criminals, missing children and adults and unidentified dead bodies, all of which lie well within the bounds of legitimate state objectives, allowing that test to be satisfied. The deployment of FRTs over large segments of the population, without their consent, is however not likely to satisfy the requirements of proportionality.

While rejecting the justification of countering black money as the basis for mandatory linkage of Aadhaar with bank accounts, the Aadhaar bench 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.[1] 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. 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.

Effectiveness of the intervention – Another element of the proportionality analysis is to examine 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. In particular, the results are affected by variations in the environment and lighting conditions and the challenges of using images gathered from non-cooperative settings.

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

Further, some of the specific functions of the NCRB's pro- posed 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). This is also reflected in the submissions made by the Ministry of Women and Child Development in a case before the Delhi High Court. The Ministry pointed to the poor performance of the facial recognition software being used by the Delhi Police to identify missing children, including, in some cases, its inability to distinguish between boys and girls (PTI, 2019).

The limited accuracy and reliability of FRTs, combined with serious privacy concerns, would therefore make it harder to justify the deployment of the technology on wide segments of the general population.

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 In- dia. 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 out- side the executive, and there is a vacuum in checks and balances to prevent the untrammelled 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 ac- cessed, by whom and under what circumstances? (Bailey, Bhandari, Parsheera, & Rahman, 2018).

Here 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 in- formation in the interest of national security cannot be faulted with, the power to make such decisions should prefer- ably be vested in the hands of a judicial officer.

6. Suggested policy interventions

Facial biometric data is one of the most sensitive categories of personal data and therefore any adoption of this techno- logy, either by state agencies or by the private sector, necessarily has to be preceded by the adoption of a robust data protection law. Such a law would determine the basic level of protection for the use of facial biometrics, including 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 of 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 under- lying models, training data being used, false positive and negative rates and other more granular information. Yet, information of this sort is necessary for there to be any in- dependent checks and analysis on the accuracy, reliability and biases in the systems. 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. The wide ranging ex- emptions available to state agencies under most data protection laws are another cause of concern.

Therefore, when it comes to the deployment of FRTs by state agencies, that will necessarily have to satisfy the standards 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. The first test to be satisfied here would be the need for a legislative authorisation for the use of FRTs.

Any thinking about the need for such a legal framework for the use of FRTs in a particular context should be based on 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. Stake- holders 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 inform the laws governing the use of FRTs for law enforcement purposes. This will, of course, also have to be ac- companied by other, more specific, requirements to be contained in binding and enforceable standard operating procedures.

1. The law should narrowly define the boundaries around 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. For instance, such uses may be limited to cases that relate to cognizable and non-bailable offences.

2. The sources that can be used for the gallery database should be limited to specific categories of persons in- stead 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.

3. In situations where FRTs are sought to be used for a specific use case, like finding missing children, the se- lection of the gallery dataset should be done in a manner that is suited to the needs of that objective. An ex- ample 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 pro- visions 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.

4. 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.

5. 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 re- cognition system.

Finally, while there are 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 the given context.

References

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

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

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

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
Buolamwin, J. & Gebru, T. (2018). Gender shades: intersec- tional accuracy disparities incommercial gender clas- sification. Retrieved from http://proceedings.mlr. press/v81/buolamwini18a/ buolamwini18a.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

Fussey, P. & Murray, D. (2019). Independent report on the london metropolitan police service's trial of live fa- cial 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

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 pro- posal for "automated facial recognition sysytem". Re- trieved from https://drive.google.com/file/d/ 1XNeqiyjCF0KWbiZB5mRUCtVyyxU2wj2v/view

Hamburg Data Protection Commissioner. (2018, Decem- ber). Order on the use of the facial recognition soft- ware "videmo 360" by the hamburg police to in- vestigate 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, al- gorithms, and thelimits of antidiscrimination dis- course. Information, Communication & Society, 22(7). Retrieved from https://doi. org/10.1080/1369118X. 2019.1573912

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

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 / supremecourt / 2012 / 35071 / 35071 2012 Judgement 26-Sep-2018.pdf

Justice Srikrishna Committee. (2018, July). A free and fair digital economy: protecting privacy, empowering in- dians. 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

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

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

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

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

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

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%20 18.pdf

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

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

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

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

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/

Smith, B. (2018). Facial recognition: it’s time for action. Re- trieved 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

Trivedi, S. & Wessler, N. F. (2019). Florida is using facial recognition to convict people without giving them a chance to challenge the tech. Retrieved from https : //www.aclu.org/blog/privacy-technology/ surveillance - technologies / florida - using - facial - recognition-convict-people

UIDAI. (2018). Implementation of face authentication. Re- trieved 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

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).

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

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.

About the Author

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

Acknowledgments

The author would like to thank Ajay Shah, 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.

Disclaimer and Terms of Use

IDFC Institute
3rd Floor, Makhija Chambers, 196 Turner Road,
Bandra(W), Mumbai 400050

/idfcinstitute @idfcinstitute /IDFCInstitute