EVALUATING PRIVACY VIOLATIONS OF FACIAL RECOGNITION TECHNOLOGY IN THE BACKDROP OF OECD PRIVACY PRINCIPLES

—Prerna Sengupta and Riddhi Bang***

Abstract—With the wave of machine learning and technological development, a new system that has arrived is the Facial Recognition Technology (hereinafter 'FRT'). From invention to accessibility, this technology has grown in every respect in the past few years. However, this technology is also controversial, primarily because of data leaks and various inaccuracies. In this essay, the authors, at first, briefly describe the functioning of this technology and a few examples of its benefits and uses. Following this, the authors use the Organisation for Economic Co-operation and Development (hereinafter 'OECD') data protection principles to illustrate how this technology violates basic privacy principles. This has been demonstrated using a variety of examples of FRT privacy violations by both state and non-state actors from across the globe. The authors then put forth the questions that arise with the implications of this technology and focus on the debate of privacy versus security. Lastly, the authors discuss the possible solutions and measures that could be taken up to balance the technology's use and privacy risks.

Keywords - Facial Recognition Technology, Privacy, OECD, Data Protection, Technology Law.

* Student, 2nd Year, BA LLB (Hons), National Academy of Legal Studies and Research, Hyderabad.

** Student, 2nd Year, BA LLB (Hons), National Academy of Legal Studies and Research, Hyderabad.

INTRODUCTION

Over the last few decades, technology has come a long way and we have adapted to the same for our own ease. One such technology being used extensively today is Facial Recognition Technology. With FRT, verifying the identity of individuals has been notched up to a whole new stage. Facial recognition technology is a subset of pattern recognition and automated reasoning, both of which were increasingly being developed by computer scientists in the 1960s.[50] In the 1970s, researchers from institutions across the world, such as Stanford University and Kyoto University, began developing technology that recognised facial forms from images. This eventually morphed into the state-of-the-art technology widely being used across the globe today.[51]

Facial recognition comes under the aegis of biometric data. Biometric data essentially includes distinctive physical characteristics or personality traits of a person which can be used to verify his/her identity. Some examples of biometric data are iris scan, fingerprint, voice recognition, etc. Facial recognition is a solution primarily designed to recognise a human face without any physical contact.[52]

This technology is been increasingly employed by private companies who are developing more sophisticated versions of photo-tagging, that is, automatically detecting people from photos online. This has enhanced the digital experience but at the cost of numerous privacy violations. More importantly, this technology is being increasingly used by government institutions for law enforcement and surveillance of citizens to ensure public safety. However, this raises privacy concerns. This article purports to prove that facial recognition technology, as is being used currently, across the world does not comply with the basic privacy principles and that there is a need for comprehensive laws and regulations to ensure that the privacy of individuals is protected.

HOW DOES FRT WORK?

Facial recognition technology primarily works through pattern recognition technology which detects and extracts patterns from data and

---

[50] Kelly A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* (NYU Press 2011) 12.

[51] Sharon Nakar and Dov Greenbaum, 'Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy' (2017) 23 BU J Sci & Tech L 88.

[52] John D Woodward and others, *Biometrics: A Look at Facial Recognition* (RAND Corporation 2003).

matches it with patterns stored in a database. The effectiveness of this system is entirely reliant on the quality of the captured image of the face. The system attempts to 'normalise' these images to the greatest extent possible, by changing their sizes, rotating them etc. The images are then transferred to the recognition software wherein the data goes through multiple stages, including extracting features to create a biometric 'template' which is then compared to the reference database. If the data collected matches the data in the database, then an alarm notifies the operator, who then verifies the match and proceeds appropriately.[53]

Facial recognition is increasingly being used to replace the existing 'documentary regime of verification' wherein official identities are assigned to people for administrative purposes.[54] States and institutional users of facial recognition are always on the hunt to simplify and hasten the verification process. Biometric identification thereby helps state institutions to achieve this goal by binding identity to the physical body through certain unique body parts such as the iris or the thumbprint. Consequently, it becomes crucial to understand to what extent the State and its institutions are willing to go to constantly track and monitor citizens using their biometric data. The private sector has been an equally crucial stakeholder, not merely for the development and application of facial recognition technology in the private sphere, but also for working in collaboration with the State and its institutions.

DIVERSE APPLICATIONS OF FRT

The most beneficial yet controversial use of FRT has been by law enforcement agencies.[55] In the hearings at the Capitol Hill following the September 11 attacks, Senator Dianne Feinstein remarked that the reason the terrorists were able to get on multiple airliners was that they could not be identified. This led to various experts suggesting that the employment of sophisticated identification technology could have prevented the drastic series of events that took place. This, to a great extent, fuelled the use of FRT by law enforcement agencies in the United States especially

---

[53] Lucas Introna and Helen Nissenbaum, 'Facial Recognition Technology: A Survey of Policy and Implementation Issues' (2010) Lancaster University Management School Working Paper 2010/030 <https://eprints.lancs.ac.uk/id/eprint/49012/1/Document.pdf> accessed 4 December 2020.

[54] Jonathan Sterne, *The Audible Past: Cultural Origins of Sound Reproduction* (Duke University Press 2003) 10.

[55] Christopher S Milligan, 'Facial Recognition Technology, Video Surveillance, and Privacy' (1999) 9 S Cal Interdisc L J 295.

by the Department of Homeland Security for border control and surveillance in airports.[56]

FRT has been used by various law enforcement agencies across the United States. For example, using FRT, an accused rapist was caught by the police in New York within 24 hours of the crime. According to an estimate in the Center on Privacy & Technology report, more than one in four of all American state and local law enforcement agencies can "run face recognition searches of their databases, run those searches on another agency's face recognition system, or have the option to access such a system." Law enforcement agencies have also partnered up with various private companies such as NEC, Cognitec, 3M Cogent, Safran Identity & Security, etc., to provide various innovative identification technologies like live-streaming and facial recognition on police body cameras.[57]

In the health care sector, facial recognition technology has been used for the diagnosis of genetic disorders and monitoring patients. Further, it also has applications in providing health indicator information in connection with ageing, pain, emotions, and behaviour.[58]

Facial recognition technology is being used across the world to ensure the mandatory wearing of masks in public spaces due to the global COVID-19 pandemic. This allows the effective monitoring of people thereby preventing the spread of the virus. Japanese Company NEC has stated that parts of the face that are not covered, such as the eyes, are used to verify the person's identity. This verification takes less than a second and has an accuracy rate of 99.9%.[59]

Payment based on facial recognition using biometrics has also emerged the world over. It rules out the need for having credit cards or cash in public places. Since it is easy to lose a credit card or forget passwords, FRT could assist in ensuring a fast and easy transaction as it detects feature vectors without any sort of physical contact.[60] This indicates the efficient performance of the FRT. Facial Recognition Technology today

---

[56] *Gates* (n 50) [2].

[57] Mariko Hirose, 'Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of Facial Recognition Technology' (2017) 49 Conn L Rev 1591.

[58] Nicole Martinez Martin, 'What are Important Ethical Implications of Using Facial Recognition Technology in Health Care?' (2019) 21(2) AMA J Ethics 180.

[59] 'Facial Recognition Identifies People Wearing Masks' (*BBC*, 7 January 2021) <www.bbc.com/news/technology-55573802> accessed 13 January 2021.

[60] Wen Kun Zhag and Min Jung Kang, 'Factors Affecting the Use of Facial-Recognition Payment: An Example of Chinese Consumers' (2019) 7 IEEE Access 154360.

is also being used in schools to ensure campus safety and automated registration.

Despite a variety of uses, some of which have been mentioned above, facial recognition technology has also received severe backlash. The most fundamental argument against the use of this technology is the right to privacy. The authors have used the *OECD data protection principles* in the backdrop of developing this idea further.

USING OECD DATA PROTECTION PRINCIPLES AS A BASIC STANDARD

To facilitate consistency in the privacy laws in times where the computers were being used to process/transfer personal data, the OECD formulated the first internationally agreed-upon privacy guidelines in 1980.[61] These rules have been promoting respect for privacy as a pertinent condition for the flow of personal data. These guidelines have taken a comprehensive approach[62] and have focused on the practical implementation by grounding their approach in risk management of privacy protection.

The OECD guidelines today form the basis of many privacy legislations in the world.[63] These guidelines are reflected and considered as the standard in the already existing and currently emerging data protection laws across nations[64] as they provide a good basis for the analytic endeavour to lessen privacy threats. These guidelines have been widely accepted to form the foundation of information practices to protect personal information. For example, the Asia-Pacific Economic Cooperation Privacy Framework and Canada's Personal Information Protection and Electronic Documents Act (*hereinafter* 'PIPEDA') are closely modelled on the OECD guidelines.[65] The EU's General Data Protection Regulation (*hereinafter* 'GDPR') also, in its details, reflects the OECD privacy framework.

---

[61] The Organization for Economic Co-operation and Development, 'The OECD Privacy Framework' (2013) <www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> accessed 5 January 2021 (OECD).

[62] Fred H. Cate, Peter Cullen and Viktor Mayer Schonberger, 'Data Protection Principles for the 21st Century' (2013) Books and Book Chapters by Maurer Faculty 23 <www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1022&context=facbooks> accessed 6 December 2020.

[63] ibid.

[64] Graham Greenleaf, 'Global Data Privacy Laws 2015: Data Privacy Authorities and their Organisations' (2015) 134 Privacy Laws & Business International Report <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2641772> accessed 8 December 2020.

[65] Mark Phillips, 'International Data-Sharing Norms: from the OECD to the General Data Protection Regulation (GDPR)' (2018) 137 Human Genetics 575 <https://link.springer.com/article/10.1007/s00439-018-1919-7> accessed 8 December 2020.

These principles were also revised and updated in 2013, keeping in mind today's technologically forward world to balance the fundamental and competing values of privacy and free flow of information.[66]

The authors have, thus, used the good practices introduced in the OECD principles to demonstrate the privacy violations in the context of Facial Recognition Technology. It is to be noted that these principles serve as a mere guide to create, adapt, and implement national laws. The national laws are to provide details to the principles mentioned. With regards to the same, the authors have analysed the use of FRT in various countries against the threshold of the OECD Privacy Principles. We demonstrate that not all countries are following the guidelines. The authors have merely used these principles as overarching guidelines.

VIOLATIONS OF OECD PRINCIPLES BY VARIOUS STATE AND NON-STATE ACTORS

Collection Limitation Principle

The collection limitation principle states that 'there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject'.[67]

This principle entails that *firstly,* there must be limits to collection and manner of collection of data when it is especially regarded as sensitive and *secondly,* the consent of the subject is essential.

Consent in this context needs to be understood by distinguishing between facial *recognition* and facial *authentication*. Facial authentication aims at checking if a person is who they claim to be, whereas facial identification aims at finding a particular person among a group by creating a biometric template.[68] Facial recognition is more so related to mass surveillance in public. This places no control in the hands of the data subject, depriving him/her of the ability to give consent.[69] This attracts

---

66 The Organization for Economic Co-operation and Development (n 61).

67 ibid.

68 'Facial Recognition: For a Debate Living up to the Challenges' (CNIL, 15 November 2019) <www.cnil.fr/sites/default/files/atoms/files/facial-recognition.pdf> accessed 10 December 2020.

69 Dean Nicolls, 'What is Facial Recognition, and How Does it Differ From Facial Authentication?' (*The Trusted Identity Blog*, 9 July 2019) <www.jumio.com/facial-recognition-vs-facial-authentication/#:~:text=For%20consumers%20and%20businesses%20alike,their%20own%20accounts%20or%20devices> accessed 11 December 2020.

much more serious privacy concerns. Facial authentication gives the data subject the choice and control as it is permission-based (an example is login protections). Facial authentication verifies an individual's identity as opposed to facial recognition that exposes it.

Recently, the European Commission, in its new Security Union package, has proposed to deploy facial recognition in the Counter-Terrorism Agenda.[70] As mentioned earlier, facial recognition technology uses facial coordinates (like the distance between a person's eyes, nose, mouth, etc.) to create a biometric map. The GDPR rules (now UK-GDPR in the United Kingdom) classify facial images under facial recognition as biometric data.[71] Thus, the Agenda suggesting wide use of facial recognition in public is unlikely to pass under these rules. The only exception is when the data subject gives explicit consent[72] which has not been obtained.

In India, the government has used FRT to identify people who were involved in the *Delhi Riots* case.[73] In 2018, the Home Ministry launched the Automated Facial Recognition System (*hereinafter* 'AFRS') which would aid the police authorities in identifying criminals and unidentified bodies.[74] This has raised privacy concerns and questions of legality as it lacks statutory backing which is a prerequisite for state interference with privacy as established by the Supreme Court in 2017.[75] Although India does not currently have a data protection law, the Personal Data Protection Bill (*hereinafter* 'PDP') draws significant parallels to GDPR in the context of consent.[76] Furthermore, the PDP Bill 2019 violates OECD guidelines under the collection-limitation principle on the ground that consent does not need to be renewed if changes in the use of the data

---

70 Riccardo Coluccini, Maria Lusia Stasi and Ella Jakubowska, 'Statement: Civil Society Challenges EU Plans to Expand Biometric Mass Surveillance' (EDR*i*, 14 December 2020) <https://edri.org/our-work/civil-society-challenges-eu-plans-to-expand-biometric-mass-surveillance/> accessed 12 December 2020.

71 EU General Data Protection Regulation (GDPR) [2016] OJ L119/1.

72 ibid.

73 Vijaita Singh, '1,100 Rioters Identified using Facial Recognition Technology: Amit Shah' *The Hindu* (Delhi, 12 March 2020) <www.thehindu.com/news/cities/Delhi/1100-rioters-identified-using-facial-recognition-technology-amit-shah/article31044548.ece.> accessed 15 December 2020.

74 'Amit Shah said 'Facial Recognition' Identified 1,900 Delhi Rioters. How does it work?' *The Week* (Delhi, 13 March 2020) <www.theweek.in/news/india/2020/03/13/amit-shah-said-facial-recognition-identified-1900-delhi-rioters-how-does-technology-work.html> accessed 15 December 2020.

75 *K S Puttaswamy v Union of India* (2017) 10 SCC 1.

76 Karishma Mehrotra, 'Explained: How Data Protection Bill Compares with its EU Counterpart' *The Indian Express* (New Delhi, 13 December 2019) <https://indianexpress.com/article/explained/how-data-protection-bill-compares-with-its-eu-counterpart-6164237/> accessed 16 December 2020.

occur, which is mandated by the OECD.[77] Mass surveillance is now being conducted to add to the existing data set by video surveillance in public areas without obtaining any consent from the public. Further, the matching and use of AFRS in public spheres is not regulated in any manner. This suggests that such collection of data is against the necessity and proportionality principles established by the *Puttaswamy* case (2017).[78] This lacuna paves way for unregulated surveillance. Further in the paper, we demonstrate that surveillance reform is the need of the hour.

In Serbia, the installation of a thousand cameras was announced in 800 different locations in Belgrade which lacked transparency.[79] A legal precondition for assessing information of public importance requires the possession of information on locations and crime rate analysis which the Ministry lacked. Further, it was devoid of legality because it had no comprehensive description of intended actions on processing such personal data and there was no risk assessment either.[80] The collection was thus not lawful and appropriate amounting to grave personal data protection law violations.

Many Police departments in the U.S. have begun utilising the technology.[81] In the U.S., there is no single federal law that regulates the collection of personal data. At the state level, however, Illinois (one of the 3 states that have passed biometric legislation) has passed the Illinois Biometric Information Privacy Act (*hereinafter* 'BIPA') to include 'face geometry' as a part of biometric information.[82] Facebook was sued for BIPA violations as it used automatic photo recognition technology without users' consent. Even though it updated its policies in 2019, it has recently agreed to pay $650M to settle the suit.[83] A similar example is the case of *Martinez v Snapchat*[84] where the app stored biometric identifiers of the faces it scanned. It never actually took the consent of the users nor

---

77 FH Cate and Mayer Schonberger, 'Notice and Consent in a World of Big Data' (2013) 3(2) International Data Privacy Law 67.

78 *Puttaswamy* (n 75).

79 'Serbia: Unlawful Facial Recognition Video Surveillance in Belgrade' (ERD*i*, 4 December 2019) <https://edri.org/our-work/serbia-unlawful-facial-recognition-video-surveillance-in-belgrade/> accessed 16 December 2020.

80 ibid.

81 Tate Ryan Mosley, 'There is a Crisis of Face Recognition and Policing in the US' (MIT Technology Review, August 2020) <www.technologyreview.com/2020/08/14/1006904/there-is-a-crisis-of-face-recognition-and-policing-in-the-us/> accessed 16 December 2020.

82 The Biometric Information Privacy Act 740/ILCS 14 (2008).

83 *Facebook Biometric Information Privacy Litigation*, *In re* Case No 3:15-cv-03747-JD (ND Cal May 14, 2018).

84 *Jose Luis Martinez et al v Snapchat Inc* Case 2:16-cv-05182-SVW-FFM.

specified the purpose or time length for which it would store the data.[85] These are some of the many examples that present the dangers of facial recognition technology and how its use amounts to a violation of the data collection principle by both state and non-state actors.

Data Quality Principle

The Data Quality Principle essentially states that personal data should be relevant, that is, related to the purpose for which it is used. It further states that proper precautions must be taken to ensure that the data is accurate, complete and up to date.[86]

Concerning facial recognition technology, inaccurate data may often have adverse effects, especially when employed as a tool by the State. An example of this is the use of facial recognition by the U.S. Customs and Border Protection (*hereinafter* 'CBP') at airports. CBP is responsible for the inspection of foreign travellers at various points of entry and exit and confirming their identities. Upon utilising FTR, the CBP found that the prescribed false acceptance rate did not reach the minimum limit required.[87] The false acceptance rate is the likelihood of a person to be matched with an a photo from the gallery that is not theirs.[88] Research has shown that this technology has proven to be especially unreliable for racial and gender minorities. One study found that the accuracy rate for white men was 99 per cent whereas the accuracy rate for women with a darker complexion was 35 per cent.[89] The implication of this is that women and people of colour may be unfairly targeted for additional screening measures. Additionally, the CBP Monitors do not alert officials when performance falls short of minimum requirements leading to unnecessary targeting of people due to technical errors.[90]

This research has further been buttressed by assessments conducted by the U.S. National Institute of Standards Technology (*hereinafter* 'NIST') where it was revealed that many facial recognition systems generate inaccurate matches due to racial bias. It was found that false-positive scans

---

85 ibid.

86 The Organization for Economic Co-operation and Development (n 61).

87 United States Government Accountability Office, 'Facial Recognition; CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues' (September 2020) <www.gao.gov/assets/gao-20-568.pdf> accessed 18 December 2020.

88 ibid.

89 Steve Lohr, 'Facial Recognition is Accurate If You're a White Guy' (*The New York Times*, 9 February 2018) <www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html> accessed 18 December 2020.

90 US Government Accountability Office (n 87).

on African American and Asian people were anywhere between 10 to 100 times more likely in various facial recognition systems.[91]

This is also the case with the Israeli army who have employed facial recognition technology to monitor Palestinians on the West Bank checkpoints into Israel. Anyvision Interactive Technologies, which is Israel's largest biometric technology firm, has confirmed that this technology is sensitive to racial and gender bias.[92]

Facial recognition for border control has, therefore, proven to have failed on multiple fronts thereby violating the data quality principle.

Facial recognition has proven to be a dangerous tool not just by law enforcement agencies but also by various private companies. An example of this is the case of misidentification by Amazon's facial recognition technology called 'Amazon Rekognition'. In 2018, the American Civil Liberties Union (*hereinafter* 'ACLU') conducted a test where the technology incorrectly identified 28 members of Congress as people who had earlier been arrested for committing a crime.[93] Most importantly, the test found that people of colour were disproportionately identified among their database of 25,000 publicly available arrest photos/mugshots. ACLU searched this database against public photos of all the members of Congress at the time.

Academic research has proven time and again that facial recognition is less accurate for women and darker-skinned women,[94] as also seen in the case of facial recognition by CBT mentioned earlier. In fact, a study conducted by Joy Buolamwini from MIT showed that commercially released facial recognition technology by tech giants Microsoft, IBM and Amazon showed both skin-type and gender biases. Furthermore, software such as

---

[91] Patrick Grother, Mei Ngan and Kayee Hanaoka, 'Face Recognition Vendor Test, Part 3: Demographic Effects' (2019) National Institute of Standards and Technology, US Department of Commerce <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf> accessed 18 December 2020.

[92] Amitai Ziv, 'This Israeli Face-Recognition Startup is Secretly Tracking Palestinians' (*Haaretz*, 15 July 2019) <www.haaretz.com/israel-news/business/. premium-this-israeli-face-recognition-startup-is-secretly-tracking-palestinians-1.7500359> accessed 19 December 2020.

[93] Jacob Snow, 'Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots' (*American Civil Liberties Union*, 26 July 2018) <www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28> accessed 20 December 2020.

[94] Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (Conference on Fairness, Accountability and Transparency, New York, February 2018) 81 <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf> accessed 21 December 2020.

Amazon Rekognition which are freely available to the public could potentially also be used for law enforcement purposes. In such a case, false identification could bias a police officer even before an encounter begins or could lead them to search someone's home and belongings based on false data.[95] This misidentification would then potentially lead to serious breaches of privacy and impede on their freedom and civil rights. Such misidentification by software developed by private companies like Amazon is therefore in clear violation of the data quality principle.

Purpose Specification

The purpose specification principle states that the purpose for the collection of data must be specified either before or at the time of collection and subsequent use of such data must be limited to fulfilling that purpose. Furthermore, any amendment to the original purpose must be notified by any complementary or alternative way including public declarations, information to data subjects, legislation, administrative decrees, and licenses provided by supervisory bodies. Any change to the purpose must be in consonance with the original purpose. Lastly, the data must be destroyed or anonymised when it no longer serves the purpose or when control over data is lost, so as to avoid risks of theft, unauthorised copying, etc. Collection and processing of personal data should be done only with the consent of an individual and depends on the information that he/she has regarding the purpose for which the data is being used.[96] Erasing or anonymising personal data that is no longer needed, along with clear policies on storage/retention periods and erasure, reduces risks and helps comply with the purpose specification principle.[97]

An illustration of the purpose specification principle with respect to facial recognition technology is the *Hangzhou Safari Park* case. This was the first case challenging the privacy violations of FRT in China. In this case, Guo Bing, a professor of law sued the park for mandating everyone to enter via the facial recognition lane. The court held that the zoo in the card application contract specified only the collection of fingerprints and not facial recognition. The Court ruled in favour of Guo Bing since the purpose for the collection of facial data was not specified at the time/

---

95 Snow (n 93).

96 J A Cannataci and J P M Bonnici, 'The End of the Purpose-Specification Principle in Data Protection?' (2010) 24(1) Intl Rev of L Comp & Tech 101 (Principle in Data Protection).

97 Lydia F, 'What does "Storage Limitation" Mean under EU Data Protection Law?' (*Medium*, 23 January 2019) <www.medium.com/golden-data/what-does-storage-limitation-mean-under-eu-data-protection-law-fc6459ecb26c> accessed 11 March 2021.

before collection of data and for the lack of consent for collecting such data.[98]

In light of the global Coronavirus pandemic, facial recognition technology companies have developed AI that can identify facial data even with masks on. Alan Descoins, the chief technology officer of Tryolabs, a Uruguay based company that has developed mask recognition stated that the purpose of such technology was to ensure strict compliance of wearing masks in public places during the pandemic. Similar reasoning has been given by other developers of mask recognition technology. However, they are unclear as to whether such technology would be employed even after the pandemic is over. In that case, mask recognition software would be exceeding its purpose.[99]

Further, this was also pointed out in the case *In Re Facebook Biometric Information Privacy Litigation*,[100] where it was alleged that Facebook unlawfully collected and stored biometric data derived from pictures of users' faces. Facebook argued that the term 'face geometry' scan mentioned in the Illinois Biometric Information Privacy Act must be read to mean in-person scan, which was not explicitly mentioned at the time of data collection. However, the statute specifies that the purposes to be achieved must be explicitly mentioned at the time of collection of data. This 'cramped' interpretation is not mentioned in the statute and is antithetical to its purpose of protecting privacy with the rise of biometric technology and is a violation of the purpose of the specification principle. An issue with the purpose specification principle is that of compatibility assessment which guages the compatibility of further processing with the initial purpose.

The controller needs to be clear with regards to the distance between the purpose for which the data was collected, and the reason for which it is to be further processed. The methodology of compatibility assessment should be communicated along with the policy decisions. The decision with regards to this rift between the purposes is left to the individuals whose data is being collected. Hence, the controller should allow the data subject to opt-out without conditions. This implies that a mere 'right to

---

98 Feng Qunxing Pan Yingxin, 'The First Case of Facial Recognition in China was Pronounced! The Court Ordered the Zoo to Delete the Photos of Guo Bing and Compensate' *Southern Metropolis Daily* (20 November 2020) <https://m.mp.oeeee.com/a/BAAFRD000020201120382407.html> accessed 22 December 2020.

99 Wudan Yan, 'Face-Mask Recognition has - Arrived for Better or for Worse' (*National Geographic*, 11 September 2020) <www.nationalgeographic.com/science/2020/09/face-mask-recognition-has-arrived-for-coronavirus-better-or-worse-cvd/> accessed 22 December 2020.

100 *Facebook Biometric Info Privacy Litig, In re* (n 83).

object' would not suffice as in such cases, the controller would be free to take time to assess the objection that is raised which allows him/her to devise persuasive reasons to discard the request.[101]

An example of big data companies using this principle to their advantage is in the case of communications data where data controllers have argued that providing information such as billing, network management, and fraud prevention is sufficient to show purpose. However, they are of the opinion that the contents of communication do not need to be specified under the purpose specification.[102] Therefore, this debate on what is actually to be retained, i.e., storage limitation under purpose specification poses a challenge.

Use Limitation Principle

This principle states that, 'Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except a) with the consent of the data subject; or b) by the authority of law.'[103]

These exceptions are widely misused and abused. The second exception allows the state to have extensive data-sharing systems. Such an umbrella exception is a threat to the protections that are offered for personal data. There is a need to tread carefully to ensure that these exemptions are not reduced to become superfluous with regards to the State and the exchange of information among state agencies. Further, limits need to be placed in the context of relying on the consent given by data subjects in cases where for example, there is a disparity in power.

Exceptions like this exist to allow some leeway to the State to monitor citizens efficiently. An example is the use of Aadhar, India's national biometric database, for purposes ranging from school admissions to obtaining death certificates. Another example is the use of Eurodac, a biometric database that allows EU Member States to check whether asylum seekers have previously applied for asylum and if they are receiving social benefits from another EU country. This database also collects fingerprints

---

[101] Wouter Seinen and others, 'Compatibility as a Mechanism for Responsible Further Processing of Personal Data' (*Baker McKenzie*, 2018) <https://bakermckenzie.com/-/media/files/insight/publications/2018/10/compatibility_mechanism_responsible_further_personal_data_processing.pdf?la=en> accessed 11 March 2021.

[102] Principle in Data Protection (n 96).

[103] The Organization for Economic Co-operation and Development (n 61).

of asylum seekers for prevention, detection, and investigation of terrorist offences or other grave crimes.[104]

A lawsuit filed against the South Wales police for deploying automated facial recognition (*hereinafter* 'AFR') cameras highlighted the breaches of privacy.[105] The police had argued that it is the same as photographing a person in public and does not retain data.[106] As mentioned earlier, the GDPR regulates facial recognition processing[107] and even if the data is not retained, it is still being captured, processed, and compared to a database for identification. This processing of data without the consent of the subjects goes against the limitation principle.

The example of the use of FRT in India, as mentioned earlier, began with its use by the Delhi Police. While the police department had gotten permission to use this technology for purposes like finding missing children, it is now being used for much wider surveillance and investigation[108] resulting in a 'function creep' (which happens when someone uses data for a purpose other than the original purpose).[109] Further, the AFRS hasn't been built on any legal basis firstly, as it fails the test of proportionality[110] (rational nexus between the aims and means adopted to achieve them), and legality[111] (there must be a law in existence).

A digital right advocacy 'Fight for the Future' group presented a map to visualise how the U.S. law enforcement agencies use this technology without the consent or knowledge of the subjects in America.[112] It highlighted that the ICE and FBI are using the FRT to scan drivers' license

---

[104] Privacy International, 'Data Protection Principles: A Guide for Policy Engagement on Data Protection' <https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf> accessed 11 March 2020.

[105] Jenny Rees, 'Facial Recognition Use by South Wales Police Ruled Unlawful' (*BBC*, 11 August 2020) <https://bbc.com/news/uk-wales-53734716> accessed 24 December 2020.

[106] Steven Morris, 'Office Worker Launches UK's First Police Facial Recognition Legal Action' *The Guardian*, (London, 21 May 2019) <https://theguardian.com/technology/2019/may/21/office-worker-launches-uks-first-police-facial-recognition-legal-action> accessed 24 December 2020.

[107] EU General Data Protection Regulation (n 71).

[108] Rina Chadran, 'Mass Surveillance Fears as India Readies Facial Recognition System' (*Reuters*, 7 November 2019) <https://reuters.com/article/us-india-tech-facialrecognition-trfn-idUSKBN1XH0S9> accessed 25 December 2020.

[109] Muhammad Safdar and others, *Function Creeption in Surveillance Techniques* (2016) 2 IJSRSET 983, 984-85.

[110] *Puttaswamy* (n 75).

[111] ibid.

[112] Fight for Future, 'Map of United States of America' <www.banfacialrecognition.com/map/> accessed 26 December 2020.

photo datasets without citizens' consent.[113] Without a comprehensive data protection law that applies to the U.S uniformly, this has increased the discrepancies and anxieties among the citizens.

A report published by security researchers found that Suprema, a biometrics research and development company was in breach of privacy where biometric data including facial recognition records of millions of people were exposed.[114] Suprema's Biostar 2 biometric identity is used across 83 countries by thousands of organisations including police and governments thereby amounting to an international breach. Such a breach is apparently a use limitation violation with the data being disclosed without consent.

In January of last year, IBM released a set of data including around a million photos taken from Flickr and annotated the same with skin tone descriptions.[115] The catch is that it had taken no consent from people.[116] Microsoft, Google, and Amazon have also faced legal suits by users that claim that their faces were used without their consent.[117]

Vimeo, an app used for streaming, creation, and sharing of HD videos was sued for illegally collecting and storing biometric data of the users without consent or notice.[118] The photos uploaded by the users were analysed to create facial templates to later recognise them in photos and also identify their age, gender, race, and also location without permission.[119] A suit was filed by the Illinois users to highlight the violations of BIPA.

---

[113] Drew Harwell, 'FBI, ICE Find State Driver's License Photos are a Gold Mine for Facial-Recognition Searches' *(The Washington Post,* 9 July 2019) <https://washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/> accessed 26 December 2020.

[114] Noam Rotem and Ran Locar, 'Report: Data Breach in Biometric Security Platform Affecting Millions of Users' (*VPNMentor*, 26 January 2021) <www.vpnmentor.com/blog/report-biostar2-leak/> accessed 28 January 2021.

[115] John R Smith, 'IBM Research Released 'Diversity in Faces' Dataset to Advance Study of Fairness in Facial Recognition System' (IBM, 29 January 2019) <www.research.ibm.com/artificial-intelligence/publications/paper/?id=Diversity-in-Faces> accessed 30 December 2020.

[116] Charlotte Jee, 'People's Online Photos are Being Used Without Consent to Train Face Recognition AI' (*MIT Technology Review*, 13 March 2019) <www.technologyreview.com/2019/03/13/136638/peoples-online-photos-are-being-used-without-consent-to-train-face-recognition/> accessed 2 January 2021.

[117] 'Amazon, Google, Microsoft Sued for Allegedly Using Biometric Data Without Consent: Report' (*The Times of India,* 19 July 2020) <https://timesofindia.indiatimes.com/gadgets-news/amazon-google-microsoft-sued-for-allegedly-using-biometric-data-without-consent-report/articleshow/77047947.cms> accessed 4 January 2021.

[118] *Acaley v Vimeo, INC*, (2020) No 1:2019 cv 07164 (Northern District of Illinois III).

[119] Charlie Osborne, 'Vimeo Embroiled in Biometric "Face Map" Lawsuit Over User Privacy Consent' (*ZDNet*, 27 September 2019) <www.zdnet.com/article/vimeo-faces-facial-biometric-database-lawsuit-over-user-privacy-rights/> accessed 5 January 2021.

These examples present how apps are using the data uploaded for unspecified purposes without the consent of users and against the law.

Security Safeguards Principle

This principle states that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification, or disclosure of data.[120]

In the absence of safeguards, law enforcement agencies have a higher degree of discretion in the way this technology is to be used. This could potentially culminate in violations of purpose specification and use limitation principles as well. Legal controls have not been able to maintain pace with the advancement of this technology. There have been legal instruments attempting to curb this misuse such as the 'risk-based' approach mentioned in Articles 24 and 25(1) of the GDPR. This approach states that data controllers must account for the rights and freedoms of data subjects while taking any risks.[121] However, this approach poses certain issues and challenges in the context of the right-based character of laws regarding data protection. When the risk-based approach is adopted, the responsibility to protect the fundamental rights of the individuals' shifts to the controllers who in turn are not qualified to consider and appraise these risks.[122]

In the Indian context, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (*hereinafter* 'Rules')[123] provides a legal safeguard against body corporates in possession of sensitive personal data or information (*hereinafter* 'SPDI'). However, this poses to be a challenge because it is not applicable to government entities that may also possess sensitive data. Furthermore, the definition of SPDI under Section 3 of the Rules excludes crucial criteria such as ethnicity/caste, email/home addresses, electronic communication records, etc. The term "biometric definition" is also not defined thereby leaving scope for misuse of

---

[120] The Organization for Economic Co-operation and Development (n 61).

[121] Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach' (2018) 9(3) EJRR 502.

[122] Seda Ilik, 'The Shift Towards a "Risk-Based Approach" with GDPR: Critical Assessment of its Advantages and Disadvantages' (*Turkish Law Blog*, 12 October 2018) <https://turkishlawblog.com/read/article/36/the-shift-towards-a-risk-based-approach-with-gdpr-critical-assessment-of-its-advantages-and-disadvantages> accessed 11 March 2021.

[123] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

biometric data such as data collected by facial recognition software.[124] Security of SPDI is another issue because of the lack of a centralised dedicated authority to oversee enforcement of data protection laws and redress related grievances.[125]

In Scotland, the FRT is available to the police and was questioned when the report from the Justice Sub-committee stated that "*the use of this technology would be a radical departure from Police Scotland's fundamental principle of policing by consent*."[126] This springs from the fact that the technology in use must be 'provided for in legislations'. In New Zealand, the government has gone from testing budding facial recognition on passports to state-wide systems using tools like Briefcam that scans CCTV footage for facial recognition[127] and like most of the countries here as well, there is no infrastructure and regulatory framework for mass surveillance; indicating a lack of control and access. In both these countries, the FRT is being used without any safeguards.

In the United States, the Department of Homeland Security (*hereinafter* 'DHU') was sued by the American Civil Liberties Union (*hereinafter* 'ACLU') for failing to give details regarding the use of facial recognition at airports and against US Customs and Border Protection (*hereinafter* 'CPB'). In 2019, hackers stole photos and license plates from the CPB database[128] indicating that the government agencies could potentially lose control of data. Thus, without sufficient safeguards, such unregulated use of technology carries along with it dangers of misuse.

With the Black Lives Matter protests, IBM, Amazon, and Microsoft withdrew facial recognition services from the US police to urge the

---

[124] Vrinda Bhandari and Renuka Sane, 'Analysing the Information Technology Act (2000) from the Viewpoint of Protection of Privacy' (*The Leap Blog*, 18 March 2016) <https://blog.theleapjournal.org/2016/03/analysing-information-technology-act.html> accessed 11 March 2021.

[125] Supratim Chakraborty & Aritri Roy Chowdhury, 'Privacy Policy: Draft Data Protection Law has many Gaps' The Financial Express (20 November 2018) <www.financialexpress.com/opinion/privacy-policy-draft-data-protection-law-has-many-gaps/1386938/> accessed 11 March 2021.

[126] Justice Sub-Committee on Policing, 'Facial Recognition: How Policing in Scotland Makes Use of this Technology' (*SP Paper 678*, 2020) <https://sp-bpr-en-prod-cdnep.azureedge.net/published/JSP/2020/2/11/Facial-recognition--how-policing-in-Scotland-makes-use-of-this-technology/JSPS0520R01.pdf> accessed 7 January 2021.

[127] Nessa Lynch and others, '*Facial Recognition Technology in New Zealand*' (*The Law Foundation*, November 2020) <https://assets.documentcloud.org/documents/20419414/fr-tech-framework-report-dec-2020.pdf> accessed 7 January 2021.

[128] Drew Harwell, 'US Customs and Border Protections Says Photos of Travels were Taken in a Data Breach' *The Washington Post* (Washington DC, 10 June 2019) <www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/> accessed 9 January 2021.

government to regulate the use of this technology.[129] In the wake of this and due to the increasing deployment of facial recognition systems in Australia, Human Rights Commissioner Edward Santow has stated that there are no clear legal protections in place to prevent misuse in the areas like law enforcement.[130]

Clearview AI, an American software firm, was hit by a facial recognition data breach of its data of around 3 billion online images which were allegedly stolen.[131] It goes without saying that the privacy of the customers was compromised. Microsoft President Brad Smith has urged tech companies to come up with safeguards for facial recognition.[132] He also stated that Microsoft would begin to implement principles to manage the use and development of the FRT out of which one is 'lawful surveillance 'with which the company advocates for safeguards for people's privacy in law enforcement scenarios.

Openness Principle

This principle requires that there be general openness regarding the developments, practices, and policies concerning personal data. Furthermore, information regarding the collection, storage, and usage of personal data should be made easily available without any extraneous costs, knowledge, travel arrangements, etc. The major component, therefore, is the principle of transparency which is manifested by way of providing information and enabling the right to access relevant documents.[133]

---

[129] Julia Horowitz, 'Tech Companies are Still Helping Police Scan Your Face' (*CNN Business*, 3 July 2020) <https://edition.cnn.com/2020/07/03/tech/facial-recognition-police/index.html> accessed 11 January 2021.

[130] Tim Biggs, ' "Harm against Humans": Rights Chief Warns of Facial Recognition Threat' *The Sydney Morning Herald* (Sydney, 13 June 2020) <www.smh.com.au/technology/harm-against-humans-rights-chief-warns-of-facial-recognition-threat-20200611-p551o6.html#:~:text=Australian%20Human%20Rights%20Commissioner%20Edward%20Santow%20has%20repeated,to%20use%20it%20without%20proper%20safeguards%20in%20place> accessed 14 January 2021.

[131] Mike Snider, 'Clearview AI, which has Facial Recognition Database of 3 Billion Images, faces Data Theft' *USA Today* (New York, 26 Feb 2020) <www.usatoday.com/story/tech/2020/02/26/clearview-ai-data-theft-stokes-privacy-concerns-facial-recognition/4883352002/> accessed 14 January 2021.

[132] Brad Smith, 'Facial Recognition: It's Time for Action' (*Microsoft*, 6 December 2018) <https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/> accessed 14 January 2021.

[133] Alberto Alemanno, 'Unpacking the Principle of Openness in EU Law: Transparency, Participation and Democracy' (2014) 39(1) EL Rev 72 <https://ssrn.com/abstract=2303644> accessed 15 January 2021.

As mentioned earlier, U.S. Customs and Border Protection[134] has a website that has an option for frequently asked questions and other information on the Biometric Entry-Exit Program. However, it was found that the website did not accurately reflect the locations where CBP used or tested facial recognition technology thereby preventing travellers from accurately knowing where facial recognition technology is being used. Additionally, their call centre for travel or customs questions was often found to be inoperative in the ports of entry that use facial recognition.

In the case of *Patel v Facebook,*[135] the plaintiffs sued Facebook for using its facial recognition technology to collect biometric information in its Tag Suggestions Tool. This information was taken without providing any notice to users and no option for opting out. This is a clear demonstration of lack of openness and failure to notify technical updates that involve the collection and storage of biometric facial data. The Court, in this case, ruled in favour of the plaintiffs although no 'actual' and 'concrete' harm was suffered by the plaintiffs.

Individual Participation Principle

The Individual Participation Principle enumerates a fourfold right that individuals have against data controllers. The first is the right to obtain or confirm whether the data controller has certain data. This is followed by the right to reasonably communicate such data and the right to challenge the data controller if such communication is denied. Lastly, individuals have the right to challenge data concerning them and can have the data erased, rectified, completed, or amended if the challenge is successful.

There are various challenges to this principle. The case of Facebook can be used to understand these issues. In 2009, a participatory governance system was implemented by Facebook that enabled users to vote on its privacy policy. This system was terminated three years later because of participatory issues like insufficient information about participation commitments and possibilities of users, an attempt to transfer voting on to a third-party platform and spreading misconstrued data ownership claims. These are some practical hindrances that could arise in the implementation of this principle.[136]

---

[134] US Government Accountability Office (n 87).

[135] *Patel v Facebook Inc*, No 18-15982 (9th Cir 2019).

[136] Severin Engelmann, Jens Grossklags and Orestis Papakyriakopoulos, 'A Democracy Called Facebook? Participation as a Privacy Strategy on Social Media' in Manel Medina and others (eds), *Privacy Technologies and Policy* (Springer 2018).

Along with the right to confirm and obtain, individuals should also have the right to block the processing of personal data and the right to erasure in certain circumstances. This has been recognised in GDPR and in the data protection frameworks of Nigeria and South Africa. This right is especially important to ensure that the data being processed is accurate. For example, the processing of inaccurate medical data could have far-reaching consequences such as the data subject not receiving the assistance that he/she requires. This right needs to be carefully considered in the Indian context so that it is not open to misuse. Further, the right to object should also be formulated in a manner that the burden to prove the need for continuation of data processing should be on the controller. [137] Thus, the Indian legislature is to make sure that the data subject has power and control of his/her personal data and is in a position to ask the controller to make available the data that is being processed.

In the Capitol Attacks of January 2021, the Federal Bureau of Investigation is said to have used Facial Recognition Technology to identify suspects. However, when approached by various people including news agencies, the FBI has stayed completely silent on the matter despite confirmation from Clearview AI. Clearview, a facial recognition application, confirmed a spike in searches of its database used by law enforcement. A separate news agency also confirmed that facial recognition technology was used by investigators to identify suspects. The FBI's silence on the matter of whether they possess such data goes against the individual participation principle.[138] A similar example is the refusal to furnish details on facial recognition information collected by the Delhi and Kolkata Police Departments in response to a Right to Information (*hereinafter* 'RTI') query.[139]

Furthermore, the Washington Post reported that Huawei developed a facial recognition system for China to specifically detect people from the Uighur community and had a "Uighur" alarm to alert authorities upon identifying people of the Uighur ethnicity. However, Huawei refused to

---

[137] Privacy International, 'The Keys to Data Protection: A Guide for Policy Engagement on Data Protection' (August 2018) <https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf> accessed 11 March 2021.

[138] Rae Hodge, 'Capitol Attack: FBI Mum on Facial Recognition, Clearview AI Searches Spike' (*CNET*, 12 January 2021) <www.cnet.com/news/capitol-attack-fbi-mum-on-facial-recognition-clearview-ai-searches-spike/> accessed 18 January 2021.

[139] Aditya Chunduru, 'RTI: Kolkata, Delhi Police Refuse to Give Information on Facial Recognition Systems' (*MediaNama*, 2 December 2020) <www.medianama.com/2020/12/223-rti-replies-delhi-kolkata-police-telangana-facial-recognition-iff/> accessed 18 January 2021.

confirm whether technology was merely being tested or was being used on the ground.[140]

Accountability Principle

The accountability principle states that the data controller should be accountable for complying with the aforementioned privacy principles. Accountability, in this case, refers to both accountabilities – those supported by legal sanctions and those established by codes of conduct.

A UK Court of Appeal opined that the use of facial recognition technology by South Wales is a violation of human rights and agreed that facial recognition is an intrusive and discriminatory mass surveillance tool. However, the court also found that the benefits of this technology outweigh the distress caused to the individual plaintiff. As a result, the court ruled that the use of FRT must be regulated. The judgment also ensured that racial or sexual bias is eliminated from FRTs used by various other police forces as well.[141]

PROBLEMATISING THE RISE OF FRT

In today's world, technology has its presence in almost all aspects of your lives. While on one hand, such technology comes with many benefits like aiding law enforcement to react quickly and efficiently, it raises questions and debates. Naturally, one of the most rudimentary and crucial questions is that of privacy.

Privacy has been recognised as a fundamental human right under Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights. Such recognition of privacy at an international level reinforces how integral privacy is to live a life where an individual has control over their own information. In this era of technological advancement, severe tensions have originated between individual privacy and the unfettered collection of data. The laws and regulations governing the accumulation of data and protection of privacy have proved to be insufficient. The authors have demonstrated

---

[140] Drew Harwell and Eva Dou, 'Huawei Tested AI Software that Could Recognize Uighur Minorities and Alert Police, Report Says' *The Washington Post* (Washington DC, 8 December 2020) <www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/> accessed 19 January 2021.

[141] *Edward Bridges v South Wales Police* [2020] EWCA Civ 1058.

with multiple illustrations, how facial recognition technology violates all the basic principles of privacy.

Are people aware that their pictures are being collected and stored for the purpose of identification? Have they consented to the same? Is the data being utilised exclusively for its stipulated purposes? Have laws and policies on collection and access been formed after taking appropriate privacy considerations? Have such laws and policies been stated definitively, and do they take into consideration various contexts in which this data is reasonably expected to be protected? Do the external actors have access to such personal data? These are some of the vital questions that arise while one attempts to bridge the gap between privacy and the progress in technology. The possibility of over-reach and mission creep that could arise, especially when the technology is of great appeal to governments and corporate entities alike is another concern besides the potential for misrecognition and fallibility. The widespread use of this technology supports the large-scale generation of databases of people which are poorly regulated and promotes a system in which the subject has little or no control over their own details.

In addition to concerns about privacy, another pertinent question is that of the technology impeding individual autonomy and freedom, as it constrains people's capacity to determine their actions and values. This needs to be understood under the existing standards of autonomy, freedom, and security in the world. The aspect of fairness is also worth questioning in this scenario where the benefits of the technology may be disproportionate to a certain class of individuals.

THE WAY FORWARD

The authors are of the opinion that despite the multifarious purposes that facial recognition technology purports to serve, it must be regulated in a more stringent fashion. Facial recognition technology needs to be devised to make sure that access and sharing of personal data do not occur inappropriately. The threshold for the implementation, operation, and maintenance of this technology needs to be elevated in comparison to existing privacy laws governing biometric data. We can achieve this balance *firstly,* by limiting the context in which this technology is used by ensuring that it only serves the purposes for which it was built in an appropriate manner. To ensure this appropriateness, there needs to be an explicit declaration of its purposes, the environment in which it is to be used, and the manner of implementation. An example of such regulation

would be authorities mandating the approval and monitoring (especially by the public) of FRT used in public spaces. proposed,

Secondly, deliberations upon the technical requirements of FRT to serve its purpose without compromising on privacy are required along with the specifications of the kind of images that can be collected and the duration for which they may be stored. There needs to be expenditure on identity management systems and on the employment of professionally trained staff that can interpret the data correctly and understand its drawbacks and exceptions. There is also a dire need for a proper redressal mechanism in the instance of there being inaccurate results. It is highly important to consider whether the benefits of the use of this technology in a particular context are proportionate to the dangers and inaccuracies that it entails. Furthermore, routine updates regarding the utilisation of the technology should be communicated. *Lastly*, the laws need to be designed to incorporate the people's right to access and challenge the handling of their data. Upon such challenges, the data holders should be amenable to erasing the data or rectifying how it is used.

The dichotomy between the uses and the violation of this technology inevitably puts lawmakers in a difficult position. As discussed in this essay, facial recognition technology has multiple uses but the right to privacy of individuals cannot, in any way, be compromised. In the Indian scenario, the Supreme Court of India in the Puttaswamy judgment[142] established the 'compelling state interest' test as an exception where privacy can be infringed by the State. No illustration of what constitutes completing state interest was given and the only criterion is, that the State must pursue the least intrusive means of achieving its objective.[143] However, the Supreme Court themselves failed to engage with the least intrusive alternatives while applying their own test to the Aadhar Act.[144] Furthermore, no compelling state interest in the context of the need to have the Aadhaar program deployed has ever been introduced, and, or formally brought forward for deliberation before the national legislature.[145] This gap allows the State to use the 'compelling state interest' criteria to violate individual privacy in future cases. The authors have used the OECD principles as basic privacy protection guidelines. These

---

[142] *Puttaswamy* (n 75).

[143] Vrinda Bhandari and others, 'An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict' (2017) 11 IndraStra Global 1.

[144] Mariyam Kamil, 'The Aadhaar Judgment and the Constitution – II: On Proportionality (Guest Post)' (*Indian Constitution Law and Philosophy*, 30 September 2018) <https://indconlawphil.wordpress.com/2018/09/30/the-aadhaar-judgment-and-the-constitution-ii-on-proportionality-guest-post/> accessed 11 March 2021.

[145] Tathagata Satpathy, 'The Aadhaar: "Evil" Embodied as Law' (2017) 7 Health and Technology 469.

guidelines need to be incorporated into the national privacy laws and the strategies which are implemented by governments across the globe. As an immediate step, countries could organise privacy management programs to urgently curtail the gross violations of privacy. It is also pertinent for the lawmakers to consider, along with the technical aspects, the ethical repercussions of violation of freedom, individual autonomy, and fairness. Therefore, both technological and moral implications must be thoroughly considered as we move forward into the digital age.