Page 1142 - 1154 **DOI:** *https://doij.org/10.10000/IJLMH.111422*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 4

2021

Facial Recognition Technology and its Impact on Privacy Rights of Children

KONINA MANDAL[1]

ABSTRACT

India is gradually becoming the data center hub of the world. Covid-19 has contributed towards this growth by pushing the nation to adapt to the virtual world, thereby, accelerating our technological capabilities. With these technological advancements such as Facial Recognition Technology, India is entering into Mass Surveillance State and the danger of data breaches and privacy violations is also looming large. As fast as the nation is modernizing, the pace of legislation to incorporate data protection has been, by far, unsatisfactory. Although the potential violation of privacy affects all strata of society, children are, arguably, the most vulnerable group. Educational institutes such as schools and colleges are some of the biggest perpetrators in the privacy violation of kids. Thus, this issue of violation of privacy via the employment of Facial recognition technology requires immediate attention as it is a major threat to our fundamental right to privacy and human rights. Therefore, this research paper attempts to trace the impact of these technologies on privacy rights, especially children, by critically examining relevant statutes from the national as well as international perspective. Further, the paper explores the violation of privacy by educational institutes such as schools and colleges. Lastly, the paper concludes by recommending some solutions to curb the blatant abuse of the privacy rights of children.

Keywords: *Privacy, FRT, children, data protection.*

I. INTRODUCTION

Privacy has a chequered meaning throughout history; the definition itself differs according to the era, society, moral notions, culture, location, and individuals. In 1890, we first came across the privacy notion as the "right to be let alone". Since then, this concept has evolved and become an intricate fundamental human right for many countries.[2] Privacy in Today's world is the basic perception of human dignity, and although there is no harmonized definition attached

[1] Author is a Lecturer at Jindal Global Law School, OP Jindal Global University, India

[2] Adrienn Lukács, WHAT IS PRIVACY? THE HISTORY AND DEFINITION OF PRIVACY, http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf.

 [ISSN 2581-5369]

to the concept, it is indispensable for a democratic country such as India[3].

However, with the technological advances and the pandemic state, India is headed towards a mass surveillance state.[4] Artificial intelligence technologies like facial recognition technology (hereinafter referred to as "FRT") are being used by the police forces, civil departments, aviation, and educational institutes. Even though India does not have any data protection laws that define the scope of this FRT, the government is still publicly exploiting its power to collect private data just like in the book "1984". The very act of using these technologies without any legal protection framework violates article 21 of the Indian constitution as well as the internal laws such as Article 17 of the International Covenant for Civil and Political Rights and Article 12 of the Universal Declaration of Human Rights.[5]

Thus, it becomes imperative to examine FRT from a modern perspective. That is why these paper endeavors to critically examine the FRT and its impact on society's privacy rights with a special focus on the most vulnerable category, i.e., Children. The paper employs doctrinal research whereby the author analyses the applicable statutory provisions of domestic as well as international law. Further, the paper explores the violation of privacy by educational institutes such as schools and colleges. Lastly, the paper concludes by recommending some solutions to curb the blatant abuse of the privacy rights of children.

II. BACKGROUND

Artificial intelligence technologies like facial recognition technology are being used by the police forces, civil departments, aviation, and educational institutes. Even though India does not have any data protection laws that define the scope of this FRT, the government is still publicly exploiting its power to collect private data. The very act of using these technologies without any legal protection framework violates article 21 of the Indian constitution as well as the internal laws such as Article 17 of the International Covenant for Civil and Political Rights and Article 12 of the Universal Declaration of Human Rights. [6]

Privacy has a varying meaning throughout history, the definition itself differs according to the

[3] Privacy, Protection of Personal Information and Reputation Rights, Discussion Series Paper Series on Children's Rights and Business in digital World, UNICEF, 7, https://sites.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf.

[4] Akshit Sangomla, Is India moving towards a mass surveillance state Down To Earth (2020), https://www.downtoearth.org.in/video/science-and-technology/is-india-moving-towards-a-mass-surveillance-state-73374 (last visited Jul 6, 2021).

[5] Prajakta Pradhan, How Facial Recognition Systems Threaten the Right to Privacy Tech Law Forum @ NALSAR (2020), https://techlawforum.nalsar.ac.in/how-facial-recognition-systems-threaten-the-right-to-privacy/ (last visited Jul 6, 2021).

[6] Pradhan, *supra* note at 4.

era, society, moral notions, culture, location, and individuals. In 1890, we first came across the privacy notion as the "right to be let alone". Right to Privacy for children includes the right to be free from outside interference, the right to be left alone along with the freedom to grow up without constant surveillance.[7] However, this gets disregarded in the attempt to provide protection and safety to children, although it is possible to simultaneously maintain privacy as well as safety.[8]

The Privacy and Freedom of Expression in the Age of Artificial Intelligence (2018) Report of 2018 has stated that any form of mass surveillance that interferes with privacy can be justified only if it is prescribed by law to achieve a legitimate aim, along with being proportionate to the aim pursued in.[9] The Privacy Judgement of 2017 has also stated that any breach of the right to privacy has to be proportional to a legitimate aim.[10]

III. GOVERNING LAWS

1. National Perspective

Article 21 of the Constitution reads as "No person shall be deprived of his life or personal liberty except according to a procedure established by law[11]." Herein, the article mentions a 'person' which includes every individual who is an Indian citizen or not of India. However, we fail to realize that the most serious threat to privacy is experienced by children since there is a greater range of actors than any other group. Since a child's right to privacy for Indian parents would be alien terminology, they tend to over-exposure on social media, exploit private spaces or create identity crises. Parents are considered to be the biggest violators of their children's privacy due to the prevalent moral beliefs. [12]. This makes children a vulnerable demographic who are not aware of their rights. The problem becomes even severe when they are further surveillance in public spaces.

Further, there are statutory laws in place which are specifically for the welfare of the children. The Juvenile Justice Act, 2015(hereinafter referred to as "JJ Act") has a Principle which deals with the right to privacy and confidentiality. It states that every child shall have a right to protection of his privacy and confidentiality, by all means, and throughout the judicial process.

[7] Nila Bala, The Danger of Facial Recognition in Our Children's Classrooms, 18 DUKE L. & TECH. REV. 249, 253 (2020).
[8] Id., at 253
[9] UC Berkeley Human Rights Center Research Team, Memorandum on AI and Children's Rights, UNICEF, 30 (2019), https://www.unicef.org/innovation/media/10501/file/Memorandum%20on%20Artificial%20Intelligence%20and%2 0Child%20Rights.pdf.
[10] K.S. Puttaswamy and Another v. Union of India (2017) 10 SCC 1, at ¶309.
[11] INDIA CONST. art 21.
[12] Geeta Chopra, Rights in India Challenges and Social Action, (1st Ed, 2015).

While Protection of Children from Sexual Offences (POCSO) Act, 2012 ensures that children have the right to privacy during the pre-trial and trial process. These parts ensure that a child has the right to privacy when it comes to judicial procedures however they don't explicitly mention the importance or a protection framework for a child to know their right to privacy. Schools and colleges have exploited their students in the name of protecting them and since most of the students are unaware that this right even exists due to the normalcy of exploitative nature of both public and private life. This exploitation by Schools and Colleges has been further dealt with in length and breadth in subsequent headings.

The right to privacy finds further strength through The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. (Hereinafter referred to as "Privacy Rules") According to Section 3 of Privacy Rules, biometrics are termed as sensitive personal data. The term biometrics is defined under Section 2(b) of Privacy Rules as facial patterns, eye retinas, and irises and voice patterns, among other things, all of which can be stored by CCTV footage, coupled with FRT.

According to section 6, consent needs to be obtained from the information provider before disclosing any kind of sensitive personal data. However, since minors cannot consent, the existing Rules do not provide clarity when it comes to the transfer and disclosing of biometrics of children. Moreover, the Rules apply only to body corporates, which does not include the government.[13] This would imply that students' data can be used, without any restrictions, by government bodies.

While on social media, children have the option to be selective about what data they share, they do not have the same choice in schools. Most schools in India have strict uniforms that prevent them from covering their faces, hence, making it difficult for them to hide their faces (and their biometrics) from surveillance technology. Additionally, the fact that students are compelled to expose their sensitive personal data brings into question the idea of 'informed consent of FRT' in schools.[14]

2. International Perspective

The Convention on the Rights of the Child (CRC) has a specific provision for children's right to privacy. Article 16 of the CRC states that "No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful

[13] Sangomla *supra* note at 3.
[14] Mark Andrejevic & Neil Selwyn, Facial recognition technology in schools: critical questions and concerns, Learning, Media and Technology, 45:2, 115-128, (2020), DOI: 10.1080/17439884.2020.1686014.

 [ISSN 2581-5369]

attacks on his or her honour and reputation," and reaffirms that "the child has the right to the protection of the law against such interference or attacks."

In a nutshell, the provision summarizes that:

- They have the right to a private family life,
- They have the right to a private space where they can go to be alone, even if they're in an institution.
- They have the right to keep their phone calls and emails private.

Furthermore, CRC can read in consonance with JJ Act because JJ Act has a purpose to uphold the standards of all the international instruments. This act becomes essential when we are discussing the implementation of facial recognition technologies in schools. Since children have limited levels of literacy and comprehension skills involving law, the state should be more concerned about this technology.

Article 16 would also imply that every child has the right to a private space, even if they are within a public institution.[15] However, when children are brought up in surveilled environments, where FRT monitors every movement of theirs, it can lead to a chilling effect on the freedom of expression, right to privacy, and freedom of assembly and association.[16] In a commentary on the ICCPR by the Human Rights Committee,[17] it was stated that all individuals should have the right to know and consent to personal data being stored in a digital format.[18] As mentioned earlier, since students often have no choice but to disclose their facial data, including voice patterns, their biometric data gets stored without their informed consent, thus, violating international standards.

Due to the lack of transparency of digital technology, along with its complexity, merely 'having rights' or 'having knowledge' does not help to protect people. In an article in the Freedom Report, it was stated that the responsibility should not be on children or their parents but rather, on legislators, data controllers, and regulators.[19] Keeping in mind Article 3 of the UNCRC, which urges states to work towards the best interest of children, a more transparent

[15] Children and Young People's Commissioner (Scotland), UNCRC Simplified, https://cypcs.org.uk/rights/uncrc/articles/article-16/

[16] (Dr.) Eva Lievens, The Rights of the Child in the Digital Environment: From Empowerment to De Responsibilisation, Rights Foundation, https://freedomreport.5rightsfoundation.com/the-rights-of-the-child-in-the-digital-environment-from-empowerment-to-de-responsibilisation (last visited Jul 6, 2021).

[17] The commentary can be applied to analyze the UNCRC as well since both the ICCPR and the UNCRC define privacy in the same language.

[18] Office of the High Commissioner For Human Rights, CCPR General Comment No. 16: Article 17, UNHRC (1988) https://www.refworld.org/docid/453883f922.html (last visited Jul 6, 2021).

[19] Lievens *supra* note at 15.

system should be introduced.

Facial recognition systems are mostly tested on adults and hence, cannot accurately work for children.[20] This increases the potential of children being misidentified in schools for acts they did not engage in and for behavior they did not portray.

Children also have the 'right to obscurity', as a part of the right to privacy. Students develop a sense of identity in schools and often prefer "blending into the background";[21] this, however, becomes impossible due to FRT which has led to the "normalized elimination of practical obscurity".[22]

IV. CONSTITUTIONALITY OF FRT

In the iconic judgment in 2017[23], the Supreme Court of India stated that the Right to Privacy is a part of the fundamental right guaranteed under Article 21 of the Indian Constitution. This judgment ensured that an individual has the right to consent before any data is collected. The court also laid down the proportionality test to set a standardized rule where an act of collecting personal information can or cannot be recognized as a violation of the right to privacy. The rule tests the proportionality between the object and the means to achieve it, and procedural standards to check the abuse of State interference. However, there was no legal protection when it comes to the Automated Facial Recognition System (hereinafter AFRS) and personal data protection in India. Subsequently, The Indian Government, in 2019, introduced the Personal Data Protection Bill (PDP), in the Lower House of the Parliament (Lok Sabha) which made AFRS legal. However, the proposed bill left out significant elements of the privacy issue. The proposed Bill provided the Government with three major exemptions: it grants the right to collect personal data without consent in matters relating to the security of the state and public order. Secondly, the personal data of an individual could also be collected to prevent or detect any offense. Lastly, the Government could also collect and use personal data for 'reasonable' purposes. It allowed the government to use these technologies in public spaces arbitrarily. Instead, the Parliament should have made a strong statute on its privacy charter protecting everyone their freedom from forms of behavior collection and mass data analysis that are demonstrably harmful given our democratic nature[24].

[20] Karen Hao, Live Facial Recognition is Tracking Kids Suspected of Being Criminals, MIT Technology Review (2020) https://www.technologyreview.com/2020/10/09/1009992/live-facial-recognition-is-tracking-kids-suspected-of-crime.
[21] Andrejevic & Selwyn *supra* note at 13.
[22] Andrejevic & Selwyn *supra* note at 13.
[23] K.S. Puttaswamy and Another v. Union of India (2017) 10 SCC 1 at ¶309.
[24] Mishi Chaudhary & Eben Moglan, Why India must resist facial recognition tech, Hindustan Times, Feb 15, 2020, https://www.hindustantimes.com/analysis/why-india-must-resist-facial-recognition-tech-opinion/story-

V. USE OF FRT IN THE EDUCATIONAL SECTOR

The educational sector has become one of the public settings where the FRT is being used extensively since it plays a crucial role in monitoring and implemented disciplinary actions[25]. Since as a society, we already believe in increasing the use of surveillance in the name of protecting and securing young people, this tool has been disguised as a gift for the Indian government.

This technology was accepted by some of the schools and colleges due to various challenges that they face. Firstly, problems like fake attendance and proxies are common phenomena in Indian classrooms, FRT in school seems like the bridge to overcome the gaps and omission that arises when teachers are conducting the roll-call of a vast number of students. Secondly, the school traditionally has a custom of collecting and maintaining photographic records of the student accompanying with a detailed personal database, the technology is just acting as a better mechanism for similar purposes. The extensive practice of video monitoring and CCTV in schools is already a norm and adding the FRT is just an enhancement. Thirdly, this technology is being used in the current pandemic, virtual learning context wherein the institutes can control access to online education as well as using webcam-based facial recognition to authenticate online learners. Some schools are also using e-assessment security i.e. verifying the identity of students taking computer-based tests and examinations, and confirming their continued presence during the whole examination period.

The rationale behind the institutes opting for this technology falls deficient due to manifold reasons which are as follows -

1. The Supreme Court held that there has to be consent of the parties before the data collection. Here, since this responsibility falls on the legal or local guardian to consent on behalf of their child, the lack of attention given to a child's privacy at home can result in adults supporting surveillance in public spheres too. Considering an individual wants to opt out of this system, the system even then has to scan the student's face before it can recognize that they have opted out. For this system to not be used in schools, collective action has to be taken by parents who are often uninformed and lack knowledge regarding the effects of this FRT. This tool then acts as a counterproductive system that creates a facade of free consent.

2. Multiple studies have proven that surveillance has a detrimental effect on free speech. Students modify their behavior when they are been observed wherein they are less likely to speak

18O8lvhiXj5L2D7cW3gCqJ.html (last accessed at Jul 6, 2021).

[25] Andrejevic & Selwyn *supra* note at 13.

freely or act individually. Self-censorship and pushing conformist ideology in students might result in 'idealist' behavior but this would be at the expense of their true expression which is a fundamental right in a democratic country like India. The fear of being aligned with a group due to different ideologies or how one may be viewed by an authority figure can also cause a psychological impact on children. Since there is no tangible evidence to prove otherwise, making school a testing ground can put the children in jeopardy.

3. Surveillance conducted with facial recognition systems is intrinsically oppressive. Since these are implemented to regulate, control, and discipline the minds and bodies of students. This technology will further increase the harm by enhancing the authoritarian tendencies of the schools. The technology "punishes nonconformity" where students will have to dress and appear in specific ways. For example, many reports highlight that schools in India often over-monitor Girls when it comes to dressing and behavior, this will then allow them to further restrict their movement and conform to their notions of right and wrong. Hence, if one doesn't allow through, they will be called out or lose their attendance for the day which will ultimately result in systematic abuse.

4. One of the common arguments used by schools is along the lines of 'if you have nothing to hide then you have nothing to fear'. This overlooks different needs and requirements of some students, for example, a student should not face substantial curtailment just for not following the standardized way of doing things. A lot of students have legitimate coping strategies and an invaluable means of 'doing' school on their terms wherein the schools help them develop that sense of social identity and confidence in a supportive and nurturing setting.

5. This technology is ‘detecting’ the gender and race of those individuals that it identifies where it arbitrarily divides the students into boxes. Even if the identifications are technically accurate, it can be argued that sorting students into socially constructed racialized and/or gendered categories remains a discriminatory practice – conflating biological characteristics with social attributes.

VI. ISSUES WITH FRT VIS-À-VIS RIGHT TO PRIVACY

As earlier mentioned, The Privacy and Freedom of Expression in the Age of Artificial Intelligence (2018) Report of 2018 has stated that any form of mass surveillance that interferes with privacy can be justified only if it is prescribed by law to achieve a legitimate aim, along with being proportionate to the aim pursued in.[26] A similar stance was taken by the Apex

[26] UC Berkeley *supra* note at 8.

Court in the Puttaswamy judgment whereby it recognized that any breach of the right to privacy has to be proportional to a legitimate aim.[27]

Right to privacy includes the Right to be forgotten,[28] which implies that everyone has the right to have their personal information removed from online algorithms and directories. However, FRT violates this right since it gathers students' information and holds on to that data.[29] Additionally, 'false positives' are also created, which can lead to discriminatory profiling.[30] Children, whose personalities and voices change at a very fast pace, should not be subject to profiling and have data embedded into the system that cannot be altered.

Even if students have the option of opting out of providing biometric data since most schools have CCTV cameras, images from that footage can be used to extract biometrics even without the students' consent.[31]

AFRS is also inaccurate with women, racial minorities, non-binary persons, and children, implying that the chances of false positives and misidentification are higher for these groups of people. Thus, AFRS does not just violate privacy but also breaches the right to equality and the right against discrimination. A UNICEF memorandum, speaking out against AI and FRT in education, stated that such technology may affiliate a woman (or what appears to be a woman's face) with subjects/occupations related to humanities and art;[32] while for a male, it may associate it with STEM subjects. The potential to manipulate classroom opportunities also violates the right to be treated equally**.**

Additionally, a heavily monitored environment confines children to self-censorship and social control, while going against the freedom of choice, freedom of expression, and self-determination[33] all of which are entailed in the constitution of India.

VII. RECOMMENDATIONS

In this paper, we have meticulously analyzed the position of FRT in Indian as well as the International scenario. We have also discussed the probable misuse of FRT especially against the rights of privacy of a minor. In the light of these, certain recommendations can be suggested

[27] K.S. Puttaswamy and Another v. Union of India (2017) 10 SCC 1, at ¶309.
[28] *Id*, at ¶634.
[29] UC Berkeley *supra* note at 8.
[30] *Id.*
[31] Anushka Jain, The Problems with Facial Recognition Technology Operating in a Legal Vacuum, Panoptic Tracker (2020) https://panoptic.in/case-study/problems-with-facial-recognition-technology-operating-in-a-legal-vacuum (last visited Jul 6, 2021).
[32] UC Berkeley *supra* note at 8.
[33] *Id.* at 11.

to minimize, if not eliminate, the risk associated with the use of FRT in our private life.

One of the primary recommendations can be a complete ban on the employment of AFRS in the school and colleges, especially for pre-primary and primary level students. This will provide students a safer environment to grow and express themselves. Ban on such technologies will remove ever prevailing hindrance in the personality and identity development of these young kids.

While advocating for a complete ban of AFRS, another recommendation is the deployment of certain regulatory measures temporarily. According to the European General Data Protection Regulation, recital 58 states that since children require special protection, any data processing involving minors should be in "clear and plain language".[34] A similar approach can be availed in our country by incorporating these provisions in the Data Protection Bill, Information Technology Act, 2000, and Privacy Rules. These will safeguard the rights and interests of minors in the regulation of their private affairs.

Moreover, while implementing FRT, consent should be taken wherever possible. In instances where consent cannot be taken due to practical reasons, disclaimers should be provided by the authority. These authorities shall maintain utmost privacy and deploy adequate security measures to securitize the data of the parties which they are collecting. Furthermore, such authorities shall be held liable for the breach of these earlier recommended provisions.

Lastly, raising awareness among children and their parents is also suggested. The govt. along with the NGOs, educational institutes and technological pioneers should initiate a dialogue for the better regulation and implementation of earlier recommendations.

VIII. CONCLUSION

Implementation of these FRT has a devastating effect on the children who are incapable of making such decisions. In the name of safety and protection, children are often subjected to FRT without them having any control of their privacy. According to a Global Survey, India is the third-worst country when it comes to data privacy.[35] The report also mentions how government agencies have the power to decrypt and monitor data without prior approval from the home secretary. According to a case study by The Panopticon Tracker, FRT systems in

[34] European GDPR: Recital 58 reads as –
"Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand."
[35] Yash More & Shailendra Shukla, Analysing the Impact of the Personal Data Protection Bill, 2019 on the Fundamental Right to Privacy, 6 INDIAN J.L. & PUB. POL'y 42, 58 (2020).

India are being developed and used by institutions without any technical thresholds.[36] With the possibility of faulty technology, along with the dearth of data protection, children become especially vulnerable when exposed to constant surveillance.

Parents post pictures of their children online; the ramification of this is the fact that these pictures can be added to facial recognition databases without their consent or knowledge to improve FRT algorithms in schools.[37]

Subsequently, the legal infrastructure to regulate such use and storage of enormous data is grossly under-compensating. Therefore, the need of the hour is to tighten up and get a hold on such blatant abuse of the right to privacy of the children; at least till they attain the majority to make better decisions pertaining to their private affairs. As India is gearing up to become a digital powerhouse of the world, the State shall introduce and incorporate better legislative reform to regulate the digital affairs of its citizens. These will not only protect its citizens but also empower them to lead a greater dignified life.

*****

[36] Jain *supra* note at 30.
[37] Lindsey Barrett, Ban Facial Recognition Technologies for Children – And for Everyone Else, 26 B.U. J. Sci. & TECH. L. 223 (2020).

 [ISSN 2581-5369]

IX. REFERENCE

1. Adrienn Lukács, WHAT IS PRIVACY? THE HISTORY AND DEFINITION OF PRIVACY, http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf.
2. Akshit Sangomla, Is India moving towards a mass surveillance state Down To Earth (2020), https://www.downtoearth.org.in/video/science-and-technology/is-india-moving-towards-a-mass-surveillance-state-73374 (last visited Jul 6, 2021).
3. Anushka Jain, The Problems with Facial Recognition Technology Operating in a Legal Vacuum, Panoptic Tracker (2020) https://panoptic.in/case-study/problems-with-facial-recognition-technology-operating-in-a-legal-vacuum (last visited Jul 6, 2021).
4. Children and Young People's Commissioner (Scotland), UNCRC Simplified, https://cypcs.org.uk/rights/uncrc/articles/article-16/
5. Geeta Chopra, Rights in India Challenges and Social Action, (1st Ed, 2015).
6. Karen Hao, Live Facial Recognition is Tracking Kids Suspected of Being Criminals, MIT Technology Review (2020) https://www.technologyreview.com/2020/10/09/1009992/live-facial-recognition-is-tracking-kids-suspected-of-crime.
7. Mark Andrejevic & Neil Selwyn, Facial recognition technology in schools: critical questions and concerns, Learning, Media and Technology, 45:2, 115-128, (2020), DOI: 10.1080/17439884.2020.1686014.
8. Mishi Chaudhary & Eben Moglan, Why India must resist facial recognition tech, Hindustan Times, Feb 15, 2020, https://www.hindustantimes.com/analysis/why-india-must-resist-facial-recognition-tech-opinion/story-18O8lvhiXj5L2D7cW3gCqJ.html (last accessed at Jul 6, 2021).
9. Nila Bala, The Danger of Facial Recognition in Our Children's Classrooms, 18 DUKE L. & TECH. REV. 249, 253 (2020).
10. Office of the High Commissioner For Human Rights, CCPR General Comment No. 16: Article 17, UNHRC (1988) https://www.refworld.org/docid/453883f922.html (last visited Jul 6, 2021).
11. Prajakta Pradhan, How Facial Recognition Systems Threaten the Right to Privacy Tech Law Forum @ NALSAR (2020), https://techlawforum.nalsar.ac.in/how-facial-recognition-systems-threaten-the-right-to-privacy/ (last visited Jul 6, 2021).

12. Privacy, Protection of Personal Information and Reputation Rights, Discussion Series Paper Series on Children's Rights and Business in digital World, UNICEF, 7, https://sites.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf .UC Berkeley Human Rights Center Research Team, Memorandum on AI and Children's Rights, UNICEF, 30(2019), https://www.unicef.org/innovation/media/10501/file/Memorandum%20on%20Artificial%20Intelligence%20and%20Child%20Rights.pdf.

13. Yash More & Shailendra Shukla, Analysing the Impact of the Personal Data Protection Bill, 2019 on the Fundamental Right to Privacy, 6 INDIAN J.L. & PUB. POL'y 42, 58 (2020).

*****