

The image features the Indian national flag (Tiranga) waving against a blue sky. The flag is partially obscured by a large, semi-transparent green circle and a vertical green rectangle. The Ashoka Chakra is visible on the white band of the flag.

STAKEHOLDER REPORT

Universal Periodic Review

41st Session – India

Submitted by PI

April 2022

privacyinternational.org

Stakeholder Report: Universal Periodic Review 41st Session: India

**This Universal Periodic Review (“UPR”) stakeholder report is
a submission by Privacy International**

1. Privacy International (PI) is a non-governmental organization in consultative status with ECOSOC. PI researches and advocates globally against government and corporate abuses of data and technology. It exposes harm and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change. PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy.
2. This stakeholder report focusses solely on concerns related to the use of education technology (EdTech) in India, and the subsequent processing (collection, analysis, retention and sharing) of children and teacher’s data in schools.

Uptake of EdTech in India and the impact of the pandemic

3. India’s educational system is the largest in the world, with over 250 million students,¹ 50% of whom attend publicly administered schools.²
4. Although India has long been developing several programs for the digitization of education in the country, most formal education was still implemented in the traditional way: in person. With the Coronavirus disease (COVID-19) pandemic, 1.5 million Indian schools were closed in March 2020³ and 247 million children enrolled in elementary and secondary schools were impacted.⁴ It is noteworthy that education technologies were already heavily used in after-school tutoring, which is very popular in India to supplement school programs and prepare students for entrance exams.⁵
5. Given this turn of events, investment in EdTech in the country grew dramatically. The current market size is about \$700–800 million and should become \$30 billion in the next 10 years.⁶ The company Byju increased its activities by 150% in the first month of the lockdown,⁷ while Edumarshal witnessed a 250% surge over the first

three-month period.⁸ From January 2020 onwards, three Indian EdTech startups have turned into unicorns—i.e., companies valued above \$1 billion – and one into a decacorn – i.e., companies valued above \$10 billion.⁹ Nevertheless, much of the investment in the sector is still foreign: from April 2000 to June 2020, there was an inflow of \$3.29 billion in foreign direct investments (FDI).¹⁰

6. Despite the immense growth of this sector, only 25% of children had access to digital devices before the pandemic¹¹. Furthermore, the National Institution for Transforming India (NITI) Aayog (Hindi for Policy Commission) Sustainable Development Goals (SDGs) India Index 2020-2021 report has revealed that only 55% of Indian people have an Internet connection and 84% use data to connect to the Internet.¹²
7. While recognizing the unique circumstances of the pandemic, the UN Special Rapporteur on the Right to Education highlighted that ‘Past failures to build strong and resilient education systems and to fight entrenched inequalities have had a dramatic impact on the most vulnerable and marginalized, a situation to which no temporary measure adopted in haste could have fully responded.’¹³
8. India has a positive obligation to take necessary steps to ensure the enjoyment of this right as protected by Article 8 and 29 of the UN Convention on the Rights of the Child (‘UNCRC’).

Right to privacy and access to education: Facial recognition

9. The enjoyment of the right to education cannot be understood in isolation of the other rights of the UNCRC, including the right to privacy.¹⁴ Article 16, UNCRC provides that “No child shall be subjected to arbitrary or unlawful interference with [their] privacy”. Any interference should be in accordance with law, necessary to achieve a legitimate aim, and the legal framework should provide adequate and effective safeguards against abuse. The best interests of the child should be a primary consideration (Article 3, UNCHR).
10. PI is concerned that the use of EdTech poses unique and grave threats to children’s privacy and their right to access to education should not be conditional on the loss of their privacy. As the UN CRC Committee has underlined ‘Children do not lose their human rights by virtue of passing through the school gates’.¹⁵ The use of biometric technologies, such as facial recognition

technologies ('FRT') in EdTech without adequate safeguards can have significant harms.

11. India is a country that intensively uses biometric technologies in the most diverse situations, and education is no exception.¹⁶ We are particularly concerned about the increasing use of FRT in schools in India. The use of FRT has a seismic impact on the way society is monitored. The roll out of such intrusive technology does not only pose significant privacy and data protection questions, but also ethical questions around whether modern democracies should ever permit its use. For example, the radical introduction of FRT will inevitably result in the normalisation of surveillance across all societal levels and accordingly cast a "chilling effect" on the exercise of fundamental rights, such as our freedom of expression or our right to protest.
12. The introduction of such intrusive technologies, as FRT, in schools where young minds are formed and shaped amplifies these concerns. We want to raise the alarm as FRT seems to be introduced without appropriate prior consideration, due process, legal framework, or appropriate safeguards. We would like to highlight two initiatives for the use of facial recognition tools by the public authorities in the education environment hereinafter.
13. The first is that facial recognition is being used to provide students access to academic documents, which was apparently introduced without any prior human rights risk and impact assessment, including a data protection impact assessment, and without appropriate legal and security safeguards.
14. The Central Board of Secondary Education (CBSE) has started using facial recognition technology to provide students with access to their academic documents for classes 10 and 12.¹⁷ This repository is hosted on DigiLocker, an Aadhaar-based¹⁸, cloud-based locker, and doesn't have a privacy policy. In their response to a freedom of information request, CBSE said that "they were not using facial recognition technology[;] instead[,] they were using face matching technology."¹⁹ In response to another information request, the same institution though stated that its facial recognition system does not have a privacy policy because it is a "simple face matching process."²⁰ A source from MediaNama affirmed that "the system has just been launched, and the department will rectify any errors along the way".²¹ These responses suggest that data protection issues were not thought through neither beforehand nor as it was rolled out. Currently,

India does not have a comprehensive data protection law- the bill pending in Parliament as well as the report submitted by a Joint Parliamentary Committee have carved out a separate section when it comes to processing of children data and the responsibility of the data fiduciaries while processing children's data.

15. An even more serious situation has occurred in Delhi, a territory where facial recognition cameras have been installed in classrooms, which also allows parents to monitor their children.²² Such use of FRT is particularly concerning. First, constant surveillance can hinder the development of children's autonomy by creating a space where mistakes are not tolerated, use of facial recognition software in this context may severely impact the children's right to education and their freedom of expression.²³ Second, facial recognition has a lower performance in children and also in people of color. As a result, the chance of false negatives and false positives in this group is high. Given the greater vulnerability of children in this stage of life, the mistaken involvement of law enforcement procedures poses severe risks to children's well-being, health, educational and professional prospects, and freedoms.²⁴ Finally, from the information collected, it was not possible to know whether the system also supports emotion recognition. If this is the case, this could generate the stigmatization of normal behavior²⁵ and generate several grave negative effects to children's development by amplifying feelings, such as anxiety and fear.

16. In addition, in terms of public procurement, no information was found regarding the company that provides the technology and the CCTV cameras to Delhi schools and what kind of public procurement procedure was used. Regarding the CBSE system, the institution affirmed that no private company was involved and that the system was developed in technical collaboration with the National e-Governance Division, under the IT Ministry. However, due to the large extent of existing public-private partnerships in India in this area, it is not known, for example, if this data would be stored on private servers or if it would at any time be shared with any private actor. States ought to adhere to certain formal processes for procuring and assessing the services of private companies for delivery of public duties.²⁶

17. India is using extremely dangerous technologies without assessing the impact on fundamental rights and without establishing safeguards for their protection. The Puttaswamy judgement that upheld the right to privacy also consisted of a three

prong test to justify the invasion of privacy of a person.²⁷ The three requirements were: legality (the justification must be backed by law), legitimate aim (where there is a goal that needs to be reached e.g., national security) and proportionality (the requirement must be proportional to the aim sought).

18. In the case of use of FRT in schools, it fails the three prong test laid out in Puttaswamy. It is not backed by law, there is no necessity to deploy FRT in schools and it is definitely not proportionate measure to the objective sought to be achieved (which also vary from recording the attendance of students to students accessing their documents).
19. Biometric data, such as facial characteristics data, is particularly sensitive and revealing of individual's characteristics and identity. As such it has the potential to be gravely abused.²⁸ The European Union's General Data Protection Regulation (GDPR) treats biometric data used for identification purposes as "special category data", meaning it is considered more sensitive and in need of enhanced protection.²⁹
20. Any interference with the right to privacy needs to comply with the principles of necessity and proportionality. The principle of necessity 'implies that restrictions must not simply be useful, reasonable or desirable to achieve a legitimate government objective,' but rather, that 'a State must demonstrate in 'specific and individualized fashion the precise nature of the threat' that it seeks to address, and a 'direct and immediate connection between the expression and the threat'.'³⁰
21. The use of biometric data presents a unique set of concerns. These are neatly summarised in the UN High Commissioner for Human Rights report on the right to privacy in the digital age, as biometric:
22. 'Data is particularly sensitive, as it is by definition inseparably linked to a particular person and that person's life, and has the potential to be gravely abused. For example, identity theft on the basis of biometrics is extremely difficult to remedy and may seriously affect an individual's rights. Moreover, biometric data may be used for different purposes from those for which it was collected, including the unlawful tracking and monitoring of individuals. Given those risks, particular attention should be paid to questions of necessity and proportionality in the collection of biometric data. Against that background, it is

worrisome that some States are embarking on vast biometric data-base projects without having adequate legal and procedural safeguards in place.’³¹

23. The High Commissioner for Human Rights has already recommended to states that FRT should never be used to identify individuals in public gatherings, such as protests.³² Introducing FRT in schools is even more concerning.

24. Recommendations

- PI recommends India to ban the use of facial recognition technologies in schools.
- PI recommends India must review its legal framework to ensure it effectively regulates the authorization and the use of EdTech for the intended legitimate purpose and includes robust and effective safeguards.
- PI urges India to ensure that robust human rights due diligence processes (including data protection impacts assessments) are in place, that include into their scope the early stages of the design and development of an EdTech technology, as well as stages of deployment and use. Details of the processes in place should be made public and available for review.
- PI recommends that India, when awarding a contract to an EdTech company, must demonstrate adherence to formal public procurement processes and must put in place formal documentation governing the partnership.
- PI urges India to ensure that applications that specifically process children's data, such as EdTech apps, do not use the data for targeted advertising and profiling and the EdTech apps practice data minimisation and retain data only till when necessary.
- PI recommends that India takes all necessary measures to ensure that all children and young children enjoy their right to education regardless of race, gender or disability.
- In addition, we suggest that India as a matter of urgency, adopts special, targeted measures, including through international cooperation, to address and mitigate the impact of the pandemic on vulnerable groups, as well as on communities and groups subject to structural discrimination and disadvantage.
- We urge India to put in place policies and measures to ensure education preparedness in cases of future emergency.

¹ India Brand Equity Foundation, Education & Training Industry in India, 22 September 2021, <https://www.ibef.org/industry/education-sector-india.aspx>

² Doraiswamy, H., Gupta, G., Kamath, D., & Sharma, S., 'India's distance learning response to the COVID-19 crisis. Central Square Foundation', EdTech Hub, September 2020, <https://doi.org/10.5281/zenodo.4705451>



- ³ Govt announces closure of all educational establishments across India till March 31, *The Times of India*, 16 March 2020 <https://timesofindia.indiatimes.com/home/education/news/govt-announces-closure-of-all-educational-establishments-across-india-till-march-31/articleshow/74659627.cms>
- ⁴ UNICEF, 'COVID-19: Schools for more than 168 million children globally have been completely closed for almost a full year, says UNICEF', Press release, 10 March 2021, <https://www.unicef.org/india/press-releases/covid-19-schools-more-168-million-children-globally-have-been-completely-closed>
- ⁵ Krishna, N., & Scharma, D., 'Making a Case for a 'Goldilocks' Regulation of the Ed-Tech Sector', *The Bastion*, 16 February 2021, <https://thebastion.co.in/politics-and/education/making-a-case-for-a-goldilocks-regulation-of-the-ed-tech-sector/>
- ⁶ Chandrasekaran, K., 'Indian EdTech industry's market size to reach \$30 billion in 10 years: Report', *The Economic Times*, 28 April 2021, <https://economictimes.indiatimes.com/tech/technology/indian-EdTech-industrys-market-size-to-reach-30-billion-in-10-years-report/articleshow/82295097.cms>
- ⁷ Ullas, S. S., 'EdTech space sees massive growth amid lockdown', *The Times of India*, 3 April 2020, <https://timesofindia.indiatimes.com/city/bengaluru/EdTech-space-sees-massive-growth-amid-lockdown/articleshow/74956839.cms>
- ⁸ Mitter, S., 'This EdTech startup grew 250 pc amid coronavirus lockdown by digitising schools', *YourStory*, 12 May 2020 <https://yourstory.com/2020/05/EdTech-startup-grew-lockdown-digitising-schools-saas-platform/amp>
- ⁹ Bhalla, K., 'From Byju's to Eruditus – India now has four EdTech unicorns, thanks to a \$4 billion fund flowing in since 20', *Business Insider*, 14 August 2021, <https://www.businessinsider.in/business/startups/news/india-now-has-four-EdTech-unicorns-byju-unacademy-eruditus-upgrad/articleshow/85300757.cms>
- ¹⁰ Nishith Desai Associates, 'Doing Business in India: The Guide for US Businesses and Organizations entering and expanding into India', February 2021, https://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research_Papers/Doing_Business_in_India.pdf
- ¹¹ UNICEF, 'COVID-19: Schools for more than 168 million children globally have been completely closed for almost a full year, says UNICEF', Press release, 10 March 2021, <https://www.unicef.org/india/press-releases/covid-19-schools-more-168-million-children-globally-have-been-completely-closed>
- ¹² NITI Aayog, 'SDG India: Index & Dashboard 2020–21, Partnerships in the Decade of Action', NITI Aayog, Government of India, 2021 https://www.niti.gov.in/writereaddata/files/SDG_3.0_Final_04.03.2021_Web_Spreads.pdf
- ¹³ Report of the Special Rapporteur on the right to education on the Right to education: impact of the coronavirus disease crisis on the right to education – concerns, challenges and opportunities, A/HRC/44/39, 30 June 2020, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/158/03/PDF/G2015803.pdf?OpenElement>
- ¹⁴ UNCRC Committee, General Comment 1 (2001): The aims of education, CRC/GC/2001/1, 17 April 2001, para 6.
- ¹⁵ UNCRC Committee, General Comment 1 (2001): The aims of education, CRC/GC/2001/1, 17 April 2001, para 6.
- ¹⁶ Hickok, E., Bedi, P., Nair, A., & Sinha, A., 'Facial Recognition Technology in India', The Centre for Internet and Society, The Human Rights, Big Data and Technology Project (University of Essex, UK), August 2021, <https://cis-india.org/internet-governance/facial-recognition-technology-in-india.pdf>
- ¹⁷ The Times of India, 'CBSE introduces 'Facial Recognition System' for accessing digital documents', October 2020, <https://timesofindia.indiatimes.com/home/education/news/cbse-introduces-facial-recognition-system-for-accessing-digital-documents/articleshow/78809577.cms>
- ¹⁸ On Aadhaar concerns see, PI, 'ID systems analysed: Aadhaar', 2021, <https://privacyinternational.org/case-study/4698/id-systems-analysed-aadhaar>
- ¹⁹ Jain, A., 'A rose by any other name? CBSE's face matching technology is just facial recognition in disguise', *Panoptic Tracker*, 21 January 2021, <https://panoptic.in/case-study/a-rose-by-any-other-name-cbse-face-matching-technology-is-just-facial-recognition-in-disguise>
- ²⁰ Barik, S., 'CBSE rebuffs need for privacy policy of facial recognition tool: 'it's a simple face matching process'', *MediaNama*, 25 November 2020, <https://www.medianama.com/2020/11/223-cbse-facial-recognition-privacy-policy/>
- ²¹ Barik, S., 'CBSE says its facial recognition tool is a 'face matching algorithm': RTI', *MediaNama*, 29 January 2021, <https://www.medianama.com/2021/01/223-cbse-facial-recognition-algorithm/>
- ²² Bala, N., 'The Danger of Facial Recognition in our Children's Classrooms' (2020) 18 *Duke Law & Technology Review* 249–267.
- ²³ Bala, N., 'The Danger of Facial Recognition in our Children's Classrooms' (2020) 18 *Duke Law & Technology Review* 249–267.
- ²⁴ Barrett, L., 'Ban Facial Recognition Technologies for Children—And for Everyone Else', Boston University (2020) 26(2) *Journal of Science and Technology Law* 223–285.
- ²⁵ Bala, N., 'The Danger of Facial Recognition in our Children's Classrooms' (2020) 18 *Duke Law & Technology Review* 249–267.
- ²⁶ PI's Safeguards for Public-Private Partnerships, December 2021, <https://privacyinternational.org/our-demands/safeguards-public-private-surveillance-partnerships>
- ²⁷ Supreme Court of India, *Justice K.S. Puttaswamy (Retd) vs Union of India*, 26 September 2018.
- ²⁸ See report of the UN High Commissioner for Human Rights, 3 August 2018, A/HRC/39/29, <https://undocs.org/A/HRC/39/29>

²⁹ Article 9, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

³⁰ UN CCPR, General Comment No. 34: General comment no. 34, Article 19, Freedoms of opinion and expression, UN Doc. CCPR/C/GC/34, 12 September 2011, para 35

³¹ Report of the UN High Commissioner for Human Rights on the right to privacy in the digital age, 3 August 2018, UN Doc. A/HRC/39/29, <https://undocs.org/A/HRC/39/29>

³² Report of the UN High Commissioner for Human Rights on the Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests, 24 June 2020, A/HRC/44/24, https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session44/Documents/A_HRC_44_24_AEV.docx

