



Why you should be worried about facial recognition in educational spaces: PI's briefing

October 2024

privacyinternational.org



ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters:
our freedom to be human.



Open access. Some rights reserved.

Privacy International wants to encourage the circulation of its work as widely as possible while retaining the copyright. Privacy International has an open access policy which enables anyone to access its content online without charge. Anyone can download, save, perform or distribute this work in any format, including translation, without written permission. This is subject to the terms of the Creative Commons Licence Deed: Attribution-Non-Commercial-No Derivative Works 2.0 UK: England & Wales. Its main conditions are:

- You are free to copy, distribute, display and perform the work;
- You must give the original author ('Privacy International') credit;
- You may not use this work for commercial purposes;
- You are welcome to ask Privacy International for permission to use this work for purposes other than those covered by the licence.

Privacy International is grateful to Creative Commons for its work and its approach to copyright.

For more information please go to www.creativecommons.org.

Photo by Fred Moon on Unsplash

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

CONTENTS

01	What are facial recognition technologies?	06
02	Facial recognition in EdTech	08
03	Key concerns with FRT in educational spaces	03
	3.1 Erosion of Privacy	
	3.2 Lack of data protection safeguards	
	3.3 Surveillance and securitisation	
	3.4 Children's development	
	3.5 Discrimination: effectiveness and categorisation	
	3.6 Role of private sector	
04	What we want: Ban FRT in educational spaces	22
05	A roadmap to assessing compatibility of the use FRT in educational spaces with human rights standards	23

Summary

The rapid expansion of educational technologies (EdTech) has introduced serious concerns about human rights protection in educational spaces. This briefing explores the impact of facial recognition technology (FRT) and heightened surveillance in these settings, highlighting many complex and multifaceted issues that demand careful consideration from a human rights perspective. These issues include the erosion of privacy; the lack of data protection safeguards; the securitisation of educational spaces –that undermines the learning and growth processes–; the negative impact on children’s development; the perpetuation of bias and discrimination; as well as the role of private interests therein. It is crucial to ban FRT in educational spaces and stop its use now. At the end of the briefing, we share a roadmap of key issues that it is necessary to consider for anyone thinking of introducing FRT in educational spaces to help analyse its impact on human rights.

Introduction

The use of technologies in educational spaces has been rapidly expanding. It has accelerated further as a response to the COVID-19 pandemic to address the need for remote learning and virtual classrooms. As an example, according to Online Education, downloads of education applications in 2020 increased by 90 percent compared to the weekly average in late 2019.¹ While the focus has been on increasing access to the internet and the use of technology to uphold the right to education,

¹ UN Human Rights Council, ‘Report of the Special Rapporteur on the right to privacy on Artificial intelligence and privacy, and children’s privacy,’ UN Doc A/HRC/46/37, 25 January 2021, <https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F46%2F37&Language=E&DeviceType=Desktop&LangRequested=False>, para 106.

many education technologies (EdTech) and their implementation in schools, present serious issues and risks to human rights, in particular the right to privacy. Furthermore, the shift to online education has amplified existing power imbalances between EdTech companies and students and between state authorities, children, and parents.²

A set of particularly worrisome initiatives are those introducing facial recognition technologies (FRT) in educational spaces. FRT amplifies existing concerns related to EdTech and introduces additional ones, including its incompatibility with the right to privacy and data protection, heightened surveillance and securitisation within educational settings, interference with child development, and the enabling of discriminatory practices. This briefing provides an overview of deployment of FRT in educational settings, the key concerns that are raised by its use, and the significant issues relevant stakeholders should consider before using it.

2 *ibid.*

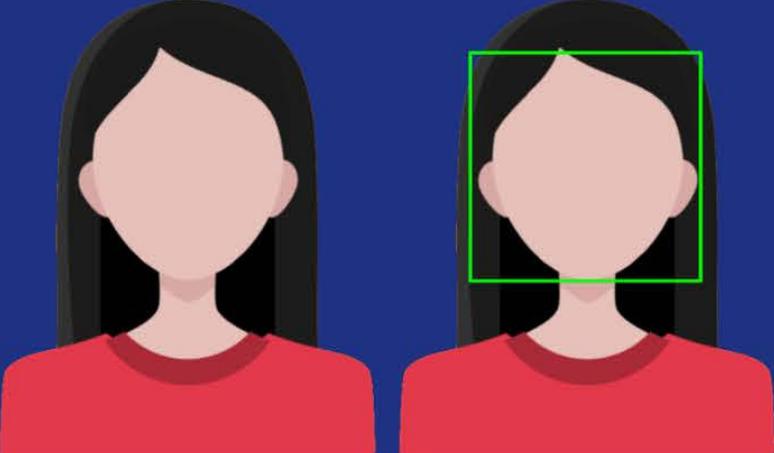
01 What are facial recognition technologies?

FRT is a technology that recognises faces in images or video, processes that data, and then uses it to record something about the person in the video sometimes in conjunction with other software. For example, the facial recognition software that the Indian state of Telangana intends to adopt for taking attendance in schools will be AI-enhanced. The system will capture a template based on 72 points on the face rather than photos of the end users. The technology works in three steps:

- 1. Face detection involves an image being processed to detect a face using cameras with software that collects and processes data about an individual's face.**
- 2. Face printing occurs when the software extracts facial features and summarises these features into numbers to make a "face print," which is as unique as a fingerprint.**
- 3. Face matching occurs when the software tries to match two or more faceprints to determine if they are the face of the same person.**

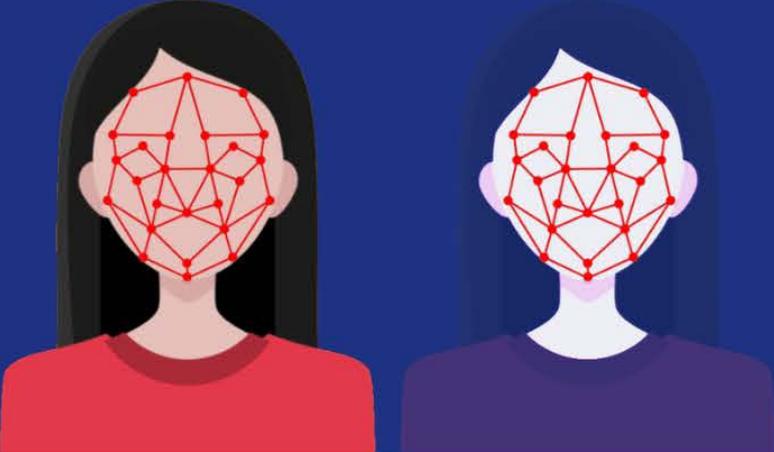
FRT can be used to verify, identify, and/or categorise an individual. Using it for verification purposes only involves a one-to-one comparison of two facial images usually presumed to belong to the same individual. This technology is like the one used when you attempt to unlock your mobile phone, if you have opted for that option. The system captures a new image of your face and compares it to the stored template. If there's a match within an acceptable level of similarity, the system verifies that you are the authorized user, and the device unlocks.

When used for identification purposes, the system compares the image



1. Face detection

An image being processed to detect a face.



2. Faceprinting

The software extracts and summarises these features to create a "faceprint".



3. Face matching

When the software tries to match two or more faceprints.

of an unknown person to a database of "known" faceprints to establish someone's identity. This technology is the kind most used by police forces. The digital equivalent of a line-up, the technology compares the faces it 'sees' to those in a database and often returns percentage probability matches.

Where FRT is used for categorisation purposes, this involves processing the facial image to record personal characteristics. This can be based on attributes such as gender, race, ethnicity, sexual orientation, and age. Furthermore, FRT can be used to attempt to classify facial expressions to establish a person's emotional state, such as happy or sad, and even attempt to identify more complex feelings, like whether a student is bored in class.

FRT can be referred to as live FRT or retrospective FRT. Live FRT refers to capturing individuals' facial images and processing them in real-time. Whereas retrospective FRT involves the capturing of individuals' facial images and processing them at a later stage. For instance, it could entail reviewing past recordings to identify who was present in a gathering.

02 Facial recognition in EdTech

Privacy International (PI) defines EdTech as technology or software that can be used in educational settings that involves the electronic processing of users' data, in particular student's data.³ This includes software used for behaviour management, for education administration purposes, and software used to assist with teaching lessons and providing educational materials.⁴ Several of these categories include the use of FRT. In this context, FRT software fundamentally relies on acquiring, extracting, storing, and occasionally sharing individuals' biometric facial data, serving various purposes broadly categorised into two primary domains: administrative and security objectives.

The first category encompasses all applications already aimed at enhancing productivity and efficiency by minimising the time required for administrative tasks and, allegedly, reducing the likelihood of errors. For instance, Brazil has adopted FRT to manage student attendance records⁵ and facilitate the distribution of meals and school supplies.⁶ In India, The Central Board of Secondary Education (CBSE) has used FRT to provide students with access to their academic documents.⁷ Similarly, China has implemented a "One Face Pass" system to authenticate students' payments

3 Privacy International, 'EdTech Needs Schooling', <https://privacyinternational.org/campaigns/edtech-needs-schooling>

4 *ibid.*

5 Rest of World, 'Brazil's embrace of facial recognition worries Black communities', <https://restofworld.org/2021/brazil-facial-recognition-surveillance-black-communities/>

6 Tavares, C.; Simão, B., Martins, F.; Santos, B., Araújo, A, 'Surveillance Technologies and Education: Mapping Facial Recognition Policies in Brazilian Public Schools', InternetLab, 2023, <https://internetlab.org.br/wp-content/uploads/2023/06/Educacao-na-mira-EN-03.pdf>

7 Privacy International, 'EdTech in India: Worst Practices', 15 November 2022, <https://privacyinternational.org/long-read/4983/edtech-india-worst-practices>

and facilitate the provision of their parents' banking information.⁸ These technologies have even directly entered the classroom, with proctoring software's mediating student's access to exams,⁹ and emotion recognition used to attempt to assess student's engagement with lessons.¹⁰

In the second category, security, the utilisation of FRT software is motivated by the desire to enhance security within educational spaces. For example, in Canada, this technology has been employed to monitor school premises and prevent unauthorised adults from accessing the school grounds.¹¹ In China, an "intelligent monitoring inspectors' system" function has been deployed by recognising students' facial features, but even going beyond, collecting data on their height, weight, body temperature, and other physical attributes.¹² This comprehensive data collection serves not only to safeguard health conditions but also to monitor and control students' bodies.

The introduction of such intrusive technologies, such as the collection of biometric data, has often been without the necessary human rights impact assessments and appropriate safeguards to ensure that their use is compatible with human rights.¹³ As mentioned earlier, FRT in educational spaces raises additional concerns beyond those associated with EdTech, as we will explore in the following sections.¹⁴

8 Alipay, 'Campus One Face Pass product introduction', 24 May 2021, <https://opendocs.alipay.com/pre-open/010nof>

9 Meaker, M, 'This Student Is Taking On 'Biased' Exam Software, Wired, DATE, <https://www.wired.co.uk/article/student-exam-software-bias-proctorio>

10 Tobin, M, Matsakis, L, 'China is home to a growing market for dubious "emotion recognition" technology', Rest of World, 25 January 2021, <https://restofworld.org/2021/chinas-emotion-recognition-tech/>

11 CNET, 'RealNetworks gives away facial recognition software to make schools safer', 17 July 2018, <https://www.cnet.com/news/privacy/realnetworks-gives-away-facial-recognition-software-to-make-schools-safer/>

12 KANKAN AI, 'Facial Recognition Pick-Up/Drop-off System', <https://www.kankanai.com.cn/en/solution/application/kindergarten/>

13 Privacy International, 'EdTech Needs Schooling', <https://privacyinternational.org/campaigns/edtech-needs-schooling>

14 Examples of this can be found at PI's EdTech surveillance Tracker, <https://privacyinternational.org/examples/edtech-surveillance-tracker>

03 Key concerns with FRT in educational spaces

While those adopting FRT systems in schools promise some benefits, as stated before, it has also raised many complex and multifaceted issues that demand careful consideration from a human rights perspective. The following sections delve into the critical issues and concerns surrounding using FRT in educational spaces, exploring its implications for privacy, surveillance, securitisation, discrimination, ethics, and the threats to the environment in which children are allowed to develop.

3.1 Erosion of privacy

The importance of the right to privacy, in educational settings and the protection of children is explicitly recognised by international law and standards. The right to privacy for children is established in Article 16 of the Convention on the Rights of the Child (UNCRC).¹⁵ Also, the Convention highlights that the best interests of the child should be a primary consideration.¹⁶ Furthermore, the resolution adopted by the UN General Assembly, titled 'Protecting Children from Bullying,' explicitly recognises that "children exercising their right to education, including through digital technologies, should not have their safety compromised and should be protected from any violation or abuse of their right to privacy".¹⁷ Also, in 2021, the UN Special Rapporteur on the Right to Privacy released a thematic report focusing on artificial intelligence, privacy, and children's

15 Article 16, 'Convention on the Rights of the Child': 1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation; 2. The child has the right to the protection of the law against such interference or attacks. , <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>

16 Article 3, 'Convention on the Rights of the Child', <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>

17 UN General Assembly, 'Protecting Children from Bullying', UN A/RES/75/166, 16 December 2020, p. 3 <https://documents.un.org/doc/undoc/gen/n20/373/31/pdf/n2037331.pdf?token=9pwKxk6JCB477c4qr5&fe=true>

privacy. This report shed light on issues and provided recommendations concerning the use of EdTech, including FRT, and their implications for children's privacy.¹⁸

The Rapporteur observed that in certain regions, there is inadequate protection for children's privacy rights in schools, leading to non-state actors routinely controlling children's digital educational records. Furthermore, schools themselves amass significant amounts of children's information. Additionally, children and parents often cannot contest privacy arrangements with educational technology companies or refuse to provide data, as education is compulsory. Consequently, the only means of preserving privacy involves rejecting such uses, potentially leading to restricted access to essential services or educational opportunities.¹⁹

The Rapporteur emphasised the need for technological offerings to be evaluated considering children's rights and their best interests, with a focus on minimising corporate access to and utilisation of children's data, including the ability to erase data. It was stressed that educational processes should not compromise the enjoyment of other human rights, including privacy.²⁰

For the operation of any FRT system, such as those described above, administrators must gather sensitive data (for more information refer to section 'Lack of data protection safeguards'). This often entails establishing a centralised database primarily dedicated to storing comprehensive facial information, mostly of children. The collection of facial images results in the creation of 'digital signatures' of identified faces.²¹

18 UN Human Rights Council, 'Report of the Special Rapporteur on the right to privacy on Artificial intelligence and privacy, and children's privacy,' UN Doc A/HRC/46/37, 25 January 2021, <https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F46%2F37&Language=E&DeviceType=Desktop&LangRequested=False>

19 *ibid.*

20 *ibid.*

21 Privacy International, 'Facial Recognition', <https://privacyinternational.org/learn/facial-recognition>

These digital signatures, and the information created as part of the processing in the FRT systems –which can include various aspects of student’s lives, from their attendance records, their payment history, religion, health conditions, interest in lessons and so on– are usually stored and can change over time. These records raise significant privacy and security concerns (see further in ‘Surveillance and securitisation’).

FRT technologies in schools have been mostly introduced without a rigorous human rights’ due diligence process. As a result, the lack of impact assessments already during the early stages of designing and developing these technologies means that their impact on and risks to students and teachers’ right to privacy are not identified and, in the cases where they are identified, they aren’t adequately addressed. Moreover, deploying such intrusive technology in educational settings, where students are exercising their right to education, must be legal, necessary to achieve a defined goal, and proportionate (any adverse impact on their rights and freedoms must be justified).

Consequently, FRT can only ever be legitimate if it is “lawful”, in the sense of falling under an appropriate legal framework that authorises such technology to be used for the purposes intended (See ‘Lack of data protection safeguards’). In addition, international human rights law requires that any interference with the right to privacy must be necessary and proportionate. Any technology that has an impact on its citizens’ privacy must therefore demonstrate in “specific and individualized fashion the precise nature of the threat”²² that it seeks to address. Moreover, the principle of proportionality requires that the interference with privacy be both “in proportion to the aim and the least intrusive option available”.²³

22 Privacy International, ‘Legality, Necessity and Proportionality’, <https://privacyinternational.org/our-demands/legality-necessity-and-proportionality>

23 *ibid.*

However, the use of FRT in schools cannot adequately justify the adverse impacts on students' rights and freedoms. Less intrusive alternatives exist to achieve the intended purposes, such as enhanced in-person methods for improving security and efficiency within the classroom and school premises (for more information about the purposes and alternative approaches, refer to the sections titled 'Facial Recognition in EdTech' and 'What We Want').

3.2 Lack of data protection safeguards

We observed that often schools have introduced FRT without abiding to an adequate data protection framework or establishing necessary safeguards. This is significant because FRT in schools involves the processing of students' (often children's) and teacher's personal data, and in particular sensitive data, such as biometric data that require enhanced protections (see further in 'What are facial recognition technologies?' and Art. 4 GDPR Definitions Art. 9 GDPR Processing of special categories of personal data²⁴).

For example, as we mentioned before, these educational spaces often lack legal basis to process this data. Typically, schools rely on parental consent as the legal foundation for implementing and using this technology.²⁵ However, in the case of implementing FRT within schools we believe that parental consent is obsolete. The power imbalance between educational authorities and students, as well as their parents, creates a situation where refusal could negatively impact the student's access to education, making consent less than fully voluntary.²⁶

24 General Data Protection Regulation GDPR, 'Art. 4 GDPR Definitions Art. 9 GDPR Processing of special categories of personal data', <https://gdpr-info.eu/>

25 See some examples: TechMonitor, 'Council breached GDPR in deploying facial recognition technology in schools – ICO', <https://www.techmonitor.ai/policy/privacy-and-data-protection/facial-recognition-technology-school-ico?cf-view>

26 If you want to learn more about consent read Privacy International's guide: Privacy International, 'A Guide for Policy Engagement on Data Protection, Part 5: Grounds for Processing Personal Data', <https://privacyinternational.org/report/2243/part-5-grounds-processing-personal-data>

Additionally, these educational spaces often lack data protection impact assessments, which should always be conducted before processing personal data. These assessments are crucial as they help identify risks and establish practices to mitigate them, especially when processing of biometric data (which is sensitive data).²⁷ At a minimum, these assessments should evaluate the necessity and proportionality of the data processing, assess potential risks to individuals, and detail the measures that will be implemented to mitigate these risks.²⁸

There are also further risks created regarding the storage and retention of this sensitive data collected by FRT and subsequent risks of unauthorised access to the data. These risks include the data collected being shared and used for other purposes than originally intended. For example, by schools sharing the data with other public bodies or even law enforcement without appropriate procedures in place.

Furthermore, these systems are rarely developed or run solely by the school. Instead, acquiring, processing, and sharing this data often involves third parties. Collecting and storing this data can be in and of itself an invasion of privacy, a violation which is exacerbated when that data is shared with these third parties, who may exploit this data for commercial gain or worse, they may even sell on or further share data for their own advantage.

This highly sensitive data has the potential to impact individuals' lives in the long term significantly. It implies that a child's private life, which should be safeguarded while in school, may be compromised by not only school administrators but also external entities. Even without being sold on, where data is collected, it can be compromised – particularly if schools are not adequately evaluating the technical capabilities of the software they are

27 If you want to learn more about consent read Privacy International's guide: Privacy International, 'A Guide for Policy Engagement on Data Protection, Part 5: Grounds for Processing Personal Data', <https://privacyinternational.org/report/2243/part-5-grounds-processing-personal-data>

28 Privacy International, 'A Guide for Policy Engagement on Data Protection, The Keys to Data Protection', <https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf>

purchasing. This is particularly damaging when data is as sensitive and personal as biometric data (see further on 'Children development', which is also part of privacy standards).

3.3 Surveillance and securitisation

Given its reliance on capturing, extracting, storing, and sharing individuals' biometric facial data, FRT has evolved into an exceptionally intrusive form of surveillance. Typically, it finds use in law enforcement for supposedly crime but has crept into public spaces such as protests.²⁹ When deployed in schools and other educational spaces; its intrusiveness can be the same as in any other public setting or even worse. This heightened intrusion is mainly due to its inescapable presence, enabling the creation of comprehensive records detailing students' movements, interactions, and daily schedules. The implications are far-reaching, exposing intimate aspects of a student's life, including their sexual orientation, health status, or religious preferences.

In essence, it transforms educational institutions into spaces where students are under constant surveillance, much like individuals in "high security" settings, such as prisons. Their every move is meticulously recorded and categorised, producing a chilling effect on their natural reactions and behaviour.³⁰ When children are subjected to such surveillance, they are treated no differently than adults, raising concerns about the potential for alarming abuses.³¹ The Special Rapporteur on the right to education, in their thematic report on academic freedom, noted that while the stated intention of FRT technologies "is to prevent abuses in classrooms, ensure security or assess the performance of students and staff. However,

29 Privacy International, 'How facial recognition technology can be used at a protest', 5 May 2021, <https://privacyinternational.org/explainer/4495/how-facial-recognition-technology-can-be-used-protest>. See further on: United Nations High Commissioner for Human Rights, 'Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests', A/HRC/44/24, 25 June 2020.

30 Privacy International, Mass surveillance, <https://privacyinternational.org/learn/mass-surveillance>

31 UNICEF, 'State surveillance and implications for children', August 2020, <https://www.unicef.org/globalinsight/media/1101/file/UNICEF-Global-Insight-data-governance-surveillance-issue-brief-2020.pdf>

education must be built on trust and educational institutions must remain safe spaces for free expression."³²

An example of how these technologies can be harmful is the 2014 Umbrella Movement in Hong Kong. During the protests, high school students such as Joshua Wong and Ivan Lam Long-in, who founded 'Scholarism' at the age of 15, were targeted by security officials. Facial recognition cameras and cyber monitoring were used to track their activities, resulting in detentions and severe punishments for their political activism.³³

In April 2022, the UN Special Rapporteur on the Right to Education issued a thematic report on the "Impact of the Digitalization of Education on the Right to Education." This Report delves into the long-term effects and costs of integrating digital technologies into education, focusing on concerns regarding state and governmental surveillance facilitated by these technologies.³⁴ The Special Rapporteur identifies several adverse impacts of digital technology, including an increased presence of commercial entities in education and heightened data collection and surveillance. These negative consequences are glaringly evident in the utilization of FRT within educational settings.³⁵

3.4 Children's development

As discussed in the preceding section, the extensive surveillance faced by children can result in a chilling effect, inhibiting their natural behaviour. However, beyond the immediate impact on their behaviour, such

32 Human Rights Council, 'Academic freedom: Report of the Special Rapporteur on the right to education, Farida Shaheed, A/HRC/56/58, 27 June 2024.

33 Dvorak, Phred and Khan, Natasha, 'Hong Kong Protesters Adjust Tactics with Lessons from 2014 Umbrella Movement', Wall Street Journal, 13 June 2019, <https://www.wsj.com/articles/hong-kong-protesters-adjust-tactics-with-lessons-from-2014-umbrella-movement-11560448247>

34 Human Rights Council, 'Impact of the digitalization of education on the right to education: Report of the Special Rapporteur on the right to education, Koumbou Boly Barry', A/HRC/50/32, 19 April 2022.

35 *ibid.*

surveillance threatens children's autonomy and dignity. At the same time, surveillance in broader societal contexts can have repercussions on how society evolves and experiments;³⁶ its effects on children are even more perilous. This heightened risk arises because children require the freedom to experiment and make mistakes as they develop into responsible citizens.³⁷

The UNCRC recognises the children's right to develop.³⁸ Article 6 of UNCRC also provides that children and young people should be able to grow up in conditions that don't impact negatively on their physical and mental wellbeing.³⁹ At the same time, the right of privacy is founded on the presumption that individuals have an area of autonomous development, interaction and liberty, a 'private sphere' free from intervention by any uninvited individuals, private actors, or the state.⁴⁰ Nowhere these rights do not become more pertinent but in educational spaces, where children must be able to enjoy a private sphere to fully develop.

In essence, this form of surveillance can impede children's natural growth and learning processes, which is at odds with Article 29 of the United Nations Convention on the Rights of the Child.⁴¹ Article 29 stipulates that states must ensure that the education of the child is directed towards the development of the child's personality, talents, and mental and physical abilities to their fullest potential. Surveillance practices that hinder their ability to explore, take risks, and learn from their experiences are a violation

36 UNICEF, 'State surveillance and implications for children', August 2020, <https://www.unicef.org/globalinsight/media/1101/file/UNICEF-Global-Insight-data-governance-surveillance-issue-brief-2020.pdf>

37 UNICEF, 'Early childhood development for every child, early moments matter', <https://www.unicef.org/early-childhood-development>

38 Article 6, 'Convention on the Rights of the Child', <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>

39 Children and Young People's Commissioner Scotland, 'UNCRC Simplified Articles', Article 6, <https://www.cypcs.org.uk/rights/uncrc/articles/article-6/>

40 Human Rights Council, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue', UN doc A/HRC/23/40, 17 April 2013, para 22, https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

41 Article 29, 'Convention on the Rights of the Child', <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>

of these fundamental rights.⁴²

Furthermore, it's important to note that children – or their parents – who choose not to be surveilled, and therefore cannot access the materials or information behind these facial recognition systems, may find themselves at a significant educational disadvantage. This not only affects their privacy but also their educational opportunities and prospects. The UN General Assembly Resolution on the Rights of the Child clearly urges states to prohibit unlawful digital surveillance of children, particularly in commercial, educational, and care settings.⁴³ Therefore, there's a pressing need to carefully consider the implications of such surveillance on the fundamental rights, educational opportunities, and overall well-being of children.

3.5 Discrimination: effectiveness and categorisation

FRT and its use in educational settings presents various technical and ethical challenges. It can exhibit notably high rates of false positives and false negatives,⁴⁴ which can potentially perpetuate bias and various forms of discrimination, particularly affecting specific populations such as individuals with dark skin or non-gender-conforming students. This poses a direct concern considering Article 24 of the UN International Covenant on Civil and Political Rights (ICCPR),⁴⁵ which acknowledges the rights of every child, without discrimination, to receive the protection they require as minors.

Moreover, Article 13 of the UN International Covenant on Economic, Social,

42 *ibid.*

43 UN General Assembly, 'Resolution on the Rights of the Children', UN Doc A/RES/78/187, 19 December 2023, <https://documents.un.org/doc/undoc/gen/n23/424/18/pdf/n2342418.pdf>

44 European Parliamentary Research Service, 'Regulating facial recognition in the EU,' September 2021, [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA\(2021\)698021_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf)

45 Article 24 UN ICCPR, 1996, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.

and Cultural Rights (ICESCR)⁴⁶ guarantees the right to education for everyone and emphasises the need for equitable access. In addition, the Committee on the Rights of the Child has emphasised that standards for digital educational technologies must ensure that their use is ethical, appropriate for educational purposes, and does not expose children to violence or discrimination.⁴⁷ If FRT is integrated into an educational context, the risks of discrimination must be carefully considered. For instance, the use of FRT could lead to the exclusion or isolation of certain students, denying them access to school premises or incorrectly identifying them for routine administrative matters such as attendance records or more serious disciplinary issues.

Nevertheless, even in scenarios where the technology is exceptionally well-trained and devoid of technical flaws – which remains highly improbable⁴⁸ there is a critical need to address its inherent capacity to categorise students into distinct datasets, often influenced by factors such as their physical appearance and identity (for more information on categorisation see 'What are facial recognition technologies?'). This categorisation process holds immense potential to exert a far-reaching impact on the broader societal landscape due to its inherent discriminatory nature, sometimes necessitating human intervention. For instance, human decisions can be involved in selecting the data for facial recognition matches or assigning labels for various purposes.⁴⁹ However, this human intervention may not be adequate to prevent discrimination. This not only raises concerns about the right to education but also the broader issue of fairness and equality in educational settings.

46 Article 13 UN ICESCR, 1996, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights>

47 Committee on the Rights of the Child, General Comment No 25 (2021) on Children's Rights in Relation to the Digital Environment, UN Doc CRC/C/GC/25, 2 March 2021, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC%2FC%2FGC%2F25&Lang=en

48 Cyphers, B, Schwartz, A, Sheard, N, 'Face Recognition Isn't Just Face Identification and Verification: It's Also Photo Clustering, Race Analysis, Real-time Tracking, and More', Electronic Frontier Foundation, October 7, <https://www.eff.org/deeplinks/2021/10/face-recognition-isnt-just-face-identification-and-verification>

49 See an example of this human-in-the-loop process: <https://humansintheloop.org/>

3.6 Role of private sector

Education technologies are implemented across various institutions, emphasising that the analysis of these practices should extend beyond those funded by public or state resources. Even in cases where private institutions offer educational access, it remains imperative to establish and uphold human rights safeguards and adhere to specific standards. The UN Special Rapporteur on the Right to Education has recommended that states and stakeholders proactively address the risks associated with increasing privatization and digitalisation of education, emphasising full compliance with the Abidjan Principles and Guiding Principles on Business and Human Rights.⁵⁰

Principle 54 of the Abidjan Principles pertains to the minimum standards applicable to private educational institutions concerning privacy and data protection.⁵¹ It underscores the importance of upholding the rule of law and ethical practices when handling personal data. States are obliged to ensure that no personal data, including biometric data, is collected or retained without explicit consent or shared with third parties for purposes unrelated to education, including commercial, immigration, or security purposes.

Furthermore, Principle 72⁵² reinforces that the integration of technology in the classroom and management systems must respect the right to privacy of both learners and educators, as well as the right of all individuals to benefit from the protection of their moral and material interests stemming from any scientific, literary, or artistic creations they author.

50 UN Human Rights Council, Report of the Special Rapporteur on the right to education on impact of the digitalization of education on the right to education, UN Doc A/HRC/50/32, 19 April 2022, para 99(a), <https://www.ohchr.org/en/documents/thematic-reports/ahrc5032-impact-digitalization-education-right-education>

51 Abidjan Principles, 2019, para 54, <https://www.abidjanprinciples.org/en/principles/overview>.

52 Abidjan Principles, 2019, para 72, <https://www.abidjanprinciples.org/en/principles/overview>.

In addition, the UN Guiding Principles on Business and Human Rights⁵³ underscore that states bear the responsibility of safeguarding against human rights violations by all societal actors, including businesses. This encompasses preventing, investigating, penalising, and rectifying human rights abuses within domestic business operations.

Consequently, it is crucial to recognise that every international rule or safeguard applicable to public educational institutions should also be extended to the private sector, particularly when protecting children's rights. In such instances, states should establish transparent and predictable legal frameworks for private entities to follow and ensure the availability of effective remedial measures. Companies providing FRT to schools should be compelled to waive commercial confidentiality and subject their technologies to comprehensive auditing processes.

53 UN Guiding Principles on Business and Human Rights, 2011, https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

04 What we want: Ban FRT in educational spaces

The introduction of facial recognition technology (FRT) into educational spaces raises significant human rights concerns. **This is why we think that FRT should not be used in educational spaces as it is incompatible with human rights standards.** Anyone considering the implementation of FRT in educational settings must address numerous critical questions before proceeding. PI has conducted an in-depth analysis, addressing some of these questions, and concluded that FRT in educational spaces should be banned and its use halted, as it constitutes an unlawful interference with the right to privacy and other human rights. A thorough and objective review of this analysis would likely lead others to the same conclusion. In their recommendations, the Special Rapporteur on Education advises that states and relevant stakeholders should “refrain from surveillance, whether physical or online, of educational institutions, staff, and students, and **ban facial recognition technologies from such institutions.**”⁵⁴

⁵⁴ Human Rights Council, 'Academic freedom: Report of the Special Rapporteur on the right to education, Farida Shaheed, A/HRC/56/58, 27 June 2024.

05 A roadmap to assessing compatibility of the use FRT in educational spaces with human rights standards.

In the following, we will delve into some of the questions identified by PI as critical; but it's important to note that the list is not exhaustive. Each case should be analysed individually, considering the potential impact on the various human rights at risk.

1. Human rights due diligence, including human rights and data protection impact assessments: In every instance, where FRT is considered in educational settings, it is imperative to conduct thorough human rights due diligence, including assessing the potential adverse human rights impacts of introducing this technology. The question we need to ask ourselves is: what are the potential impacts of introducing this technology on human rights? This assessment should encompass all individuals within the educational space, focusing especially on children. Adverse impacts may manifest directly, indirectly, or as a combination. It is essential to gather substantiated evidence to underpin this assessment, actively involving the community to address their concerns and incorporate their experiences. At a minimum, the impact on privacy and data protection (see 'Data protection safeguards'), access to education, and discrimination should be addressed. After conducting this assessment, we may conclude that the use of FRT in educational settings is incompatible with human rights standards.

2. Purpose and necessity: The deployment of these technologies typically revolves around the two purposes we outlined earlier: efficiency and security. However, it is essential to consistently inquire when introducing these privacy intrusive technologies: is there a less intrusive alternative

that can serve the same purpose? For instance, in scenarios involving meal provision or attendance tracking, it might be less intrusive and more effective to consider employing individuals for these tasks. Similarly, when it comes to security, often, enhanced in-person methods such as better training for personnel can be more effective. We must avoid assuming that technology is the panacea for all challenges. Furthermore, it's worth emphasising that these technologies are not always reliable, as we previously discussed. Hence, it becomes rare for their use to outweigh the associated risks.

3. Proportionality: When assessing proportionality, we must ask ourselves: is this in proportion to the aim, and is it the least intrusive option available? FRT implementation in educational spaces does not single out a specific individual or suspect; it affects all students simultaneously, including staff and parents. Consequently, within certain parameters, anyone within the school and its vicinity may experience infringements on their human rights, including privacy, non-discrimination, and access to education. Additionally, this technology often isn't solely aimed at identifying specific behaviours; it also involves continuously tracking students' movements and storing this data. It is doubtful that such systematic and indiscriminate surveillance could meet the requirements of the principle of proportionality under human rights law. As previously highlighted, establishing a valid and proportionate purpose for such broad surveillance measures is challenging. Even if one were to identify a goal, the potential risks associated with its implementation often outweigh the perceived benefits.

4. Data protection safeguards: When dealing with sensitive data, such as that collected by FRT, a primary inquiry should be: do we have a legal basis for this? FRT frequently lacks a legal basis for implementation, and data protection impact assessments are typically not conducted. Additionally, these educational spaces often fail to ensure secure storage or processing of sensitive data, and they may share information with third parties. At a minimum, educational spaces should adhere to specific data

protection frameworks, beginning with establishing a legal basis for data collection, conducting necessary impact assessments, and implementing robust data security measures. However, once these assessments are conducted, it may become evident that the risks of processing this data outweigh the benefits.

5. Transparency: The use of FRT often operates in an opaque and discretionary manner. One important question to consider is: do we have enough information to evaluate its use effectively? In this context, there is a conspicuous absence of mechanisms to guarantee transparency or accountability among those employing this technology. Furthermore, it remains virtually impossible to ascertain whether these technologies are being used as intended. If they were to employ FRT, authorities must uphold a high standard of transparency regarding its scope, functioning, any commercial arrangements they have with external enterprises, error rates, impact assessments, and potential oversight mechanisms, among others. By analysing the levels of transparency, we often conclude that there is insufficient information available to seek proper accountability and monitoring.

6. Public-private partnerships: The United Nations Guiding Principles on Business and Human Rights⁵⁵ mandate both states and companies to enhance their efforts in respecting, protecting, and fulfilling human rights, extending their responsibilities accordingly.⁵⁶ In the context of public-private partnerships involving technologies like FRT, it is imperative to establish a robust framework of protections to enforce these obligations and responsibilities and ensure comprehensive human rights protection while private entities are actively involved in accordance with. A crucial question to consider is: are these protections being effectively implemented

55 UN Guiding Principles on Business and Human Rights, 2011, https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

56 Privacy International, 'Safeguards for public-private surveillance partnerships', December 2021, <https://privacyinternational.org/sites/default/files/2021-12/PI%20PPP%20Safeguards%20%5BFINAL%20DRAFT%2007.12.21%5D.pdf>

in practice? In addition, to address these issues, public authorities and companies entering such partnerships should implement safeguards based on principles such as transparency, adequate procurement, accountability, legality, necessity and proportionality, oversight, and redress. These safeguards are designed to uphold human rights.⁵⁷ However, as we saw in previous sections, these partnerships would struggle to abide by those principles, as FRT constitutes an unlawful interference with the right to privacy and other human rights.

57 *ibid.*

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).