Privacy International's response to the call for contributions: safety as an element of the right to education and a precondition for its full realisation

Privacy International (PI) welcomes the opportunity to provide input to call for contributions: safety as an element of the right to education and a precondition for its full realisation, for the forthcoming report scheduled for presentation to the Human Rights Council in June 2025.[1]

PI is a London-based non-profit, non-governmental organisation (Charity Number: 1147471)[2] that 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.

The following sections provide PI's insights and analysis on the topics highlighted in the call for contributions, focusing specifically on issues of surveillance and securitisation in educational environments, as addressed in questions 1, 2, and 6.

---

[1] Special Rapporteur on the right to education, 'Call for contributions: safety as an element of the right to education and a precondition for its full realization', https://www.ohchr.org/en/calls-for-input/2024/call-contributions-safety-element-right-education-and-precondition-its-full
[2] Privacy International, https://privacyinternational.org/

1. Surveillance in schools and educational environments

The use of Education Technologies (EdTech)[3] in educational environments has rapidly expanded, [4] raising significant human rights concerns. Also, the shift to online education has exacerbated power imbalances between EdTech companies and students, as well as between state authorities, children and young people, and parents. [5]

PI has observed with concern that this expansion of EdTech includes a broad array of tools that enable the surveillance of students and academic staff. Many EdTech tools implemented in schools and educational environments facilitate surveillance by both public authorities and private entities.

Our research has shown that such surveillance undermines trust, as it makes it more difficult for students to seek help when needed due to the fear that they will be judged based on their digital footprint rather than their own experiences and perceptions.[6] These practices hinder the creation of a secure learning environment, free from threats of violence and discrimination, and endanger student's opportunity to learn in a safe and supportive space, ultimately undermining the fulfilment of the right to education under international human rights law.[7]

a) The security rationale behind the adoption of surveillance technologies in educational environments

---

[3] In the absence of internationally agreed definition, 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. This includes software used for behaviour management, for education administration purposes, and software used to assist with teaching lessons and providing educational materials. Privacy International, 'EdTech Needs Schooling', https://privacyinternational.org/campaigns/edtech-needs-schooling

[4] 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

[5] Ibid.

[6] Steeves, V; Regan, P; Regan Shade, L, 'Digital Surveillance in the Networked Classroom' http://www.equalityproject.ca/wp-content/uploads/2017/05/7-Digital-Surveillance-in-the-Networked-Classroom.pdf

[7] As outlined in Article 26 of the Universal Declaration of Human Rights (UDHR), Article 19 of the Convention on the Rights of the Child (CRC), and Article 13 of the International Covenant on Economic, Social and Cultural Rights (ICESCR), quality education extends beyond mere access to encompass the environment in which it is delivered.

Among other reasons, the adoption of surveillance technologies in educational environments is often justified by the aim of enhancing safety and security. For example, in Canada, Facial Recognition Technology (FRT) has been employed to monitor school premises and prevent unauthorised adults from accessing the school grounds.[8] Similarly, in China, an 'intelligent monitoring inspectors' system' has been deployed to recognise students' facial features and collect data on their height, weight, body temperature, and other physical attributes. This system claims to be able to eliminate incidents such as wrong pick-ups, false alarms, kidnappings, and other safety concerns, including monitoring the child's daily health. [9] Additionally, one company offering "high quality surveillance systems and CCTV for schools including sophisticated infra-red cameras which record in the darkest areas"[10] claimed that these both deter "bad or antisocial behaviour from pupils, parents and visitors" and improve the concentration, productivity and attainment of the students.[11]

As previously mentioned, the widespread adoption of these technologies undermines the creation of an environment conducive to fulfilling the right to education. By compromising the privacy and well-being of students, these technologies ultimately detract from the goal of providing a safe and supportive learning environment.

For more on its implications for privacy, see: D. The balance between security measures and the rights of students to privacy and a non-intimidating learning environment).

b) The role of facial recognition technologies in surveillance

FRT is one of the most intrusive technologies in this field as it captures, extracts, stores, and shares individuals' biometric facial data.[12] Given its reliance on sensitive data, FRT

---

[8] CNET, 'RealNetworks gives away facial recognition software to make schools safer', https://www.cnet.com/news/privacy/realnetworks-gives-away-facial-recognition-software-to-make-schools-safer/
[9] KANKAN AI, 'Facial Recognition Pick-Up/Drop-off System', https://www.kankanai.com.cn/en/solution/application/kindergarten/
[10] School Watch: electronic security systems, 'CCTV for schools", https://schoolwatch.co.uk/school-cctv/
[11] School Care, 'CCTV for Schools and Surveillance Systems', https://web.archive.org/web/20230810115554/https://www.schoolcare.co.uk/cctv-for-schools/
[12] 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.

has evolved into an exceptionally intrusive form of surveillance. Typically, it finds use in law enforcement for supposedly crime but has creeped into public spaces such as protests.[13] 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. This will negatively impact efforts to ensure an adequate environment for fulfilling the right to education under international human rights law, as quality education encompasses not only access but also the environment in which it is delivered.[14]

For more information on the impacts of facial recognition, see: Why you should be worried about facial recognition in educational spaces: PI's briefing.[15]

c) The role of emotional recognition systems in surveillance

In addition to FRT, AI systems that process data to recognise attention, mood, and emotions also raise significant concerns. Under the EU AI Act,[16] an 'emotion recognition system' is defined as an AI system designed to "identify or infer emotions or intentions of natural persons based on their biometric data."[17] The use of these systems has been banned in EU classrooms, except in cases where they are strictly required for medical or safety reasons. This decision reflects the EU's recognition that such systems are highly invasive and carry the risk of discriminatory outcomes.

EdTech systems are already in use, claiming to track eye movements to detect student's not paying attention.[18] Others claim to be able to "identify emotions and classify learner involvement and interest in the topic [being taught]" by detection of

---

[13] Privacy International, 'Mass surveillance', https://privacyinternational.org/learn/mass-surveillance

[14] Art. 26 of the Universal Declaration on Human Rights (UDHR), Art. 19 of the Convention of the Rights of the child (CRC) and Art. 13 of the International Covenant on Economic, Social and Cultural Rights (ICESCR)

[15] Privacy International, 'Why you should be worried about facial recognition in educational spaces: PI's briefing', https://www.privacyinternational.org/sites/default/files/2024-11/Briefing%20with%20graphic.pdf

[16] EU, 'The EU Artificial Intelligence Act', https://artificialintelligenceact.eu/

[17] EU, 'The EU Artificial Intelligence Act', https://artificialintelligenceact.eu/recital/44/, recital 44.

[18] Faber, M; Krasich, K; E Bixler, R; et al., 'The eye-mind wandering link: Identifying gaze indices of mind wandering across tasks', https://pubmed.ncbi.nlm.nih.gov/32730072/

eyes and head movement,[19] with the results being "plotted as feedback to the instructor to improve learner experience." [20] And others market brain-scanning headbands [21] or sell neuro-technology for STEM promotion in the classroom, [22] or produce classroom sensors that claim to identify mood and emotions[23] using "pose estimation" from faces.[24] Other AI-based tools go even further, analysing a large range of factors (not all of them physical or visible) to identify and track the emotional health of their students.

However, these technologies have similar, if not more detrimental, impacts than FRT on the right to education. Their experimental nature, coupled with the highly intrusive collection and analysis of personal data, risks further undermining the ability of students to learn in a safe, supportive, and non-intimidating environment

For more information on the impacts of facial emotion recognition systems, see: Studying under Surveillance: the securitisation of learning.[25]

2. Balance between security measures and the rights of students to privacy and a non-intimidating learning environment

The importance of the right to privacy, in educational settings and the protection of children is explicitly recognised by international law and standards.[26] In 2021, the UN Special Rapporteur provided recommendations concerning the use of EdTech, including FRT, and their implications for children's privacy.[27] The Rapporteur observed

---

[19] L.B, K; Priya, L, 'Emotion Recognition System (SERS) for e-learning Improvement Based on Learner Concentration Metric', https://www.sciencedirect.com/science/article/pii/S1877050916306147
[20] Ibid.
[21] Quartz, 'A "brain-reading" headband for students is too much even for Chinese parents'
https://qz.com/1742279/a-mind-reading-headband-is-facing-backlash-in-china
[22] Neuromaker, 'NeuroRacing: Speed Through Focus', https://www.neuromakerstem.com/neuroracing
[23] ViewSonic, 'myViewBoard Sens overview', https://myviewboard.com/kb/en_US/category-1/sens-overview
[24] ViewSonic, 'ViewSonic myViewBoard Sens Helps Smestow Academy to Improve Student Engagement and Wellness with the Power of AI', https://www.viewsonic.com/global/presscenter/content/viewsonic-myviewboard-sens-helps-smestow-academy-to-improve-student-engagement-and-wellness-with-the-power-of-ai_5138
[25] Privacy International, 'Studying under Surveillance: the securitisation of learning',
https://privacyinternational.org/long-read/5463/studying-under-surveillance-securitisation-learning11/Briefing%20with%20graphic.pdf
[26] The right to privacy for children is established in Article 16 of the Convention on the Rights of the Child (UNCRC). Also, the Convention highlights that the best interests of the child should be a primary consideration. 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".
[27] 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/

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, education is compulsory, and students and parents may not be able to refuse consent for data-intensive technologies or withhold data without risking loss of access to opportunities or facing exclusion in the classroom. Moreover, if this is the case, they often cannot transfer to another school that shares their concerns.

Also, these technologies 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 academic staff' right to privacy are not identified and, in the cases where they are identified, they aren't adequately addressed. Moreover, deploying such intrusive technologies 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).[28]

In the case of FRT in schools, the adverse impacts on students' rights and freedoms cannot be adequately justified. 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 on the balance between security measures and the rights of students to privacy, see: Why you should be worried about facial recognition in educational spaces: PI's briefing, sections 3.1 "Erosion of privacy" and section 3.2 "Lack of data protection safeguards".[29]

3. The securitisation of educational environments

Mobile?FinalSymbol=A%2FHRC%2F46%2F37&Language=E&DeviceType=Desktop&LangRequested=False.
[28] Ibid.
[29] Privacy International, 'Why you should be worried about facial recognition in educational spaces: PI's briefing', https://www.privacyinternational.org/sites/default/files/2024-11/Briefing%20with%20graphic.pdf

The introduction of technologies such as FRT and emotional recognition systems transforms educational environments 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] Some studies have shown that this effect is directly related to various changes in behaviour, which can include greater restraint in political conversations, increased self-censorship, amplified awareness of surroundings, and eroded interpersonal trust.[31] As the Special Rapporteur on the right to education has recognised in their thematic report on academic freedom, while the stated intention of FRT is to prevent abuses in classrooms and ensure security, 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]

Additionally, another study looking at surveillance tools in American schools found that approximately 5 in 10 students in schools using activity monitoring technologies agreed with the statement: "I do not share my true thoughts or ideas because I know what I do online may be monitored" (a number which increased when speaking specifically to students with physical disabilities or leaning differences). Moreover, 8 in 10 agreed "I am more careful about what I search online because I know what I do online may be monitored."[34]

---

[30] Privacy International, 'Mass surveillance', https://privacyinternational.org/learn/mass-surveillance
[31] Murray, D; Fussey, P; Hove, Kuda, et al, 'The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe", Journal of Human Rights Practice, huad020, https://doi.org/10.1093/jhuman/huad020
[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] Center for Democracy and Technology, 'Hidden Harms: The Misleading Promise of Monitoring Students Online' pg 22, https://cdt.org/insights/report-hidden-harms-the-misleading-promise-of-monitoring-students-online/

The same study also found that surveillance technologies put students at risk of increased interactions with law enforcement; LGBTQ+ students being disproportionately targeted for action; students' mental health suffered; and students that rely more heavily on school issued devices, including in this case those from low-income families, Black students, and Hispanic students, were at a greater risk of harm.[35] These figures suggest a significant chilling effect of these tools, directly impacting the creation of safe, high-quality, and equitable learning environments.

The chilling effects of surveillance, combined with the potential repercussions students, teachers, and administrative personnel may face in their daily lives, profoundly shape their interactions within educational environments. This surveillance limits their comfort in asking questions, sharing information, accessing resources, and influences their behaviour and social interactions in these spaces.[36]

However, this has also specific and more profound impact on children. 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. Surveillance practices that hinder their ability to explore, take risks, and learn from their experiences are a violation of this fundamental right and their right to education.

4. Recommendations

PI suggests the UN Special Rapporteur to call on s**tates and other educational institutions and private actors where relevant to**:

1. **Conduct human rights due diligence, including human rights and data protection impact assessments**: This includes assessing the potential adverse human rights impacts on safety as an integral element of the right to education.

---

[35] Ibid.
[36] More examples can be found at: Privacy International, EdTech Surveillance Tracker, https://privacyinternational.org/examples/edtech-surveillance-tracker

2. **Conduct necessity and proportionality analysis**: In the deployment and implementation of EdTech in educational settings, relevant stakeholders must consistently assess whether the use of privacy-intrusive technologies is necessary and if less intrusive alternatives could achieve the same purpose. When assessing proportionality, stakeholders must evaluate whether the use of EdTech is proportionate to the intended goal and if it is the least intrusive option available.

3. **Introduce data protection safeguards in EdTech**: The development and implementation of EdTech must adhere to robust data protection frameworks. Authorities should establish a clear legal basis for data collection, and relevant stakeholders should conduct necessary data protection impact assessments, ensuring the implementation of strong data security measures to safeguard students' personal information.

4. **Ensure transparency in the development and implementation of EdTech**: This includes disclosing the scope and functioning of the technology, any commercial arrangements with private entities, error rates, impact assessments, and potential oversight mechanisms to ensure accountability.

5. **Implement safeguards in public-private partnerships**: Public authorities, private companies, and relevant stakeholders involved in EdTech partnerships should implement safeguards grounded in principles of transparency, accountability, legality, necessity, proportionality, and oversight. These safeguards should ensure that human rights are respected and that obligations under the United Nations Guiding Principles on Business and Human Rights are fully upheld.

6. **Ban facial recognition technology (FRT) and emotional recognition systems in educational settings:** Facial recognition technology (FRT) and emotional recognition systems should be prohibited in educational settings and their use stopped due to their disproportionate security risks, inaccuracies, and discriminatory biases. These technologies pose significant threats to the right to education and may undermine students' privacy and security.