February 2024

Privacy International's response to the call for contributions on academic freedom and freedom of expression in educational institutions

Privacy International (PI) welcomes the opportunity to provide input to the call for submissions of the UN Special Rapporteur on the right to education on for the forthcoming report scheduled for presentation to the Human Rights Council in June 2024.[1] We consider this upcoming report as an essential platform to examine the intricate interplay between academic freedom, freedom of expression, and surveillance conducted by both public and private entities through Education Technologies (EdTech).

Privacy International (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. Within its range of activities, PI investigates how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks. It has advised and reported to international organisations like the Council of Europe, the European Parliament, the Organisation for Economic Cooperation and Development, the UN Office of the High Commissioner for Human Rights and the UN Refugee Agency.

The subsequent sections offer Privacy International's insights and analysis on various topics outlined in the call for submission, specifically those related to the question of surveillance and the potential interference by private actors and its impact on academic freedom.

[1] Call for contributions: academic freedom and freedom of expression in educational institutions, UN Special Rapporteur on the right to education, https://www.ohchr.org/en/calls-for-input/2024/call-contributions-academic-freedom-and-freedom-expression-educational

[2] Privacy International, https://privacyinternational.org/

1. Surveillance in education: impact on academic staff and students

The use of technologies in educational settings 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. According to Online Education, downloads of education applications in 2020 increased by 90 percent compared to the weekly average in late 2019.[3] The implementation of many EdTech tools in educational institutes presents serious issues regarding surveillance by public authorities and some private parties. Furthermore, the shift to online education has amplified existing power imbalances between EdTech companies and children and between state authorities, children, and parents.[4]

In the absence of internationally agreed definition, 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.[5] This includes software used for behaviour management, for education administration purposes, and software used to assist with teaching lessons and providing educational materials.[6] PI has been observing with concern that the rapid expansion of technologies in educational settings has also included a wide array of tools that allow the surveillance of students and academic staff to the detriment of their privacy and academic freedom.

a. Motivations underlying the adoption of surveillance technologies in educational settings

EdTech solutions, including surveillance solutions, in educational settings has been regularly introduced to allegedly: (i) enhance productivity and efficiency, encompassing the delivery of educational content; and/or (ii) to strengthen the security and well-being of students, teachers, and personnel in educational premises. EdTech security solutions have among others been introduced to allegedly, enhance productivity and efficiency by minimizing the time required for administrative tasks and assumingly reduce the likelihood of errors. For instance, Brazil has adopted facial recognition technologies (FRT) to manage student attendance records and facilitate the distribution of meals and school supplies.[7] In India, The Central Board of Secondary Education (CBSE) has used FRT to provide

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

[4] *ibid*.

[5] Privacy International, EdTech Needs Schooling, https://privacyinternational.org/campaigns/edtech-needs-schooling

[6] *ibid*.

[7] Internet Lab, Surveillance Technologies and Education: Mapping Facial Recognition Policies in Brazilian Public Schools, https://internetlab.org.br/wp-content/uploads/2023/06/Educacao-na-mira-EN-03.pdf

students with access to their academic documents.[8] Similarly, China has implemented a "One Face Pass" system to authenticate students' payments and facilitate the provision of their parents' banking information.[9] These technologies have also directly entered the classroom, with among others proctoring software mediating student's access to exams,[10] emotion recognition used in China to assess students' engagement in classes[11], and CCTV cameras – some with facial recognition capability – installed in Indian classrooms[12].

Intertwined with these purposes, the utilization of surveillance technologies is motivated by the desire to enhance safety and security within educational environments. For example, in Canada, FRT has been employed to monitor school premises and prevent unauthorized adults from accessing the school grounds.[13] In China, an 'intelligent monitoring inspectors' system' has been deployed to recognize 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.[14]

b. Intrusive surveillance tools in educational settings: a focus on facial recognition technology and digital surveillance systems

As the examples in previous section indicate FRT is one of the most intrusive technologies in this field as it captures, extracts, stores, and shares individuals' biometric facial data.[15] Increasingly, it is used in law enforcement, particularly in public spaces such as protests.[16] However, when deployed in educational settings not only does it have an impact on privacy similar to other public spaces but it can further impact academic freedom. This heightened intrusion is mainly due to its inescapable presence, enabling the creation of comprehensive records detailing academic staff and students' movements, interactions, and daily schedules. It also extends to information about teachers. professors, and other

[8] Privacy International, EdTech in India: Worst Practices, https://privacyinternational.org/long-read/4983/edtech-india-worst-practices

[9] Alipay, Campus One Face Pass product introduction, https://opendocs.alipay.com/pre-open/010nof

[10] Wired, This Student Is Taking On 'Biased' Exam Software, https://www.wired.co.uk/article/student-exam-software-bias-proctorio

[11] Rest of World, China is home to a growing market for dubious "emotion recognition" technology https://restofworld.org/2021/chinas-emotion-recognition-tech/

[12] Privacy International, EdTech in India: Worst Practices, https://privacyinternational.org/long-read/4983/edtech-india-worst-practices

[13] 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/

[14] KANKAN AI, Facial Recognition Pick-Up/Drop-off System, https://www.kankanai.com.cn/en/solution/application/kindergarten/

[15] Privacy International, Facial Recognition, https://privacyinternational.org/learn/facial-recognition

[16] Privacy International, How facial recognition technology can be used at a protest, https://privacyinternational.org/explainer/4495/how-facial-recognition-technology-can-be-used-protest

personnel interacting within the environment. The implications are far-reaching, exposing intimate aspects of their lives, including potentially their sexual orientation, health status, or religious preferences.

In addition to FRT, schools are deploying extensive digital surveillance systems[17] that rely on monitoring social media,[18] tip reporting apps, or scanning the private digital content of millions of students using state-issued computers and accounts.[19] This not only impacts students, but potentially also extends to educational staff. Moreover, there is evidence that social media monitoring companies track the posts of everyone in the areas surrounding schools.[20] These tools have a direct impact on academic freedom and are employed to enforce restrictive social norms, aligning with increasingly stringent laws such as Florida's "Don't Say Gay" Bill, which prohibits discussions of sexual orientation and gender identity at schools across all grade levels.[21]

A notable example is the student monitoring tool, GoGuardian, which according to the company's website, oversees more than twenty-seven million students across more than ten thousand schools.[22] A report by the Electronic Frontier Foundation revealed that GoGuardian, by design, operates as a red flag machine for 'harmful' content but has a notable tendency to produce false positives. This results in tens of thousands of students being flagged for viewing content that is educational or informative. Such flagged content includes college application sites and college websites, counselling and therapy sites, sites with information about drug abuse, sites with information about LGBTQ+ issues, sexual health sites, sites with information about gun violence, sites about historical topics, sites about political parties and figures, medical and health sites, news sites, and general educational sites.[23]

c. Securitization of education: Evaluating the influence of EdTech implementation on academic freedom

[17] Education Week, Schools Are Deploying Massive Digital Surveillance Systems. The Results Are Alarming, https://www.edweek.org/technology/schools-are-deploying-massive-digital-surveillance-systems-the-results-are-alarming/2019/05

[18] For more on Social Media Intelligence: Privacy International, Social Media Intelligence, https://privacyinternational.org/explainer/55/social-media-intelligence

[19] FairPlay, Get Gaggle out of schools today, https://fairplayforkids.org/get-gaggle-out-of-schools-today/

[20] Education Week, Schools Are Deploying Massive Digital Surveillance Systems. The Results Are Alarming, https://www.edweek.org/technology/schools-are-deploying-massive-digital-surveillance-systems-the-results-are-alarming/2019/05

[21] Maya Yang, 'Florida board approves expansion of 'don't say gay' ban to all school grades', *The Guardian*, https://www.theguardian.com/us-news/2023/apr/19/florida-education-board-approves-expansion-dont-say-gay-bill

[22] GoGuardian, https://www.goguardian.com/

[23] Electronic Frontier Foundation, How GoGuardian Invades Student Privacy, https://www.eff.org/deeplinks/2023/10/how-goguardian-invades-student-privacy

The implementation of EdTech has often been without the necessary human rights impact assessments and appropriate safeguards to ensure that their use does not interfere with human rights.[24] Furthermore, procurement processes of such technologies have been conducted without the necessary due diligence and have led to corporate profiteering through data exploitation.[25]

In essence, intrusive EdTech transforms educational settings into environments where children and teachers are under constant surveillance, much like individuals in high security settings, such as prisons. Their every move is meticulously recorded and categorized, producing a chilling effect on their natural reactions and behaviour.[26] 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.[27]

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."[28] These figures suggest a significant chilling effect of these tools for academic freedom.

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 are at a greater risk of harm.[29]

[24] Privacy International, EdTech Needs Schooling, https://privacyinternational.org/campaigns/edtech-needs-schooling

[25] Further examples of this can be found at, Privacy International, EdTech Surveillance Tracker: https://privacyinternational.org/examples/edtech-surveillance-tracker

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

[27] Daragh Murray, Pete Fussey, Kuda Hove, Wairagala Wakabi, Paul Kimumwe, Otto Saki, and Amy Stevens, "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

[28] 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/

[29] Center for Democracy and Technology, 'Hidden Harms: The Misleading Promise of Monitoring Students Online', , https://cdt.org/insights/report-hidden-harms-the-misleading-promise-of-monitoring-students-online/

The chilling effects, along with the potential repercussions that students, teachers, and administrative personnel may face in their daily lives due to surveillance, will profoundly shape their interactions with freedom of expression and academic freedom. This will limit their comfort in asking questions, sharing, and accessing information, and determining their behaviour and social interactions within these environments.[30]

However, this has also specific and more profound impact on children. When subjected to surveillance, children are treated no differently than adults, raising concerns about the potential for alarming abuses.[31] For instance, during the 2014 Umbrella Movement, high school students in Hong Kong, China, played a pivotal role. Joshua Wong and Ivan Lam Long-in founded "Scholarism" when both were 15 years old. Security officials tracked them using facial recognition cameras and cyber monitoring, which led to detentions and severe punishments for their political activism.[32]

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.[33] 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 of this fundamental right.

d. States withdrawing FRT in educational settings

PI is particularly concerned by use of FRT and other surveillance in educational settings that does not only constitutes an unjustified interference with right to privacy but also academic freedom. Some states that had previously introduced FRT have now withdrawn these technologies. This includes

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

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

[32] Dvorak, Phred and Khan, Natasha, Hong Kong Protesters Adjust Tactics with Lessons from 2014 Umbrella Movement, Wall Street Journal, https://www.wsj.com/articles/hong-kong-protesters-adjust-tactics-with-lessons-from-2014-umbrella-movement-11560448247

[33] Article 29 Convention on the Rights of the Child, https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

Sweden[34] – who's Data Protection Authority fined a school for running a pilot testing facial recognition to monitor attendance including on the grounds that it was too invasive for that purpose.[35]

It is also important to note, that while there have been reports of China implementing a moratorium on the use of facial recognition in schools and in 2019 a member of the Chinese government promised to 'curb and regulate' it's use[36] 'a 2021 report by Article 19 suggests widespread use and promotion of emotion recognition – a technology that builds on facial recognition - including by companies building emotion recognition platforms for prison surveillance and police interrogations.[37]

2. Role and responsibilities of private actors in ensuring privacy and academic freedom

Educational technologies are rarely developed or run solely by the educational institutions who deploy them, instead it is private companies who are selling and operating EdTech solutions in schools, universities, and other educational settings. PI and its partners have documented several cases where public authorities have partnered with private companies to expand their surveillance capabilities and process mass quantities of personal data (including biometric data, such as facial images).[38] These public-private partnerships (PPPs) are taking on a new form, diverging from traditional public procurement relationships. There is an increasing dependency on private companies to run core functions in education in and around classrooms. EdTech companies will, more often than not, also be processing the data.

This becomes even more problematic if, without the correct protections, the collected data is further processed for commercial gain and shared with third parties. A Human Rights Watch report showed that this practice is widespread.[39] Of 163 EdTech products that they reviewed, 145 direct sent or granted access to personal data to 196 third-parties that they describe as "overwhelmingly AdTech".[40] These products may not all be apps, in Brazil, for example, 7 educational websites were extracting

[34] European Data Protection Board, Facial recognition in school renders Sweden's first GDPR fine, https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_sv
[35] International Association of Privacy Professionals, How to interpret Sweden's first GDPR fine on facial recognition in school, https://iapp.org/news/a/how-to-interpret-swedens-first-gdpr-fine-on-facial-recognition-in-school/
[36] BBC News, China to curb facial recognition and apps in schools, https://www.bbc.co.uk/news/world-asia-49608459
[37] Article 19, E Emotional Entanglement: China's emotion recognition market and its implications for human rights, p 28, https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf
[38] Privacy International, Public Private Surveillance Partnerships, https://privacyinternational.org/learn/public-private-surveillance-partnerships
[39] Human Rights Watch, "How Dare They Peep into My Private Life?", https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments
[40] *ibid*

children's data, including tracking their physical location, accessing their contact list, and downloading personal information about their family and friends.[41]

This creates serious concerns for academic freedom, as educational institutions – particularly those with inadequate data protection safeguards – are not be able to guarantee the final destination of that data.[42] While this kind of data collection and profiling is primarily used by advertising firms, buyers in America alone have included the National Security Agency (NSA),[43] the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), the US Special Operations Command (SOCOM), and more.[44] Moreover, EdTech will often collect highly sensitive data, including biometric data, that require enhanced protections.

The UN Special Rapporteur on the Right to Education has already underscored the importance for proactive measures by states and private stakeholders to address the associated risks of growing privatization and digitalization in education.[45] Principle 72 of the Abidjan Principles recognises that the integration of technology in the classroom and management systems must respect the right to privacy of both learners and educators.[46] In addition, the UN Guiding Principles on Business and Human Rights underscore that states bear the responsibility of safeguarding against human rights violations by all relevant stakeholders actors, including in privatised education.[47] In addition, states should establish transparent and effective legal frameworks for private actors, including private educational institutions and companies, to follow and ensure the availability of effective remedial measures.

[41] Submission by Privacy International, Data Privacy Brazil Research Association and Internet Lab in advance of the third periodic report of Brazil on the implementation of the International Covenant on Civil and Political Rights during the 138th session of the UN Human Rights Committee, https://www.dataprivacybr.org/wp-content/uploads/2023/06/20230526-PI-IL-DPB-submission-ICCPR-Brazil-final.pdf

[42] Privacy International, The companies in control of our secret identities, https://privacyinternational.org/long-read/4398/companies-control-our-secret-identities

[43] Ron Wyden United States Senator for Oregon, Wyden Releases Documents Confirming the NSA Buys Americans' Internet Browsing Records; Calls on Intelligence Community to Stop Buying U.S. Data Obtained Unlawfully From Data Brokers, Violating Recent FTC Order, https://www.wyden.senate.gov/news/press-releases/wyden-releases-documents-confirming-the-nsa-buys-americans-internet-browsing-records-calls-on-intelligence-community-to-stop-buying-us-data-obtained-unlawfully-from-data-brokers-violating-recent-ftc-order

[44] Electronic Freedom Foundation, How the Federal Government Buys our Cell Phone Location Data, https://www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data

[45] In 2022 the special rapporteur called for full abidance with the Abidjan Principles and the UN Guiding Principles on Business and Human Rights, which already offer guidance to ensure human rights-respecting practices in the EdTech sector. 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, para 99(a), https://www.ohchr.org/en/documents/thematic-reports/ahrc5032-impact-digitalization-education-right-education

[46] Abidjan Principles, 2019, https://www.abidjanprinciples.org/en/principles/overview

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

Aligned with the United Nations Guiding Principles on Business and Human Rights, PI has formulated an extensive set of safeguards to guide these partnerships.[48] Targeted at both states and companies, these safeguards are designed to mitigate the inherent risks of human rights abuses stemming from PPPs reliant on personal data processing.

One Danish city was found, for example, to have failed to carry out a mandatory risk assessment for Google technologies they implemented in schools[49] – and as such didn't really understand where the data that the systems collected went or what steps they should have been taking to protect the data being entrusted to Google. This kind of inadequate understanding and review is exacerbated when academic institutions are given technologies allegedly for free – which is an increasingly common feature of these kind of public private partnerships.[50]

It is vital for the protection and promotion of academic freedom that these partnerships are as transparent, clear, and protective as possible.

3. Recommendations

In particular, PI suggests the UN Special Rapporteur to call on states to:

- **Adhere to human rights standards:** Uphold international and national human rights standards, prioritizing the right to privacy as a foundational gateway right crucial for ensuring academic freedom. Additionally, consider the rights of the child in the context of EdTech.
- **Regulate EdTech use:** Implement regulations governing the use of EdTech in academic settings (including private institutions), ensuring alignment with robust data protection standards and to guarantee educational institutions create an environment which enables rather than supresses academic freedom.
- **Ban facial recognition technology (FRT) in educational settings:** Prohibit the use of facial recognition technology (FRT) in educational settings due to its disproportionate impact, security risks, inaccuracies, and discriminatory biases that pose threats to academic freedom.

[48] Privacy International, Safeguards for Public-Private Surveillance Partnerships, https://privacyinternational.org/our-demands/safeguards-public-private-surveillance-partnerships

[49] Wired, A Danish City Built Google Into It's Schools Then Banned It, https://www.wired.co.uk/article/denmark-google-schools-data

[50] USA Today, Free Google Wi-Fi transforms rural schools buses into rolling classroom, https://eu.usatoday.com/story/tech/news/2018/04/02/google-giving-rural-school-bus-riders-free-wi-fi-homework/476899002/; The Verge, Google donates free Chromebooks and 100,000 mobile hotspots for rural California students, https://www.theverge.com/2020/4/2/21204057/google-free-chromebooks-wi-fi-hotspots-california-schools-students-remote-learning-coronavirus; Valley News Live, All Middle and High Schools in ND to Receive Donation of Virtual Reality Headsets, https://www.valleynewslive.com/2024/02/01/all-middle-high-schools-nd-receive-donation-virtual-reality-headsets/

- **Conduct human rights due diligence:** Implement robust human rights due diligence processes, including data protection and child rights impact assessments prior and throughout to their deployment in educational settings.
- **Formal public procurement processes:** Adhere to formal and transparent public procurement processes when awarding contracts to EdTech companies, accompanied by comprehensive documentation governing the partnership.