



**Human Rights Watch Submission
to the United Nations Human Rights Committee
Review of Colombia
138th Session
May 2023**

We write in advance of the 138th session of the Human Rights Committee (“the Committee”) and its review of Colombia in its implementation of the International Covenant on Civil and Political Rights. This submission focuses solely on government-endorsed online learning during the Covid-19 pandemic.

Children’s Rights Abuses by Government-Endorsed Online Learning During the Covid-19 Pandemic (articles 2, 17, 18, 19, and 24)

In a global investigation of education technology (EdTech) products endorsed by the world’s most populous countries for children’s education during the Covid-19 pandemic, Human Rights Watch found that the Colombian government directly violated children’s right to privacy and other rights.¹

Human Rights Watch analyzed Aprender Digital, a website developed and launched by the Colombian Ministry of National Education on March 16, 2020 to provide students with digital educational content during Covid-19 school closures,² as well as seven other privately-built platforms recommended by the ministry: Dropbox, Edmodo, Jumpshare, Padlet, Remind, WeTransfer, and Workflow.³ Of these eight products, one was a mobile application (“app”), three were websites, and four were available in both formats.

Our analysis found that all eight EdTech products surveilled or had the capacity to surveil children online, outside school hours, and deep into their private lives. All eight EdTech products could or did transmit children’s personal data to third-party advertising technology (AdTech) companies.

Finding Out Who Children Are

¹ Human Rights Watch, *“How Dare They Peep into My Private Life?”: Children’s Rights Violations by Governments that Endorsed Online Learning during the Covid-19 Pandemic* (New York: Human Rights Watch, 2022), <https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments>.

² Colombia Ministerio de Educación Nacional, “‘Aprender Digital: Content for Everyone’ strategy brings together digital educational content on one platform for school levels in all knowledge areas,” (“Estrategia ‘Aprender Digital: Contenidos para Todos’ reúne contenidos digitales educativos en una misma plataforma para los niveles escolares en todas las áreas del conocimiento”) March 16, 2020, <https://www.mineducacion.gov.co/portal/salaprensa/Noticias/394002:Estrategia-Aprender-Digital-Contenidos-para-Todos-reune-contenidos-digitales-educativos-en-una-misma-plataforma-para-los-niveles-escolares-en-todas-las-areas-del-conocimiento> (accessed April 17, 2023).

³ See “Students Not Products” (webpage), Human Rights Watch interactive index, 2022, <https://www.hrw.org/StudentsNotProducts>.

Four EdTech products authorized by the education ministry for children's use had the capability to collect their users' Android Advertising IDs, allowing them to tag, collectively, an estimated 1.25 billion users and uniquely identify their devices for the sole purpose of advertising to them.⁴

These identifiers enabled companies to infer the interests and characteristics of individual children for commercial purposes. Every time a child connects to the internet and comes into contact with tracking technology, any information collected about that child is tied back to the identifier associated with them by that company, resulting in a comprehensive profile over time. Data tied together in this way do not need a real name to be able to target a real child or person.

Human Rights Watch submits that these tracking techniques are neither proportionate nor necessary for these products to function, or to deliver educational content to children. Their use on children in an educational setting arbitrarily interferes with children's right to privacy.

Tracking Who Children Know

Four apps recommended by the education ministry for children's use had the ability to collect information about their users' friends, family, and other acquaintances by accessing the contacts list saved on users' phones.⁵ This allowed these apps to learn personal details about these contacts, including any saved names, phone numbers, emails, addresses, relationships, and profile photos. Human Rights Watch found that this data was neither necessary for these apps to function, nor provided educational benefit to children.

When details about the personal relationships of a child are collected without consent or awareness by the child or by the family member or friend in question, it is an arbitrary intrusion on the privacy of each of these individuals. For contacts, the right to privacy is affected by the "mere collection of personal data" in which they lose control over information, in addition to the risk of experiencing potential misuse of their personal data.⁶

Tracking What Children Do Inside and Outside the Classroom

Ad trackers and third-party cookies are generally used by AdTech companies to scrutinize a person's every action and behavior, infer their characteristics and interests, and deliver

⁴ Human Rights Watch, "Privacy Snapshot: Remind,"

https://features.hrw.org/features/StudentsNotProducts/files/privacy_snapshots/Privacy%20Snapshot%20-%20Colombia%20Remind.pdf; "Privacy Snapshot: Global: Padlet,"

https://features.hrw.org/features/StudentsNotProducts/files/privacy_snapshots/Privacy%20Snapshot%20-%20Global%20Padlet.pdf;

"Privacy Snapshot: Global: Edmodo,"

https://features.hrw.org/features/StudentsNotProducts/files/privacy_snapshots/Privacy%20Snapshot%20-%20Global%20Edmodo.pdf; "Privacy Snapshot: Dropbox,"

https://features.hrw.org/features/StudentsNotProducts/files/privacy_snapshots/Privacy%20Snapshot%20-%20Colombia%20Dropbox.pdf.

⁵ Human Rights Watch, "Privacy Snapshot: Remind,"

https://features.hrw.org/features/StudentsNotProducts/files/privacy_snapshots/Privacy%20Snapshot%20-%20Colombia%20Remind.pdf; "Privacy Snapshot: Global: Padlet,"

https://features.hrw.org/features/StudentsNotProducts/files/privacy_snapshots/Privacy%20Snapshot%20-%20Global%20Padlet.pdf;

"Privacy Snapshot: Global: Edmodo,"

https://features.hrw.org/features/StudentsNotProducts/files/privacy_snapshots/Privacy%20Snapshot%20-%20Global%20Edmodo.pdf; "Privacy Snapshot: Dropbox,"

https://features.hrw.org/features/StudentsNotProducts/files/privacy_snapshots/Privacy%20Snapshot%20-%20Colombia%20Dropbox.pdf.

⁶ United Nations Human Rights Council, Report of the UN High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/39/29, August 3, 2018, para. 7.

customized ads and content that follow them around the internet. All seven EdTech websites extracted and sent children's data to AdTech companies, using ad trackers and third-party cookies that tracked users across the internet.

Of these, three websites, including Aprender Digital, the website owned and operated by the education ministry, sent children's data to AdTech companies that specialize in behavioral advertising or whose algorithms determine what children see online. In doing so, these companies not only distorted or risked distorting children's online experiences, but also risked influencing their opinions and beliefs at a time in their lives when they are at high risk of manipulative interference.⁷ Human Rights Watch also found Aprender Digital sending children's data to Google through Google Analytics' "remarketing audiences" tool, allowing the website to potentially track its users with ads across the internet.

This unnecessary, disproportionate data surveillance enabled advertisers and other companies to use children's data for commercial purposes, and exposed children to further risk of misuse and exploitation of their data. Their use on children in an educational setting unreasonably infringes on children's right to privacy.

Government Failure to Protect

All EdTech products reviewed by Human Rights Watch engaged in data practices that unreasonably infringed on children's rights or risked doing so.

All the privately-owned EdTech products were marketed as free and appeared to have been provided to the Colombian government at no direct financial cost. In the process of endorsing these and promoting their wide adoption by schools, teachers, and students, the Colombian education ministry offloaded the true costs of providing education online onto children, who were forced to pay for their learning with their rights to privacy, access to information, and freedom of thought.

Human Rights Watch did not find evidence that the education ministry took measures to prevent or mitigate children's rights abuses by companies, or that it checked whether the EdTech products it was rapidly endorsing were safe for children to use. As a result, children whose families were able to afford access to the internet and connected devices, or who made hard sacrifices in order to do so, were exposed to the privacy practices of the EdTech products they were told or required to use during Covid-19 school closures.

Children, parents, and teachers were largely kept in the dark about these data surveillance practices. Neither the government nor the companies informed children and their parents of the full extent of these data practices that risked or infringed on children's rights. As these tracking technologies were invisible to the user, children had no reasonably practical way of knowing the existence and extent of these data practices, much less the impacts on their rights. By withholding critical information, the government and these companies impeded children's access to justice and remedy.

⁷ Human Rights Watch, *"How Dare They Peep into My Private Life?"*, pp. 67-87.

Even if children, parents, and teachers had known about these data practices, Human Rights Watch found that the data surveillance took place in virtual classrooms and educational settings where children could not reasonably object to such surveillance. These companies did not allow students to decline to be tracked; this monitoring happened secretly, without the child's knowledge or consent. In most instances, it was impossible for children to opt out of such surveillance and data collection without opting out of compulsory education and giving up on formal learning during the pandemic.

Human Rights Watch recommends that the Committee ask the government of Colombia:

- What recourse or remedy does the government provide, or is planning to provide, to children who have experienced unreasonable infringements of their rights as a result of their use of these EdTech products and whose data remain at risk of misuse and exploitation?

Human Rights Watch recommends that the Committee call on the government of Colombia to:

- Update and strengthen implementation of the data protection law to deliver a comprehensive child data protection framework that protects the best interests of the child in complex online environments, and ensures that companies respect children's rights and are held accountable if they fail to do so.
- Provide remedy for children whose data were collected through their use of EdTech products. To do so:
 - Conduct a data privacy audit of all EdTech websites and apps it has endorsed for children's online learning. If the products fail this audit, rescind endorsement of these products, and immediately notify and guide affected schools, teachers, parents, and children to prevent further collection and misuse of children's data.
 - Require EdTech companies with failed data privacy audits to delete any children's data collected during the pandemic.
 - Require AdTech companies to identify and immediately delete any children's data they received from EdTech companies during the pandemic.
- Ensure that any services that are endorsed or procured to deliver online education are safe for children. In coordination with data protection authorities and other relevant institutions:
 - Require all companies providing educational services to children to identify, prevent, and mitigate negative impacts on children's rights, including across their business relationships and global operations.
 - Require child data protection impact assessments of any educational technology provider seeking public investment, procurement, or endorsement.
 - Ensure that public and private educational institutions enter into written contracts with EdTech providers that include protections for children's data.
 - Define and provide special protections for categories of sensitive personal data that should never be collected from children in educational settings, such as precise geolocation data.