“How Dare They Peep into My Private Life?”

Children’s Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic
“How Dare They Peep into My Private Life?”

Children's Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic
Human Rights Watch defends the rights of people worldwide. We scrupulously investigate abuses, expose the facts widely, and pressure those with power to respect rights and secure justice. Human Rights Watch is an independent, international organization that works as part of a vibrant movement to uphold human dignity and advance the cause of human rights for all.


For more information, please visit our website: HRW.org
“How Dare They Peep into My Private Life?”

Children’s Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic

Summary

Recommendations
- To Governments
- To Ministries and Departments of Education
- To Education Technology Companies
- To Advertising Technology Companies and other Third-Party Companies that May Receive Data from EdTech Products

Methodology
- Selection Criteria
- Product Types
- Access and Archival
- Technical Analysis: Apps
  - Dynamic Analysis and Children’s Participation
- Technical Analysis: Websites
- Technical Limitations
- Interviews with Children, Parents, and Teachers
- Requests for Comment

I. Covid-19, Education, and Technology
- Covid-19 and Children’s Education
- How the Internet-Based Economy Works

II. Hidden Surveillance: Children’s Data Harvested
- Children’s Data and their Right to Privacy
- Finding Out Who Children Are
  - Apps: Persistent Identifiers
- Inescapable Surveillance
  - Websites: Canvas Fingerprinting
- Tracking Where Children Are
  - Apps: Precise Location Data
  - Websites: Coarse Location Data
- Tracking Who Children Know
- Tracking What Children Do in the Classroom
- Websites: Ad Trackers
- Websites: Session Recording, Key Logging
  - Apps: Software Development Kits (SDKs)
- Tracking Children Outside of the Classroom
  - Website Cookies

HOWARD LEW-ADLER
1 HOW DARE THEY PEEP INTO MY PRIVATE LIFE?

Summary

On school days, 9-year-old Rodin wakes up every morning at 8 a.m. in Istanbul, Turkey. He eats a bowl of chocolate cereal for breakfast; his mother reminds him, as she always does, to brush his teeth afterwards. By 9 a.m., he logs into class and waves hello to his teacher and to his classmates. He hopes that no one can tell that he’s a little sleepy, or that he’s behind on his homework.

During breaks between classes, Rodin reads chat messages from his classmates and idly doodles on the virtual whiteboard that his teacher leaves open. He watches his best friend draw a cat; he thinks his friend is much better at drawing than he is. Later in the afternoon, Rodin opens up a website to watch the nationally televised math class for that day. At the end of each day, he posts a picture of his homework to his teacher’s social media page.

Unbeknownst to him, an invisible swarm of tracking technologies surveil Rodin’s online interactions throughout his day. Within milliseconds of Rodin logging into class in the morning, his school’s online learning platform begins tracking Rodin’s physical location—at home in his family’s living room, where he has spent most of his days during the pandemic lockdown. The virtual whiteboard passes along information about his doodling habits to advertising technology (AdTech) and other companies; when Rodin’s math class is over, trackers follow him outside of his virtual classroom and to the different apps and sites he visits across the internet. The social media platform Rodin uses to post his homework silently accesses his phone’s contact list and downloads personal details about his family and friends. Sophisticated algorithms review this trove of data, enough to piece together an intimate portrait of Rodin in order to figure out how he might be easily influenced.

Neither Rodin nor his mother were aware that this was going on. They were only told by his teacher that he had to use these platforms every day to be marked as attending school during the Covid-19 pandemic.1

This report is a global investigation of the education technology (EdTech) endorsed by 49 governments for children’s education during the pandemic. Based on technical and policy analysis of 163 EdTech products, Human Rights Watch finds that governments’ endorsements of the majority of these online learning platforms put at risk or directly violated children’s privacy and other children’s rights, for purposes unrelated to their education.

1 Human Rights Watch interview with Rodin R. and his mother, Istanbul, Turkey, June 11, 2021. The names of all children quoted in this report have been changed to protect their privacy.
The coronavirus pandemic upended the lives and learning of children around the world. Most countries pivoted to some form of online learning, replacing physical classrooms with EdTech websites and apps; this helped fill urgent gaps in delivering some form of education to many children.

But in their rush to connect children to virtual classrooms, few governments checked whether the EdTech they were rapidly endorsing or procuring for schools were safe for children. 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.

Human Rights Watch conducted its technical analysis of the products between March and August 2021, and subsequently verified its findings as detailed in the methodology section. Each analysis essentially took a snapshot of the prevalence and frequency of tracking technologies embedded in each product on a given date in that window. That prevalence and frequency may fluctuate over time based on multiple factors, meaning that an analysis conducted on later dates might observe variations in the behavior of the products.

Of the 163 EdTech products reviewed, 145 (89 percent) appeared to engage in data practices that put children's rights at risk, contributed to undermining them, or actively infringed on these rights. These products monitored or had the capacity to monitor children, in most cases secretly and without the consent of children or their parents, in many cases harvesting data on who they are, where they are, what they do in the classroom, who their family and friends are, and what kind of device their families could afford for them to use.

Most online learning platforms installed tracking technologies that trailed children outside of their virtual classrooms and across the internet, over time. Some invisibly tagged and fingerprinted children in ways that were impossible to avoid or get rid of—even if children, their parents, and teachers had been aware and had the desire and digital literacy to do so—without throwing the device away in the trash.

Most online learning platforms sent or granted access to children’s data to third-party companies, usually advertising technology (AdTech) companies. In doing so, they appear to have permitted the sophisticated algorithms of AdTech companies the opportunity to stitch together and analyze these data to guess at a child’s personal characteristics and interests, and to predict what a child might do next and how they might be influenced. Access to these insights could then be sold to anyone—advertisers, data brokers, and others—who sought to target a defined group of people with similar characteristics online.

Children are surveilled at dizzying scale in their online classrooms. Human Rights Watch observed 146 EdTech products directly sending or granting access to children's personal data to 199 AdTech companies. Of the 163 EdTech products reviewed, 145 (89 percent) appeared to engage in data practices that put children's rights at risk, contributed to undermining them, or actively infringed on these rights. These products monitored or had the capacity to monitor children, in most cases secretly and without the consent of children or their parents, in many cases harvesting data on who they are, where they are, what they do in the classroom, who their family and friends are, and what kind of device their families could afford for them to use.

Most online learning platforms installed tracking technologies that trailed children outside of their virtual classrooms and across the internet, over time. Some invisibly tagged and fingerprinted children in ways that were impossible to avoid or get rid of—even if children, their parents, and teachers had been aware and had the desire and digital literacy to do so—without throwing the device away in the trash.

Most online learning platforms sent or granted access to children’s data to third-party companies, usually advertising technology (AdTech) companies. In doing so, they appear to have permitted the sophisticated algorithms of AdTech companies the opportunity to stitch together and analyze these data to guess at a child’s personal characteristics and interests, and to predict what a child might do next and how they might be influenced. Access to these insights could then be sold to anyone—advertisers, data brokers, and others—who sought to target a defined group of people with similar characteristics online.

Children are surveilled at dizzying scale in their online classrooms. Human Rights Watch observed 145 EdTech products directly sending or granting access to children’s personal data to 196 third-party companies, overwhelmingly AdTech. Put another way, the number of AdTech companies receiving children’s data was discovered to be far greater than the EdTech companies sending this data to them, illustrating the financial incentives that place economic value on children’s data and fuel extraordinarily intrusive surveillance and deep erosions of their privacy.
Some EdTech products targeted children with behavioral advertising. By using children’s data—extracted from educational settings—to target them with personalized content and advertisements that follow them across the internet, these companies not only distorted 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. Many more EdTech products sent children’s data to AdTech companies that specialize in behavioral advertising or whose algorithms determine what children see online.

It is not possible for Human Rights Watch to reach definitive conclusions as to the companies’ motivations in engaging in these actions, beyond reporting on what we observed in the data and the companies’ and governments’ own statements. In response to requests for comment, several EdTech companies denied collecting children’s data. Some companies denied that their products were intended for children’s use, or stressed that their virtual classroom pages for children’s use had adequate privacy protections, even if Human Rights Watch’s analysis found that pages adjacent to the virtual classroom pages (such as the login page, home page or adjacent page with children’s content) did not. AdTech companies denied knowledge that the data was being sent to them, indicating that in any case it was their clients’ responsibility not to send them children’s data.

Governments bear the ultimate responsibility for failing to protect children’s right to education. With the exception of a single government—Morocco—all governments reviewed in this report endorsed at least one EdTech product that risked or undermined children’s rights. Most EdTech products were offered to governments at no direct financial cost to them; in the process of endorsing and ensuring their wide adoption during Covid-19 school closures, governments offloaded the true costs of providing online education onto children, who were unknowingly forced to pay for their learning with their rights to privacy, access to information, and potentially freedom of thought.

Many governments put at risk or violated children’s rights directly. Of the 42 governments that provided online education to children by building and offering their own EdTech products for use during the pandemic, 39 governments produced products that handled children’s personal data in ways that risked or infringed on their rights. Some of these governments made it compulsory for students and teachers to use their EdTech product, not only subjecting them to the risks of misuse or exploitation of their data, but also making it impossible for children to protect themselves by opting for alternatives to access their education.

Children, parents, and teachers were denied the knowledge or opportunity to challenge these data surveillance practices. Most EdTech companies did not disclose their surveillance of children through their data; similarly, most governments did not provide notice to students, parents, and teachers when announcing their EdTech endorsements.

In all cases, this data surveillance took place in virtual classrooms and educational settings where children could not reasonably object to such surveillance. Most EdTech companies did not allow their students to decline to be tracked; most of 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 altogether during the pandemic.
Remedy is urgently needed for children whose data were collected during the pandemic and remain at risk of misuse and exploitation. Governments should conduct data privacy audits of the EdTech endorsed for children's learning during the pandemic, remove those that fail these audits, and immediately notify and guide affected schools, teachers, parents, and children to prevent further collection and misuse of children's data.

In line with child data protection principles and corporations' human rights responsibilities as outlined in the United Nations Guiding Principles on Business and Human Rights, EdTech and AdTech companies should not collect and process children's data for advertising. Companies should inventory and identify all children's data ingested during the pandemic, and ensure that they do not process, share, or use children's data for purposes unrelated to the provision of children's education. AdTech companies should immediately delete any children's data they received; EdTech companies should work with governments to define clear retention and deletion rules for children's data collected during the pandemic.

As more children spend increasing amounts of their childhood online, their reliance on the connected world and digital services that enable their education will continue long after the end of the pandemic. Governments should develop, refine, and enforce modern child data protection laws and standards, and ensure that children who want to learn are not compelled to give up their other rights in order to do so.

Children should be actively consulted throughout these processes, helping to build safeguards that protect meaningful, safe access to online learning environments that provide the space for children to develop their personalities and their mental and physical abilities to their fullest potential.
To Governments

Facilitate urgent remedy for children whose data were collected during the pandemic and remain at risk of misuse and exploitation. To do so:

- Conduct data privacy audits of the EdTech endorsed for children’s learning during the pandemic, remove those that fail these audits, 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 identify and immediately 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.

- Prevent the further collection and processing of children’s data by technology companies for the purposes of profiling, behavioral advertising, and other uses unrelated to the purpose of providing education.

Adopt child-specific data protection laws that address the significant child rights impacts of the collection, processing, and use of children’s personal data. Where child data protection laws already exist, update and strengthen implementation measures to deliver a modern child data protection framework that protects the best interests of the child in complex online environments.

Enact and enforce laws ensuring that companies respect children’s rights and are held accountable if they fail to do so. In line with the United Nations Guiding Principles on Business and Human Rights, such laws should require companies to:

- Conduct and publish child rights due diligence processes.

- Provide full transparency in data supply chains, and publicly report on how children’s data are collected and processed, where they are sent, to whom, and for what purpose.

- Provide child-friendly, age-appropriate processes for remedy and redress for children who have experienced infringements on their rights; such mechanisms should be transparent, independently accountable, and enforceable.

Require child rights impact assessments in any public procurement processes that provide essential services to children through technology.

Ban behavioral advertising to children. Commercial interests and behavioral advertising should not be considered legitimate grounds of data processing that override a child’s best interests or their fundamental rights.

Ban the profiling of children. In exceptional circumstances, governments may lift this restriction when it is in the best interests of the child, and only if appropriate safeguards are provided for by law.
To Ministries and Departments of Education

Where online learning is adopted as a preferred or hybrid mechanism for delivering education, allocate funding to pay for services that safely enable online education, rather than allowing the sale and trading of children’s data to finance the services.

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. Children should not be expected to enter into a contract, and children and guardians cannot give valid consent when it cannot be freely refused without jeopardizing a child’s right to education.

- 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.

Provide child-friendly, age-appropriate, and confidential reporting mechanisms, access to expert help, and provisions for collective action in local languages for children seeking justice and remedy. Such measures should avoid placing undue burden or exclusive responsibility on children or their caregivers to seek remedy from companies by acting individually or exposing themselves in the process.

Develop and promote digital literacy and children’s data privacy in curricula. Provide training programs for ministry staff, teachers, and other school staff in digital literacy skills and protection of children’s data privacy, to support teachers to conduct online learning for children safely.

Seek out children’s views in developing policies that protect the best interests of the child in online educational settings, and meaningfully engage children in enhancing the positive benefits that access to the internet and educational technologies can provide for their education, skills, and opportunities.
To Education Technology Companies

Provide urgent remedy and redress where children’s rights have been put at risk or infringed through companies’ data practices during the pandemic. To do so:

- Immediately stop collecting and processing children’s data for user profiling, behavioral advertising, or any purpose other than what is strictly necessary and relevant for the provision of education.

- Stop sharing children’s data for purposes that are unnecessary and disproportionate to the provision of their education. In instances where children’s data are disclosed to a third party for a legitimate purpose, in line with child rights principles and data protection laws, enter into explicit contracts with third-party data processors, and apply strict limits to their processing, use, and retention of the data they receive.

- Apply child flags to any data shared with third parties, to ensure that adequate notice is provided to all companies in the technology stack that they are receiving children’s personal data, and thus obliged to apply enhanced protections in their processing of this data.

- Inventory and identify children’s personal data ingested during the pandemic, and take measures to ensure that these data are no longer processed, shared, retained, or used for commercial or other purposes that are not strictly related to the provision of children’s education.

- Companies with EdTech products designed for use by children should stop collecting specific categories of children’s data that heighten risks to children’s rights, including their precise location data and advertising identifiers.

Undertake child rights due diligence to identify, prevent, and mitigate companies’ negative impact on children's rights, including across their business relationships and global operations, and publish the outcomes of this due diligence process.

Respect and promote children’s rights in the development, operation, distribution, and marketing of EdTech products and services. Ensure that children's data are collected, processed, used, protected, and deleted in line with child data protection principles and applicable laws.

Provide privacy policies that are written in clear, child-friendly, and age-appropriate language. These should be separate from legal and contractual terms for guardians and educators.

Provide children and their caregivers with child-friendly mechanisms to report and seek remedy for rights abuses when they occur. Remedies should involve prompt, consistent, transparent, and impartial investigation of alleged abuses, and should effectively end ongoing infringements on rights.
To Advertising Technology Companies and other Third-Party Companies that May Receive Data from EdTech Products

Inventory and identify all children’s data received through tracking technologies the technology companies own and take measures to promptly delete these data and ensure that these data are not processed, shared, or used. To do so:

- Identify all apps and websites that have installed tracking technologies owned by technology companies and transmitted user data to them.

- Of these, classify and create a list of services primarily directed at children, which should be monitored and updated periodically. Notify the parent companies of these services that they need to provide explicit evidence that their service is not made for children to remove their product from this list.

- Using this list, companies should review and promptly delete any children’s data received from services made for children.

Prevent the use of technology companies’ tracking technologies to surveil children, or any user of these services designed for use by children.

- Regularly audit incoming data and the companies sending them. Delete or otherwise disable the use of any received children’s data or user data received from services designed for use by children, when detected.

- Notify and require companies and clients that use tracking technologies to declare any children’s data collected through these tools with a child flag or through other means, so that tagged data can be automatically flagged and deleted before transmission to third-party companies.

Develop and implement effective processes to detect and prevent the commercial use of children’s data collected by technology companies’ tracking technologies.

Undertake child rights due diligence to identify, prevent, and mitigate technology companies’ impact on children’s rights, including across their business relationships and across global operations, and publish the outcomes of this due diligence process.

Provide children and their caregivers with child-friendly mechanisms to report and seek remedy for infringements on rights when they occur. Remedies should involve prompt, consistent, transparent, and impartial investigation of alleged infringements, and should end ongoing violations.
Methodology

This report covers 49 countries that recommended 163 educational technology (EdTech) products for children to use for online learning during Covid-19 school closures.

Human Rights Watch conducted technical analysis on each product to assess how it handled children’s data, then compared the results to the product’s privacy policy to determine whether the EdTech company disclosed its data practices to children and their caregivers. Human Rights Watch also examined the advertising technology (AdTech) companies and data brokers found to receive children’s data, and analyzed the marketing materials and developer documentation of those found to be receiving significant amounts of children’s data.

The methods used in this report were free and available for use by governments prior to endorsing or procuring any of the EdTech products analyzed here. While a tool that was used to analyze websites, Blacklight, was published in September 2020, the tests it runs to identify privacy-infringing technologies were individually available and free to use in the form of various privacy census tools built over the past decade. As of November 2021, no government reviewed in this report was found to have undertaken a technical privacy evaluation of the EdTech products they recommended after the declaration of the pandemic in March 2020.

Human Rights Watch invites experts, journalists, policymakers, and readers to recreate, test, and engage with our findings and research methods. Our datasets, preserved evidence, and a detailed technical methodology can be found online.

Selection Criteria

Human Rights Watch examined the Covid-19 education emergency response plans, documents, and announcements of 68 of the world’s most populous countries. Of these, 49 countries adopted online learning as a component of their national plans for continued learning throughout school closures. The EdTech products endorsed or procured by these ministries or departments of education were included for analysis in this report.

In countries where the education ministry recommended a large number of EdTech products—in some cases, numbering in the hundreds—a Mersenne Twister pseudorandom number generator was used to randomly select a maximum of ten products that would serve as an illustrative sample of that education ministry’s decisions.2

---

Seven countries—Australia, Brazil, Canada, Germany, India, Spain, and the United States—delegate significant decision-making authority to state—or regional—level education authorities. During the pandemic, this included decisions about what EdTech to endorse or procure for school use. Human Rights Watch identified the two most populous states or provinces in these countries and included their EdTech endorsements for analysis. Similarly for the United Kingdom, the two most populous constituent countries—England and Scotland—were identified for analysis.

As a result, 163 products were analyzed from the following 49 countries: Argentina, Australia (New South Wales, Victoria), Brazil (Minas Gerais, São Paulo), Burkina Faso, Cameroon, Canada (Quebec), Chile, China, Colombia, Côte d’Ivoire, Ecuador, Egypt, France, Germany (Baden-Württemberg, Bavaria), Ghana, Guatemala, India (Maharashtra, national, Uttar Pradesh), Indonesia, Iran, Iraq, Italy, Japan, Kenya, Malawi, Malaysia, Mexico, Morocco, Nepal, Nigeria, Pakistan, Peru, Poland, Republic of Korea, Romania, Russian Federation, Saudi Arabia, South Africa, Spain (Andalucía, Catalonia), Sri Lanka, Taiwan, Thailand, Turkey, United Kingdom (England, Scotland), United States (California, Texas), Uzbekistan, Venezuela, Vietnam, and Zambia.

Product Types

Of the 163 EdTech products investigated by Human Rights Watch, 39 were mobile applications (“apps”), 90 were websites, and 34 were available in both formats. Of the products available in both app and website formats, Human Rights Watch analyzed both, except for four products where the app versions were no longer available online, or offered only in iOS, Apple’s operating system.

Apps running on Google’s Android operating system are the focus of this report. Android is the dominant mobile operating system worldwide, in large part due to the ubiquity of lower-cost mobile phones that run Android.4 Children living in the countries covered by this report are more likely to have access to an Android device, if they have access to a device at all. This was reflected in the choices that governments made: almost all EdTech products endorsed by the governments covered in this report offer their apps for the Android platform.

In addition, Android’s open architecture makes it possible to easily access and observe the interactions between an app and the operating system, as well as to identify the data transmissions from the device running the app to online servers.

While this report focuses on apps built for Android, apps built for Apple’s iOS can also employ data tracking technologies and target behavioral advertising to users.5

---

3 Canada’s Ontario, and the single EdTech product that it recommended, was originally included in our analysis. After additional rounds of data verification and analysis of the EdTech product, which yielded an inconclusive assessment, Human Rights Watch removed Ontario from its list.


Access and Archival

To investigate how EdTech products handled children’s data and their rights, Human Rights Watch downloaded a copy of the latest version of the product and its privacy policy between February 19 and March 15, 2021. Human Rights Watch conducted the primary phase of its investigation between March and August 2021, and conducted further checks in November 2021 to verify findings.

To preserve documentation and to invite readers to recreate, test, and engage with our findings, the privacy policy, and EdTech website or app were archived, whenever available, on the Internet Archive’s Wayback Machine. The versions of the EdTech apps examined by Human Rights Watch are listed in the appendices.

EdTech products were sorted into the following categories:

1. Products that do not require a user account to access learning content;
2. Products that offer the choice to sign up for an optional user account;
3. Products that require a user account to access learning content; and
4. Products that require verification of the child’s identity as a student, either by their school or their ministry of education, to set up a mandatory account to access the service.

To avoid misleading EdTech companies as to our affiliation and the nature of our research, no user accounts were created for products identified in categories 1, 2, and 4.

Human Rights Watch created user accounts for a limited number of EdTech products in category 3. As it is possible to disassemble and analyze apps’ code without having to sign into a user account, accounts were created only for 27 websites in this category to test for privacy violations in the same environment used by children to attend classes. In these instances, Human Rights Watch explicitly identified the nature of our engagement, populating mandatory input fields with the following values to signal our affiliation and intent. Optional fields were left blank.

Email: iamaresearcher@hrw.org
User name: hrwresearcher
Organization / School name: Human Rights Watch
First Name: HRW
Last Name: Researcher
Phone number: [a real number]

Throughout its investigation, Human Rights Watch did not interact with other users or enter into virtual classrooms.

Human Rights Watch did not create user accounts for products in category 4, as that would have entailed falsely assuming the identity of a real student. For these websites, technical analysis was restricted to webpages that children likely had to interact with in order to access their virtual classroom, prior to logging in, such as the product’s home page or login page.

Some of the companies that offered EdTech products in category 4 told Human Rights Watch that the virtual classrooms and related spaces accessible to children after the login were adequately protective of privacy. These companies asserted that the pages before their product’s login (e.g., the login page, home page, or adjacent page designed for children) were designed for use by teachers, parents and other adults, and not properly described as designed for children’s use.
Technical Analysis: Apps

There are two methods of disassembling and analyzing a mobile app. The first is through static analysis, which analyzes an app’s code and identifies its capabilities, or the functions and instructions that may be executed when the app is run. The second is through dynamic analysis, which runs the app under realistic conditions and observes what data is transmitted where, and to whom.

Human Rights Watch conducted manual static analysis tests on 73 apps, using Android Developer Studio to decompile the app and to analyze its code. All results were verified by scanning each app using Pithus, an open source mobile threat intelligence platform that conducts automated static analysis tests on mobile apps, and exodus by exodus Privacy, an open source privacy auditing platform that scans for trackers embedded in Android apps, and corroborating the results against Human Rights Watch’s analyses.

Additionally, Human Rights Watch commissioned Esther Onfroy, founder of Defensive Lab Agency, and the creator of both Pithus and exodus Privacy, to conduct in-depth static and dynamic analysis on eight apps, which were used as a final check to ensure the accuracy of our results.

Dynamic Analysis and Children’s Participation

Human Rights Watch collaborated with four children from India, Indonesia, South Africa, and Turkey who participated in an in-depth investigation to uncover how an EdTech app recommended by their government handled their privacy.

These children and their guardians were informed of the nature and purpose of our research, that they would receive no personal service or benefit for speaking to us, and our intention to publish a report with the information gathered. Human Rights Watch requested and received consent from the children and their guardians, and informed each that they were under no obligation to speak with us or to participate in the project.

Human Rights Watch asked each child to download a virtual private network (VPN) and the EdTech app on their mobile device. They were then asked to open, run, and close the VPN and the EdTech app several times within a single day, interacting with the app as if they were using it for school or for learning. After 24 hours, children deleted both from their phones.

Esther Onfroy of the Defensive Lab Agency received the data files and analyzed them to identify data flows and transmissions. These findings were corroborated against dynamic analysis conducted on each app, using a VPN to simulate app usage in the child’s country. This methodology design maximally protected children’s privacy by encrypting the child’s data and ensuring that only the data flows could be analyzed, without revealing the substance of children’s personal data.

All children’s data were securely stored, then deleted, at the end of the investigation. The data files for one child’s experiment were provided to the child, at their request.

Technical Analysis: Websites

To understand how websites handle children’s data, Human Rights Watch used Blacklight, a real-time website privacy inspector built by Surya Mattu, senior data engineer and investigative data journalist at The Markup.7

Released in September 2020, Blacklight emulates how a user might be surveilled while browsing the web.8 The tool scans any website, runs tests for seven known types of surveillance, and returns an instant privacy analysis of the inspected site. Built on the foundation of robust privacy census tools built over the past decade, Blacklight monitors scripts and network requests to observe when and how user data is being collected, and records when this data is being sent to known third-party AdTech companies.9

Blacklight exists in two formats: as a user-friendly interface on The Markup’s website, and as an open source command-line tool.10 Human Rights Watch chose to work with the latter, as it provides the flexibility to adapt the tool to provide customized analysis, as well as a higher observational power that yields fine-grained evidence of the surveillance it detects on websites. Surya Mattu of The Markup generously assisted Human Rights Watch in customizing Blacklight for this investigation.

In order to recreate the experience of a child using an EdTech website in their country, and how their data might be collected, handled, and sent to third parties, Human Rights Watch conducted all technical tests while running a VPN set to the country where the product was endorsed by the government for children’s education. This proved essential: early tests conducted by Human Rights Watch found that the prevalence of surveillance technologies embedded in a website changed depending on the country the website believed that its user was located. Many of the observed differences appeared to be related to that country’s data protection laws, where they exist.

---

Human Rights Watch selected for examination websites that were explicitly recommended by governments for use for children’s online education. In response to Human Rights Watch’s findings, some companies noted that their government-recommended products were designed for use by teachers, parents and other adults, and not for use by children. Accepting those claims as fact, this still raises the question of why the governments recommended pages for use by children that were not adequately vetted to protect their privacy, as well as the question of whether the companies should have changed their privacy practices on those pages once the government made its recommendation.

Technical Limitations

Analyzing apps using static analysis may yield false positives, as not all of the app’s source code might be implemented in practice when a user runs the app. Put another way, an app may not use all of the programmed functionalities of which it is capable. Human Rights Watch notes this limitation by distinguishing between analysis of the code’s capabilities (static analysis) and detections of actual transmission of children’s data (dynamic analysis) throughout the report.

A technical analysis does not definitively determine the intent of any particular tracking technology, or how the collected data is used. For example, an EdTech product can include third-party computer code that collects information that may be useful to monitor the product’s performance and stability. The same data collected by the same third-party code may also be used in tandem with other third-party code to enable data collection for advertising or other marketing purposes. In a static analysis, it is not possible to conclude whether user data were collected, or the scope or purpose of the data collection. Neither is it possible solely with a technical analysis to determine how the collected data is used by the third party.

As another example, third-party computer code embedded in a product to perform an administrative function can be designed also to enable access to a device’s camera, microphone, or another feature. In a static analysis, it is possible to detect the capability, but not whether the capability is utilized. In addition, the EdTech company implementing such third-party code for an administrative function may not have plans to enable those features, and may not be aware of the possibility. Note also that access by any code to an Android device’s camera or microphone is possible only if the user settings on the device enable such sharing.

Where possible, Human Rights Watch worked to reduce ambiguity by examining the parent companies that own the tracking technologies found in an EdTech product, as well as the companies found to receive transmissions of children’s data. Human Rights Watch conducted further analysis on companies that receive, analyze, trade, or sell people’s personal data for commercial and other purposes, and reviewed their publicly available marketing materials and developer documentation.

Blacklight’s analysis is limited by three other factors: the simulation may trigger different surveillance responses from the website under examination, because it is a simulation of user behavior, not actual user behavior; the possibility of producing false positives while scanning for canvas fingerprinting; the possibility of producing false negatives through a stack tracing technique. Further investigation by The Markup determined that the probability of these false errors occurring is very low, and that Human Rights Watch’s methodology design may have further reduced this risk.\textsuperscript{11} A detailed discussion of these technical limitations can be found on Blacklight’s methodology, available online.\textsuperscript{12}

\textsuperscript{11} According to The Markup, false positives with canvas fingerprinting occur “very occasionally” when Blacklight is run in the cloud, because it is difficult to distinguish the tool from any other bot. As Human Rights Watch conducted its technical tests by running Blacklight on a local machine with a VPN, this, in theory, would have further reduced the risk of false positives. Furthermore, The Markup notes that the stack tracing technique did not produce false negatives in their tests or in their survey of the 100,000 most popular websites on the internet. See: Surya Mattu and Aaron Sankin, “How We Built a Real-time Privacy Inspector,” The Markup, September 22, 2020, https://themarkup.org/blacklight/2020/09/22/how-we-built-a-real-time-privacy-inspector (accessed July 7, 2021).

\textsuperscript{12} Ibid.
For readers seeking to replicate Human Rights Watch’s findings, it is important to note that the observed behavior of these apps and websites, and the detected prevalence and frequency of tracking technologies embedded in them, may fluctuate. This is influenced by multiple factors, including the geographical location of the user, date and time of testing, and the device or browser type, among other variables. In addition, apps and websites that use AdTech services to offer advertisers and other third-party companies the opportunity to target their students with ads through an electronic high-frequency trading process known as real-time bidding, further described in Chapter 1, may yield different results as to the recipient of the children’s data, as different third parties may have won the bid each time.

Human Rights Watch conducted manual analysis on four websites—Distance Learning (Cameroon), Eduyun (China), Smart Revision (Zambia), and e-learning portal (Zambia)—on which Blacklight tests failed for a variety of technical failures. One site was incompatible with the browser used by Blacklight, and another refused to load upon detecting the VPN service used by Human Rights Watch. The manual analysis conducted on these four sites followed the same methodology used by the Blacklight tool.

Interviews with Children, Parents, and Teachers

Human Rights Watch interviewed students, parents, and teachers between April 2020 and April 2021 about their experiences with online learning. Interviewees were based in the following 17 countries: Australia, Chile, Denmark, Germany, Indonesia, India, Iran, Italy, Lebanon, Republic of Korea, Russia, Serbia, Spain, South Africa, Turkey, United Kingdom, and the United States.

Interviewees lived in capital cities, other cities, Indigenous communities, rural and remote locations, suburbs, towns, and villages.

Interviews were conducted directly, or with interpretation, in Arabic, Bahasa Indonesian, Danish, English, Ewe, Farsi, German, Hindi, Italian, Korean, Russian, Serbian, Spanish, and Turkish.

Interviewees were not paid to participate. Interviewees were informed of the purpose of the interview, its voluntary nature, and the ways in which the information would be used. They provided oral and written consent to be interviewed.

Many parents and teachers requested that their names not be used in this report to protect their privacy or the privacy of their children or students, or to feel free to speak about their school, or for cultural reasons. Children’s identities are protected with pseudonyms of their own choosing. Pseudonyms are reflected in the text with a first name followed by an initial and are noted in the footnotes.

Requests for Comment

Human Rights Watch shared the findings presented in this report with 95 EdTech companies, 199 AdTech companies, and the 49 governments covered in this report, and gave them the opportunity to respond and provide comments and clarifications. Of these, 48 EdTech companies, 78 AdTech companies, and 10 governments responded as of May 24, 2022 at 12:00pm EDT.
I. Covid-19, Education, and Technology

There were no doubts that the online platforms and tools used could be unsafe. It was never questioned.

— A single mother of two school-aged boys, Izhevsk, Udmurt Republic, Russia

Covid-19 and Children’s Education

The novel coronavirus has devastated children’s education around the world. On March 11, 2020, the World Health Organization (WHO) declared that an outbreak of Covid-19 had reached global pandemic levels. Within weeks, almost every country in the world closed down their schools in an attempt to stop the spread of Covid-19, upending the lives and learning of 1.6 billion children and young adults, or 90 percent of the world’s students. By March 2021, a full year into the pandemic, half of the global student population remained shut out of school.

Most countries pivoted to some form of online learning, replacing physical classrooms with phones, tablets, and computers. This deepened existing inequities in children’s access to education, in the form of digital divides between children with access to technologies critical for online learning, and those without. It also created a dependence and need for affordable, reliable connectivity and devices so overwhelming that it triggered global shortages for both. Supply chains for computers buckled under staggering demand, as shortages of essential parts created two-year shipment delays.


As more people became heavily reliant on the internet to work, communicate, play, and study during Covid-19 lockdowns, the resulting explosion of traffic clogged the internet and dumped unprecedented stress on its infrastructure. Nine days after the WHO’s pandemic declaration, the European Commission took the extraordinary step of asking internet companies, video streaming services, and gaming platforms to reduce their services in Europe to reserve bandwidth for work and education.\textsuperscript{19}

Teachers and schools faced a bewildering array of digital platforms to choose from as they scrambled to set up virtual classrooms. In response, governments issued endorsements of educational technologies (EdTech) for use. Some governments rapidly signed contracts with EdTech companies to purchase millions of licenses for teachers and students.\textsuperscript{20}

As a result, EdTech companies experienced explosive, unprecedented demand for their products. In the days and weeks after the WHO’s pandemic declaration, education app downloads worldwide surged 90 percent compared to the weekly average at the end of 2019.\textsuperscript{19} Children spent significantly more time online in virtual classrooms; by September 2020, the number of hours spent in education apps globally each week had increased to an estimated 100 million hours, up 90 percent compared to the same period in 2019.\textsuperscript{12}

Google Classroom, Google’s teacher-student communication platform, reported that the pandemic had almost quadrupled its users to more than 150 million, up from 40 million in 2019; similarly, G Suite for Education, Google’s classroom software, reported doubling its users to more than 170 million students and educators.\textsuperscript{21} “We have seen incredible growth,” Javier Soltero, a vice president at the company, said in an interview with \textit{Bloomberg}. “It actually mirrors, unfortunately, the ramp up and spread of the disease.”\textsuperscript{24}

The explosive demand also generated record revenues and profits. As the global economy plummeted, venture capital financing for EdTech startups surged to a record-setting US$16.1 billion in 2020, more than doubling the US$7 billion raised in 2019.\textsuperscript{19} Two companies, Byju’s and Yuanfudao, became the first EdTech companies to achieve “decacorn” status—an exclusive group of the world’s most valuable privately-held

worldwide and pitted desperate schools and education ministries against one another.\textsuperscript{16}
companies, valued at more than $10 billion—after attracting millions of new students and closing successful financing rounds during the pandemic.²⁶

Technology companies that provided free services to schools also benefited, gaining significant market share as millions of students became familiar with their product. Zoom Video Communications, which provided free services to more than 125,000 schools in 25 countries, as well as limited free services for the general public, reported its sales skyrocketing 326 percent to $2.7 billion and its profits propelled from $21.7 million in 2019 to $671.5 million in 2020.²⁷

The use of EdTech helped governments to fill urgent gaps and deliver some measure of learning during the pandemic. However, governments’ endorsements and procurements of EdTech also turbocharged the mass collection of children’s data, exposing their personal information to the risk of misuse and exploitation by the advertising-driven internet economy and resulting in the mass surveillance of children’s lives, both inside and outside of the classroom.

How the Internet-Based Economy Works

We don’t monetize the things we create.
We monetize users.

—Andy Rubin, creator of Android, the world’s most widely used mobile operating system²⁸

Today’s internet is powered by the advertising technology (AdTech) industry. Motivated by the belief that personalized ads are more persuasive and therefore more lucrative, AdTech companies collect massive troves of data about people to target them with ads tailored to their presumed interests and desires. The revenue generated by digital advertising pays for most of the services available on the internet today.


Most internet companies offer their website, app, or content for free, or charge a negligible fee that does not reflect the full cost of offering these services. Instead of asking people to pay for these services with money, companies require people to give up their data and attention, often without their knowledge or meaningful consent. Companies then traffic their users’ data into a complex ecosystem of AdTech companies, data brokers, and others in a set of highly profitable transactions that make up a $378.16 billion industry.

Here’s how a child using an EdTech app to attend her school online might interact with the AdTech industry. This illustration similarly describes a child’s experience using an EdTech website to attend her school online.

1. EdTech companies that make educational apps for children decide to send a child’s personal data to third-party companies and possibly to sell ads in their apps, in order to generate revenue.

2. AdTech companies help put ads in apps. They make packages of code, such as software development kits (SDKs) and other tracking technologies, for app makers to insert into their apps to personalize and display ads to their users. When this code is installed in the app, this code collects data that may be used by the AdTech company to target advertising, whether on the EdTech product or on another site or app.

3. A child opens the EdTech app that their school uses for online learning and logs in for class.

4. Instantly, the app begins to collect personal data about the child. This can include who the child is, where she is, what she does, who she interacts with in her virtual classroom, and what kind of device her parents can afford for her to use.

5. This data can be sent to AdTech companies, either by the EdTech app, or directly by the AdTech SDKs embedded in the app. In the process, AdTech companies assign an ID number to the child, so that they can piece together the data they receive to build a profile on her.

6. Some AdTech companies will also follow the child across the internet and over time. Some may search for even more information about her from public and private sources, adding definition and detail to an intimate profile of the child.

7. AdTech companies’ sophisticated algorithms analyze the trove of data received from the app. They guess at the child’s personal characteristics and interests (for example, that she’s likely to be female), and predict her future behavior (this child is likely to buy a toy).

8. AdTech companies use these insights to sell to advertisers the ability to target ads to people. This happens through real-time bidding platforms, where algorithms engage in a high-frequency auction amongst advertisers to sell off the chance to show an ad to a user—in this case, a child—to the highest bidder. From start to finish, the automated process of buying and selling between advertisers takes less than a hundred milliseconds and takes place tens of billions of times each day.

---


These insights can also be sold or shared with data brokers, law enforcement and governments, or others who wish to target a defined group of people with similar characteristics online.

A handful of the world’s most valuable internet companies own entire AdTech supply chains. Alibaba, Amazon, Facebook (Meta), Google, Microsoft, Tencent, and Yandex offer digital services that serve as the primary channels that most of the world relies on to engage with the internet. In turn, they collect extensive data about the billions of people who use or interact with these platforms. They analyze this data to infer and create new information about people, then commercialize those insights for advertising—often on their own real-time bidding platforms.

These AdTech companies may also draw upon their vast troves of data to build and offer finely-tuned tracking technologies, prediction models, and microtargeting tools to help advertisers reach their audiences. As further described in Chapter 3, these tools are embedded in most websites and apps that people use every day, enabling these AdTech companies to collect and receive data not just from people directly using their services, but from anyone who encounters their data tracking embedded across the internet. The unparalleled power of these dominant tech companies to collect, track, and combine data across much of the internet results in a powerful and pervasive surveillance of people’s lives that is extremely difficult to avoid.34

---

32 Facebook rebranded itself to Meta in October 2021. This report refers to Facebook as both the platform and the parent company, for consistency across the timeline of this investigation.


II. Hidden Surveillance: Children’s Data Harvested

How dare they? How dare [these companies] peep into my private life?

—Rodin R., 9-year-old student, Istanbul, Turkey

Children’s Data and their Right to Privacy

Privacy is a human right. Recognized under international and regional human rights treaties, this right encompasses three connected components: the freedom from intrusion into our private lives, the right to control information about ourselves, and the right to a space in which we can freely express our identities.

Privacy is about autonomy and control over one’s life. It is the ability to define for ourselves who we are to the world, on our own terms. This is especially important for children, who are entitled to special protections that guard their privacy and the space for them to grow, play, and learn.

35 Human Rights Watch interview with Rodin R., 9, Istanbul, Turkey, June 25, 2021. The names of all children quoted in this report have been changed to protect their privacy.


38 In his 2021 report to the UN Human Rights Council, the Special Rapporteur on the right to privacy stated that children’s right to privacy “enables their access to their other rights critical to developing personality and personhood, such as the rights to freedom of expression and of association and the right to health, among others.” See: 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, January 25, 2021, paras. 67-76.
Children’s privacy is vital to ensuring their safety, agency, and dignity. At school, privacy enables the very purpose of education by providing the space for children to develop their personalities and abilities to their fullest potential. For children who are survivors of abuse, privacy might mean the freedom to live safely, without exposing where they live, play, and go to school. For lesbian, gay, bisexual and transgender (LGBT) children, privacy could mean the difference between seeking life-saving information and being sent to jail, or worse.

As children spend increasing amounts of their lives online, international human rights bodies have recognized that even the mere generation, collection, and processing of a child’s personal data can threaten their privacy, because in the process they lose control over information that could put their privacy at risk. Data about children’s identities, activities, communications, emotions, health, and relationships merit special consideration, as the handling of such data may result in arbitrary or unlawful abuses of children’s privacy and in harms that may continue to affect them later in life.

The United Nations Committee on the Rights of the Child has emphasized that any digital surveillance of children, together with any associated automated processing of their data, should not be conducted routinely, indiscriminately, or without the child’s knowledge or, in the case of very young children, that of their parent or caregiver. Moreover, it should not take place “without the right to object to such surveillance, in commercial settings and educational and care settings,” and “consideration should always be given to the least privacy-intrusive means available to fulfill the desired purpose.” Any restriction upon a child’s privacy is only permissible if it meets the standards of legality, necessity, and proportionality.

The unprecedented, mass use of education technologies (EdTech) by schools during the pandemic without adequate privacy protections drastically compromised children’s right to privacy. Recognizing this, the UN special rapporteur on the right to privacy warned that, “Schools and educational processes need not and should not undermine the enjoyment of privacy and other rights, wherever or however education occurs.”


44 Ibid., para. 75.

46 Ibid.


As described below, many EdTech products endorsed by governments and used by children to continue learning during Covid-19 school closures were found to harvest children’s data unnecessarily and disproportionately, for purposes unrelated to their education. Worse still, this data collection took place in virtual classrooms and educational settings online, without giving children the ability to object to such surveillance. In most instances, it was impossible for children to opt out of such data collection without opting out of compulsory schooling and giving up on learning altogether during the pandemic.

Finding Out Who Children Are

To figure out who people are on the internet, advertising technology (AdTech) companies tag each person with a string of numbers and letters that acts as an identifier number that is persistent and unique: it points to a single child or their device, and it does not change.

While the tools described in this discussion are ascribed to AdTech companies, the same tools can be used by other companies, including EdTech companies, to collect data about how their users (including children) use the product. Information about how a user or customer interacts with the product is useful, for example, for the company to improve its product and user experience. In our discussion in this section, we focus our discussion to AdTech companies to simplify the discussion, but the same concepts apply to technology companies that are not in AdTech.

Persistent identifiers enable AdTech companies to infer the interests and characteristics of individual children. Every time a child connects to the internet and comes into contact with tracking technology, any information collected about that child—where they live, who their friends are, what kind of device their family can afford for them—is tied back to the identifier associated with them by that AdTech 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.

In addition, computers can correctly re-identify virtually any person from an anonymized dataset, using just a few random pieces of anonymous information. Given the risks of re-identification, many existing data protection laws recognize persistent identifiers as personal information, granting them the same considerations and legal protections.

Some persistent identifiers are built solely to be used for advertising. Other identifiers identify and track people across multiple devices, across the internet, or trail them from the online world into the physical world. And some identifiers are so inescapably tenacious that they are impossible to avoid or get rid of, without throwing one’s device away in the trash.
II. HIDDEN SURVEILLANCE: CHILDREN’S DATA HARVESTED

Apps: Persistent Identifiers

Advertising Identifiers

Of the 73 EdTech apps examined by Human Rights Watch, 41 apps (56 percent) were found with the ability to collect their users’ advertising IDs. This allowed these apps to tag children and identify their devices for the sole purpose of advertising to them.

An advertising ID is a persistent identifier that exists for a single use: to enable advertisers to track a person, over time and across different apps installed on their device, for advertising purposes. For those using an Android device, this is called the Android Advertising ID (AAID). An AAID is neither necessary nor relevant for an app to function; Google’s developer guidelines stipulate that app developers must “only use an Advertising ID for user profiling or ads use cases.”

The 41 apps that were found to have the capability to collect AAID were endorsed by 29 governments for children’s learning during Covid-19. Altogether, these apps may identify, tag, and track an estimated 6.24 billion users, including children.

Of these, 33 apps appear to have the ability to collect AAID from an estimated 86.9 million children, because their own materials describe and appear to market them for children’s education, with children apparently intended as their primary users.

### App Country Apparently designed for use by children? Developer Estimated Users

<table>
<thead>
<tr>
<th>App</th>
<th>Country</th>
<th></th>
<th>Developer</th>
<th>Estimated Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minecraft: Education Edition</td>
<td>Australia: Victoria</td>
<td>Yes</td>
<td>Private</td>
<td>500,000</td>
</tr>
<tr>
<td>Cisco Webex</td>
<td>Australia: Victoria, Japan, Poland, Spain, Republic of Korea, Taiwan, United States: California</td>
<td>No</td>
<td>Private</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Descomplica</td>
<td>Brazil: São Paulo</td>
<td>Yes</td>
<td>Private</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Stoodi</td>
<td>Brazil: São Paulo</td>
<td>Yes</td>
<td>Private</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Storyline Online</td>
<td>Canada: Quebec</td>
<td>Yes</td>
<td>Private</td>
<td>50,000</td>
</tr>
<tr>
<td>Remind</td>
<td>Colombia</td>
<td>Yes</td>
<td>Private</td>
<td>10,000,000</td>
</tr>
<tr>
<td>Dropbox</td>
<td>Colombia</td>
<td>No</td>
<td>Private</td>
<td>1,000,000,000</td>
</tr>
<tr>
<td>Edmodo</td>
<td>Colombia, Egypt, Ghana, Nigeria, Romania, Thailand</td>
<td>Yes</td>
<td>Private</td>
<td>10,000,000</td>
</tr>
<tr>
<td>Padlet</td>
<td>Colombia, Germany: Bavaria, Romania</td>
<td>No</td>
<td>Private</td>
<td>5,000,000</td>
</tr>
<tr>
<td>SchoolFox</td>
<td>Germany: Bavaria</td>
<td>Yes</td>
<td>Private</td>
<td>100,000</td>
</tr>
<tr>
<td>itslearning</td>
<td>Germany: Bavaria</td>
<td>Yes</td>
<td>Private</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Ghana Library App</td>
<td>Ghana</td>
<td>No</td>
<td>Government</td>
<td>10,000</td>
</tr>
</tbody>
</table>

---


54 As verified by Google Play Store user installs globally, as of October 2021.
<table>
<thead>
<tr>
<th>Application</th>
<th>Country/Region</th>
<th>Ownership</th>
<th>Type</th>
<th>Downloads</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diksha</td>
<td>India: Maharashtra, National, Uttar Pradesh</td>
<td>Yes</td>
<td>Government</td>
<td>10,000,000</td>
</tr>
<tr>
<td>e-Pathshala</td>
<td>India: Maharashtra, National, Uttar Pradesh</td>
<td>Yes</td>
<td>Government</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Rumah Belajar</td>
<td>Indonesia</td>
<td>Yes</td>
<td>Government</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Quipper</td>
<td>Indonesia</td>
<td>Yes</td>
<td>Private</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Ruangguru</td>
<td>Indonesia</td>
<td>Yes</td>
<td>Private</td>
<td>10,000,000</td>
</tr>
<tr>
<td>Kelas Pintar</td>
<td>Indonesia</td>
<td>Yes</td>
<td>Private</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Shad</td>
<td>Iran</td>
<td>Yes</td>
<td>Government</td>
<td>18,000,000</td>
</tr>
<tr>
<td>Newton</td>
<td>Iraq</td>
<td>Yes</td>
<td>Government</td>
<td>50,000</td>
</tr>
<tr>
<td>WeSchool</td>
<td>Italy</td>
<td>Yes</td>
<td>Private</td>
<td>1,000,000</td>
</tr>
<tr>
<td>schoolTakt</td>
<td>Japan</td>
<td>Yes</td>
<td>Private</td>
<td>1,000</td>
</tr>
<tr>
<td>Study Sapuri</td>
<td>Japan</td>
<td>Yes</td>
<td>Private</td>
<td>500,000</td>
</tr>
<tr>
<td>Blimland</td>
<td>Kazakhstan</td>
<td>Yes</td>
<td>Private</td>
<td>500,000</td>
</tr>
<tr>
<td>Daryn Online</td>
<td>Kazakhstan</td>
<td>Yes</td>
<td>Private</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Kundelik</td>
<td>Kazakhstan</td>
<td>Yes</td>
<td>Private</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Muse</td>
<td>Pakistan</td>
<td>Yes</td>
<td>Private</td>
<td>10,000</td>
</tr>
<tr>
<td>Taleemabad</td>
<td>Pakistan</td>
<td>Yes</td>
<td>Private</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Naver Band</td>
<td>Republic of Korea</td>
<td>No</td>
<td>Private</td>
<td>50,000,000</td>
</tr>
<tr>
<td>KakaoTalk</td>
<td>Republic of Korea</td>
<td>No</td>
<td>Private</td>
<td>100,000,000</td>
</tr>
<tr>
<td>Miro</td>
<td>Romania</td>
<td>No</td>
<td>Private</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Kinderpedia</td>
<td>Romania</td>
<td>Yes</td>
<td>Private</td>
<td>10,000</td>
</tr>
<tr>
<td>My Achievements</td>
<td>Russian Federation</td>
<td>Yes</td>
<td>Government</td>
<td>100</td>
</tr>
<tr>
<td>iEN</td>
<td>Saudi Arabia</td>
<td>Yes</td>
<td>Government</td>
<td>500,000</td>
</tr>
<tr>
<td>Extramarks</td>
<td>South Africa</td>
<td>Yes</td>
<td>Private</td>
<td>100,000</td>
</tr>
<tr>
<td>Nenasa</td>
<td>Sri Lanka</td>
<td>Yes</td>
<td>Government</td>
<td>50,000</td>
</tr>
<tr>
<td>PaGamO</td>
<td>Taiwan</td>
<td>Yes</td>
<td>Private</td>
<td>100,000</td>
</tr>
<tr>
<td>Facebook</td>
<td>Taiwan</td>
<td>No</td>
<td>Private</td>
<td>5,000,000,000</td>
</tr>
<tr>
<td>Eğitim Bilişim Ağı</td>
<td>Turkey</td>
<td>Yes</td>
<td>Government</td>
<td>10,000,000</td>
</tr>
<tr>
<td>Özelim Eğitimdeyim</td>
<td>Turkey</td>
<td>Yes</td>
<td>Government</td>
<td>500,000</td>
</tr>
<tr>
<td>Schoology</td>
<td>US: Texas</td>
<td>Yes</td>
<td>Private</td>
<td>5,000,000</td>
</tr>
</tbody>
</table>

---

None of these apps allowed their users to decline to be tracked. In fact, this data collection is invisible to the child, who simply sees the app’s interface on their device. This activity is even more covert in 27 apps that fail to inform their students—either through their privacy policy, or elsewhere on their product—that the app and its embedded third-party AdTech trackers may collect their device’s AAIDs in order to track, profile, and target students with advertising. In doing so, these apps deny children, parents, and teachers knowledge of this practice and the ability to consent, and impede their right to effective remedy (as discussed in Chapter 4).  

Collectively, these EdTech apps may have provided 33 AdTech companies with access to their students’ AAIDs. This was done through software development kits (SDKs), or packages of code embedded in an EdTech app that can be used to facilitate the transmission of users’ personal data to advertisers.

When reached for comment, Cisco stated that Webex does not collect users’ AAIDs, and that it does not share user data with third-party companies that own the SDKs embedded in Webex.

Notably, nine governments—Ghana, India, Indonesia, Iran, Iraq, Russia, Saudi Arabia, Sri Lanka, and Turkey—directly built and offered eleven learning apps that may collect AAID from children. In doing so, these governments granted themselves the ability to track an estimated 41.1 million students and teachers purely for advertising and monetization. Some governments disclosed in their app’s privacy policy that the app collects students’ AAID for commercial purposes. Rumah Belajar, for example, is an EdTech website and app developed and operated by Indonesia’s Ministry of Education and Culture to provide online education to preschool, primary, and secondary school students during the pandemic. Through Rumah Belajar’s privacy policy, the Indonesian government discloses that it automatically collects children’s “unique device identifiers” and “mobile device unique ID,” which may be used to “show advertisements to you,” “to advertise on third party websites to you after you visited our service,” and shared with third party “business partners” so that they can “offer you certain products, services or promotions.”

Through dynamic analysis commissioned by Human Rights Watch and conducted by the Defensive Lab Agency, Human Rights Watch detected students’ AAID sent from Rumah Belajar to Google and to Facebook. Specifically, children’s AAID were sent to the Google-owned domain app-measurement.com, and to the Facebook-owned domain graph.facebook.com.

Indonesia does not have a data protection law, or specific regulations that protect children’s data privacy. A draft data protection bill, introduced in January 2020 and pending further discussion in the House of Representatives as of September 2021, does not provide dedicated protections for children.

In contrast, Eğitim Bilişim Ağı, developed by Turkey’s Ministry of National Education for preschool, primary, and secondary school students to continue learning during Covid-19 school closures, does not provide a privacy policy at all. Nor does the app provide a disclosure elsewhere on the product to notify students that their AAID is collected and sent to third-party companies for advertising purposes. Through dynamic analysis, Human Rights Watch detected students’ AAID transmitted from Eğitim Bilişim Ağı to Google via the Google-owned domains www.googleleadservices.com and app-measurement.com. www.googleleadservices.com is operated by Google Ads, the company’s online advertising platform. Google Ads uses the information it collects to...
understand a person’s interests and auctions off to the highest bidder the chance to show
an ad to those in the advertiser’s target audience.\footnote{See, for example, Google Ads,
en_us/home/campaigns/display-ads/ (accessed August 25, 2021); Google Ads,
campaigns/discovery-ads/ (accessed August 25, 2021).}

Neither Indonesia’s Ministry of Education and Culture nor Turkey’s Ministry of National
Education responded to Human Rights Watch’s requests for comment. Cisco informed
Human Rights Watch that Webex does not collect AAIDs.

The collection of AAID from children is neither necessary nor proportionate to the purpose
of providing them with education, and risks exposing children to rights abuses as discussed
in Chapter 3.

Inescapable Surveillance

Human Rights Watch found 14 EdTech apps with access to either the Wi-Fi Media Access
Control (MAC) address or the International Mobile Equipment Identity (IMEI) on children’s
devices, two persistent identifiers that are so strong that a child or their parent cannot avoid
or protect against their surveillance even if they take the extraordinary step of wiping their
phones or performing a factory reset.

Eight apps granted themselves the ability to collect the Wi-Fi MAC address of a device’s
networking hardware. Located in any device that can connect to the internet, this identifier
is extremely persistent and cannot be changed by wiping the device clean with a factory
reset. Any instance of an app collecting the Wi-Fi MAC address is notable; in 2015, Google
banned developers from accessing the Wi-Fi MAC address over privacy concerns that it
was being used by third-party tracking companies as a persistent identifier that could not
realistically be changed by users.\footnote{In research commissioned by the Australian Competition and Consumer
Commission, security researchers from AppCensus noted security vulnerabilities in
Android that, when exploited, allow apps to collect the Wi-Fi MAC by circumventing the permission systems’
protections. See: AppCensus, “1,000 Mobile Apps in Australia: A Report for the ACCC,” September 24, 2020,

Recommended by 13 governments, these apps had the ability to collect the Wi-Fi MAC
addresses of an estimated 15.6 billion users. Three of these apps appear to have the ability
to do so from an estimated 610,000 children, as their own materials describe and appear to
market them for children’s education.

\begin{table}
\centering
\begin{tabular}{|l|l|l|l|}
\hline
App & Country & Apparently designed for use by children? & Estimated Users\footnote{As verified by Google Play Store user installs, as of October 2021.} \\
\hline
Minecraft: Education Edition & Australia: Victoria & Yes & 500,000 \\
\hline
YouTube & India: Uttar Pradesh, Malaysia, Nigeria, United Kingdom: England & No & 10,000,000,000 \\
\hline
Padlet & Colombia, Germany: Bavaria, Romania & No & 5,000,000 \\
\hline
LINE & Japan, Taiwan & No & 500,000,000 \\
\hline
Muse & Pakistan & Yes & 10,000 \\
\hline
KakaoTalk & Republic of Korea & No & 100,000,000 \\
\hline
Extramarks & South Africa & Yes & 100,000 \\
\hline
Facebook & Taiwan & No & 5,000,000,000 \\
\hline
\end{tabular}
\end{table}
Eight apps were found with the ability to collect International Mobile Equipment Identity (IMEI) numbers. Used to connect to cellular networks and to trace stolen phones, every mobile device has an IMEI number baked into its hardware. An IMEI cannot be changed, and it is illegal to do so in some countries. The only means of changing one’s IMEI is to throw the phone away and purchase a new one.

Recommended for children’s learning by 12 governments, these apps may have collected in the aggregate IMEI numbers from an estimated 5.6 billion users. Four of these apps are apparently designed exclusively for children, so they may collect IMEI numbers from an estimated 3.1 million children in Brazil, Indonesia, Pakistan, and South Africa.

<table>
<thead>
<tr>
<th>App</th>
<th>Country</th>
<th>Apparently designed for use by children?</th>
<th>Developer</th>
<th>Estimated Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stoodi</td>
<td>Brazil: São Paulo</td>
<td>Yes</td>
<td>Private</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Kelas Pintar</td>
<td>Indonesia</td>
<td>Yes</td>
<td>Private</td>
<td>1,000,000</td>
</tr>
<tr>
<td>LINE</td>
<td>Japan, Taiwan</td>
<td>No</td>
<td>Private</td>
<td>500,000,000</td>
</tr>
<tr>
<td>Taleemabad</td>
<td>Pakistan</td>
<td>Yes</td>
<td>Private</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Telegram</td>
<td>Russia</td>
<td>No</td>
<td>Private</td>
<td>1,000,000,000</td>
</tr>
<tr>
<td>KakaoTalk</td>
<td>Republic of Korea</td>
<td>No</td>
<td>Private</td>
<td>100,000,000</td>
</tr>
<tr>
<td>Extramarks</td>
<td>South Africa</td>
<td>Yes</td>
<td>Private</td>
<td>100,000</td>
</tr>
<tr>
<td>Facebook</td>
<td>Taiwan</td>
<td>No</td>
<td>Private</td>
<td>5,000,000,000</td>
</tr>
</tbody>
</table>

Human Rights Watch found nine apps potentially engaging in ID bridging. When the AAID is collected and bundled alongside another persistent device identifier, the resulting “bridge” between the two is so powerful that it bypasses any privacy controls that the user may have set on their device to protect themselves. This allows companies to track users with an AAID that can never be reset, in effect creating an accurate advertising profile of a user that lasts in perpetuity.

Given the risks that ID bridging poses to users’ privacy, Google’s own policies warn developers that the “advertising identifier may not be connected to persistent device identifiers (for example: SSAID, MAC address, IMEI, etc.) for any advertising purpose.”

<table>
<thead>
<tr>
<th>App</th>
<th>Country</th>
<th>Apparentley designed for use by children?</th>
<th>Potential ID bridging</th>
<th>Developer</th>
<th>Estimated Users</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


66 As verified by Google Play Store user installs globally, as of October 2021.


Minecraft: Education Edition
Australia: Victoria Yes Wi-Fi MAC Private 500,000

Stoodi Brazil: São Paulo Yes IMEI Private 1,000,000

Padlet Germany: Bavaria, Romania, Colombia Yes Wi-Fi MAC Private 1,000,000

Kelas Pintar Indonesia Yes IMEI Private 1,000,000

Muse Pakistan Yes Wi-Fi MAC Private 10,000

Taleemabad Pakistan Yes IMEI Private 500,000

KakaoTalk Republic of Korea No Wi-Fi MAC, IMEI Private 100,000,000

Extramarks South Africa Yes Wi-Fi MAC, IMEI Private 100,000

Facebook Taiwan No Wi-Fi MAC, IMEI Private 5,000,000,000

Muse, for example, was conclusively found to be engaging in ID bridging. Through dynamic analysis, Human Rights Watch observed Muse collecting and transmitting bridged ID data to Facebook through the Facebook-owned domain graph.facebook.com.

Of the 14 apps discovered to grant themselves access to their users’ Wi-Fi MAC or IMEI, 10 did not disclose this in their privacy policies. None of the 10 apps found to engage in ID bridging disclosed this practice to their users.

When reached for comment, Microsoft denied that its product engages in ID bridging, and Padlet responded that it did not intend to collect the data needed for ID bridging. In their responses, Facebook (Meta) and Muse did not answer whether their products engage in ID bridging. Kakao declined to respond to our request for comment; Extramarks, Kelas Pintar, Stoodi, and Taleemabad did not respond.

These practices are not necessary for EdTech apps to function or for the purpose of providing children’s education.

Websites: Canvas Fingerprinting

Of the many tracking technologies that websites can use to identify people and their
behaviors online, one of the most invasive is canvas fingerprinting. Virtually impossible for users to block, this technique works by drawing hidden shapes and text on a user’s webpage. Because each computer draws these shapes slightly differently, these images can be used by marketers and others to assign a unique number to a user’s device, which is then used as a singular identifier to track the user’s activities across the internet.71

Users cannot protect themselves by using standard web browser privacy settings or ad-blocking software.

Of the 124 EdTech websites examined by Human Rights Watch, eight websites were found “fingerprinting” their users and tracking them across the internet.

Notably, two of these websites are directly built and operated by government—Moscow Electronic School (Russia) and Digital Lessons (Russia)—for children’s educational use. Another website, CBC Kids (Canada), receives the majority of its funding from government.72

<table>
<thead>
<tr>
<th>Website</th>
<th>Country</th>
<th>Apparently designed for use by children?</th>
<th>Developer</th>
<th>Canvas fingerprinting script loaded from:</th>
</tr>
</thead>
<tbody>
<tr>
<td>WorkFlowy</td>
<td>Colombia</td>
<td>No</td>
<td>Private</td>
<td><a href="https://workflowy.com/media/js/82cab8d2714ada91b4.js">https://workflowy.com/media/js/82cab8d2714ada91b4.js</a> <a href="https://workflowy.com/media/js/auth_embed.min.js">https://workflowy.com/media/js/auth_embed.min.js</a></td>
</tr>
<tr>
<td>Top Parent</td>
<td>India: Uttar Pradesh</td>
<td>Yes</td>
<td>Private</td>
<td><a href="https://cdnjs.cloudflare.com/ajax/libs/fingerprintjs2/2.1.0/fingerprint2.min.js">https://cdnjs.cloudflare.com/ajax/libs/fingerprintjs2/2.1.0/fingerprint2.min.js</a></td>
</tr>
<tr>
<td>WeSchool</td>
<td>Italy</td>
<td>Yes</td>
<td>Private</td>
<td><a href="https://m.stripe.network/out-4.5.35.js">https://m.stripe.network/out-4.5.35.js</a></td>
</tr>
<tr>
<td>iMektep</td>
<td>Kazakhstan</td>
<td>Yes</td>
<td>Private</td>
<td><a href="https://st.vk.com/js/cmmodules/mobile">https://st.vk.com/js/cmmodules/mobile</a></td>
</tr>
<tr>
<td>Moscow Electronic School</td>
<td>Russia</td>
<td>Yes</td>
<td>Government</td>
<td><a href="https://stats.mos.ru/ss2.min.js">https://stats.mos.ru/ss2.min.js</a></td>
</tr>
<tr>
<td>Digital Lessons</td>
<td>Russia</td>
<td>Yes</td>
<td>Government</td>
<td><a href="https://st.vk.com/js/cmmodules/mobile">https://st.vk.com/js/cmmodules/mobile</a></td>
</tr>
</tbody>
</table>

One EdTech website, Z-kai, was endorsed by the Japanese Education Ministry for all elementary, middle, and high school students to learn core subjects during Covid-19 school closures.73 Human Rights Watch observed Z-kai fingerprinting children in Japan by secretly drawing this image on their web browsers:


Human Rights Watch observed Z-kai fingerprinting children in Japan by secretly drawing this image on their web browsers. © 2022 Hye Jung Han/Human Rights Watch

Two such canvas fingerprinting scripts were built and loaded on the Z-kai site by spider.af, a Japanese company that specializes in ensuring that advertisers’ intended audiences see their ads. Z-kai and spider.af did not respond to our request for comment.

It is not possible to determine the intent behind the use of canvas fingerprinting and how it is used by the product it is embedded in. However, none of these eight websites disclosed their use of canvas fingerprinting to their users. In doing so, these companies effectively kept their users in the dark that they were being invisibly identified and followed around the internet by tracking technology that is difficult to avoid or protect against.

This technique is neither proportionate nor necessary for these websites to function or deliver educational content to children. Its use on children in an educational setting infringes upon children’s right to privacy.

Tracking Where Children Are

Just thinking about my whole age group, the amount of data they share is not even funny. Our everyday lives, our locations. So, their whole lives must be in danger if their data is getting sold off. It’s really scary.

—Priyanka S., 16, Uttar Pradesh, India

To know where a child is, and when, is to possess information so sensitive that some governments provide special protections against its misuse and the risks of “abduction, physical and mental abuse, sexual abuse and trafficking.”


Information about a child’s physical location also reveals powerfully intimate details about their life far beyond their coordinates. Mobile phones have the ability to find and track a child’s precise physical location over time, including when and how long they were in any given place. Once collected, these data points can reveal such sensitive information as where a child lives and where they go to school, trips between divorced parents’ homes, and visits to a doctor’s office specializing in childhood cancer.

Even without names or other obviously identifiable information attached to location data, it is startlingly easy to identify real children and people without their awareness or consent. A New York Times investigation determined that just two precise location data points is enough to identify a person; journalists were, for example, able to identify a single child and where they live by tracing their daily route from home to school, as well as a middle-school math teacher by her classroom and her doctor’s office.77

At a time when many children were remotely learning from home under Covid-19 lockdowns, the surveillance of their physical presence through location data likely revealed addresses and places most significant to them.

Apps: Precise Location Data

Of the 73 apps examined by Human Rights Watch, 21 apps (29 percent) granted themselves the ability to collect precise location data, or GPS coordinates that can identify a child’s exact location to within 4.9 meters.78 These 21 apps also had the ability to collect the time of the device’s current location, as well as the last known location of the device—revealing exactly where a child is, where they were before that, and how long they stayed at each place.

Of these, 10 apps appear to have the ability to collect precise location data from an estimated 52.1 million children, as these apps’ own materials describe and appear to market them for children’s use in education. None of these apps apparently designed for use by children disclose to their students that they collect their precise location data.

Four apps are built and owned by the education ministries of India, Indonesia, Iran, and Turkey, giving these governments the ability to track an estimated 29.5 million children and pinpoint where they are, at any given moment, until the app is closed by the user.


### EdTech Product

<table>
<thead>
<tr>
<th>EdTech Product</th>
<th>Country</th>
<th>Apparently designed for use by children?</th>
<th>Developer GPS</th>
<th>Timestamp of current location</th>
<th>Last known location</th>
<th>Disclosed in privacy policy</th>
<th>Estimated Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Teams</td>
<td>Australia: New South Wales, Germany: Bavaria, Republic of Korea, Spain, Taiwan, United Kingdom: England, US: Texas</td>
<td>No</td>
<td>Private</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Zoom</td>
<td>Australia: New South Wales, Cameroon, Kazakhstan, Republic of Korea, Romania, US: California, Texas, United Kingdom: England</td>
<td>No</td>
<td>Private</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Cisco Webex</td>
<td>Australia: Victoria, Japan, Poland, Spain, Republic of Korea, Taiwan, US: California</td>
<td>No</td>
<td>Private</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Threema Work</td>
<td>Germany: Baden-Württemberg, Germany: Bavaria</td>
<td>No</td>
<td>Private</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Moodle</td>
<td>Germany: Baden-Württemberg, Romania, Kazakhstan</td>
<td>Yes</td>
<td>Private</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Padlet</td>
<td>Germany: Bavaria, Romania, Colombia</td>
<td>No</td>
<td>Private</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>YouTube</td>
<td>India: Uttar Pradesh, Malaysia, Nigeria, United Kingdom: England</td>
<td>No</td>
<td>Private</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Diksha</td>
<td>India: National</td>
<td>Yes</td>
<td>Government</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

79 As verified by Google Play Store user installs globally, as of October 2021.
II. HIDDEN SURVEILLANCE: CHILDREN’S DATA HARVESTED

Altogether, these apps include code that can enable 15 third-party companies to access children’s precise location data, potentially enabling these companies to analyze, trade, and monetize this information.

Of these 21 apps, 19 apps include code that can enable the collection of coarse location data, which reveals where children are with an accuracy approximately equivalent to a city block. Such data can also be used to infer intimate details about a child; research scientists have concluded that just four approximate, anonymous location data points is enough to re-identify 95 percent of individuals.

Human Rights Watch did not find evidence that precise location data was used to provide core app functionality or any educational benefit to children for 20 of the 21 apps. When reached for comment, Microsoft stated that Microsoft Teams may collect a user’s precise location data for many purposes, including to comply with law for users located in the United States to collect and transmit their location data to first responders when a user makes an emergency call using Microsoft Teams.

When reached for comment, Cisco stated that Webex does not collect users’ precise location, last known location or coarse location, or their call logs.

---


**Case Study: Diksha, India**

Diksha is an EdTech app owned and operated by India’s Education Ministry. First launched in 2017 and later used during the pandemic as the government’s primary means of delivering online education to students, Diksha offers lessons, textbooks, homework, and other educational material for grades 1 to 12. Diksha was downloaded by over 10 million students and teachers as of 2020. To drive further adoption, some state education ministries set quotas for government teachers to compel a minimum number of their students to download the app.1

Human Rights Watch found that Diksha collects children’s precise location data, including the date and time of their current location and their last known location. However, the Indian government does not disclose through Diksha’s privacy policy or elsewhere that it collects children’s location data. Instead, it misleadingly states that Diksha collects a different piece of information—a user’s IP address—only once, “for the limited purpose of determining your approximate location – the State, City and District of origin... and the precise location of any User cannot be determined.”

Diksha also granted access to its students’ location data to Google, through the two SDKs—Google Firebase Analytics and Google Crashlytics—embedded in the app. Through dynamic analysis, Human Rights Watch observed Diksha collecting and transmitting children’s AAID to Google. It appears that Diksha shares children’s personal data with Google for advertising purposes.

India’s Education Ministry, as well as the state education ministries of Maharashtra and Uttar Pradesh, which had endorsed the use of Diksha, did not respond to requests for comment.

As a result, children and their parents were denied the opportunity to make informed decisions about whether to permit the Indian government to surveil their location and share it with third-party companies.

**Wi-Fi SSID**

Companies can also track a child’s whereabouts by collecting information about the wireless network to which their phone is connected. Because Wi-Fi routers tend to be in fixed locations, collecting the names of wireless networks to which a child has previously connected can reveal places such as their home, school, places of worship, hospitals, addresses of extended family, and other places where a child spends significant time. Such information can then be used to infer more about a child, including their habits and relationships.

To do this, mobile phones collect the Wi-Fi SSID, which yields the name of a Wi-Fi router that the phone is connected to or the name of one nearby. Companies can look up these routers in databases that list where public Wi-Fi locations are located in the world, then map them to precise GPS coordinates.

Human Rights Watch found 18 apps accessing the Wi-Fi SSID. In seven cases, the apps’ own materials describe and appear to market them for children’s use; two of these are owned and provided by the governments of Iran and Turkey. Seven of these apps do not disclose in their privacy policy that they collect any location data from their users, much less precise location data such as the Wi-Fi SSID.
<table>
<thead>
<tr>
<th>EdTech Product</th>
<th>Country</th>
<th>Apparently designed for use by children?</th>
<th>Developer Wi-Fi SSID Disclosed in privacy policy?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Teams</td>
<td>Australia: New South Wales, Germany: Bavaria, Republic of Korea, Spain, Taiwan, United Kingdom: England, US: Texas</td>
<td>No</td>
<td>Private</td>
</tr>
<tr>
<td>Cisco Webex</td>
<td>Australia: Victoria, Japan, Poland, Spain, Republic of Korea, Taiwan, US: California</td>
<td>No</td>
<td>Private</td>
</tr>
<tr>
<td>Zoom</td>
<td>Australia: New South Wales, Cameroon, Kazakhstan, Republic of Korea, Romania, US: California, Texas, United Kingdom: England</td>
<td>No</td>
<td>Private</td>
</tr>
<tr>
<td>Threema Work</td>
<td>Germany: Baden-Württemberg, Bavaria</td>
<td>No</td>
<td>Private</td>
</tr>
<tr>
<td>Padlet</td>
<td>Germany: Bavaria, Romania, Colombia</td>
<td>Yes</td>
<td>Private</td>
</tr>
<tr>
<td>LINE</td>
<td>Japan, Taiwan</td>
<td>No</td>
<td>Private</td>
</tr>
<tr>
<td>YouTube</td>
<td>India: Uttar Pradesh, Malaysia, Nigeria, , United Kingdom: England</td>
<td>No</td>
<td>Private</td>
</tr>
<tr>
<td>WhatsApp</td>
<td>India: Uttar Pradesh, Cameroon</td>
<td>No</td>
<td>Private</td>
</tr>
<tr>
<td>Ruangguru</td>
<td>Indonesia</td>
<td>Yes</td>
<td>Private</td>
</tr>
<tr>
<td>Sekolah.mu</td>
<td>Indonesia</td>
<td>Yes</td>
<td>Private</td>
</tr>
<tr>
<td>Shad</td>
<td>Iran</td>
<td>Yes</td>
<td>Government</td>
</tr>
<tr>
<td>Telegram</td>
<td>Nigeria</td>
<td>No</td>
<td>Private</td>
</tr>
<tr>
<td>Taleemabad</td>
<td>Pakistan</td>
<td>Yes</td>
<td>Private</td>
</tr>
<tr>
<td>Naver Band</td>
<td>Republic of Korea</td>
<td>No</td>
<td>Private</td>
</tr>
<tr>
<td>KakaoTalk</td>
<td>Republic of Korea</td>
<td>No</td>
<td>Private</td>
</tr>
<tr>
<td>Extramarks</td>
<td>South Africa</td>
<td>Yes</td>
<td>Private</td>
</tr>
<tr>
<td>Facebook</td>
<td>Taiwan</td>
<td>No</td>
<td>Private</td>
</tr>
<tr>
<td>Özelim Eğitimdeyim</td>
<td>Turkey</td>
<td>Yes</td>
<td>Government</td>
</tr>
</tbody>
</table>
Websites: Coarse Location Data

Every device connected to the internet has an Internet Protocol (IP) address to send and receive data, much like a physical address is needed to send and receive physical mail. Every app or website transmits its users’ IP address in the standard course of communicating with an internet server. However, IP addresses can also be used to infer a user’s location with coarse granularity, or to identify the country, city, and postal code of the person’s location.

While it is not possible to determine from a technical assessment whether a company is using an IP address to determine a user’s approximate location, most AdTech companies that Human Rights Watch observed receiving children’s IP addresses from government-endorsed EdTech products offer geolocation targeting services based on IP addresses.

Criteo, for example, is an AdTech company that specializes in retargeting ads across the internet at people who have previously visited a given website. Decisions on who to target are made using what the company’s CEO called its “powerful flashlight” to identify people online, which is powered by the data it holds on “2.5 billion unique users globally, of which 98 percent have persistent identifiers beyond cookies.” The company claims that it has “advanced AI algorithms” which “use [...] over 120 shopping signals to create a unique ad for every user designed to get the highest engagement.”

Criteo notes that “Our partners provide us with information about your geographical location derived from your truncated IP address, points of interest that are near you (e.g. stores that are geographically close to you) ... This allows us to improve the relevance of our services by displaying advertisements for products available in your geographical area.”

Human Rights Watch observed Criteo receiving children’s data and their IP addresses from the EdTech websites Descomplica (Brazil: São Paulo), Escola Mais (Brazil: São Paulo), Study Sapuri (Japan), Z-kai (Japan), 100Ballov (Kazakhstan), Campus.pk (Pakistan), and EBS (Republic of Korea). All of these websites are designed and intended for children’s use in education.

In its response, Criteo confirmed that it specializes in behavioral advertising, and that it collects truncated IP addresses to determine a person’s location to within one km. While the company stated that it does not intentionally or knowingly collect personal information from children, it confirmed that three of these websites—Descomplica, Study Sapuri, and Z-kai—were current clients and said that it was not currently working with the other four websites. Criteo did not address whether it had received children’s data from the EdTech websites listed above.

---

91 Human Rights Watch email correspondence with Maribel Henriquez, Senior Communications Manager, Criteo, April 7, 2022.
II. HIDDEN SURVEILLANCE: CHILDREN’S DATA HARVESTED

Finding out who you know has long been considered valuable by advertisers, who recognize that one of the most effective methods of attracting new customers is through referrals made by family, friends, and contacts. The Nielsen Company, a data broker and AdTech company that Human Rights Watch detected receiving children’s data from three EdTech websites—Stoodi (Brazil: São Paulo), CBC Kids (Canada), and WeSchool (Italy)—notes that “the most credible form of advertising comes straight from the people we know and trust.”

Contact information can also be used for shadow profiling, in which companies siphon data from their users’ contacts lists in order to develop profiles on people who have never used their services. Facebook, for example, came under intense scrutiny in a series of high-profile cases for sharing the personal information of its users’ friends, without their consent or awareness, between 2010 and 2018. Among others, this enabled Cambridge Analytica, a political firm that claimed to influence people by creating uniquely detailed personality profiles and then tailoring political messaging to them, to collect information not only from the 270,000 users who consented to share their data through Cambridge Analytica’s Facebook-linked app, but also from up to 87 million unwitting people listed as their friends on Facebook.

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 privacy for both. For the contact, their 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.

Human Rights Watch identified 18 EdTech apps (25 percent) with the ability to collect information about their users’ friends, family, and other acquaintances by accessing the contacts list saved on users’ phones. This may have allowed these apps to learn personal details about these contacts, including any saved names, phone numbers, emails, addresses, and relationships (“Grandma,” “Dad”). In addition, all of these apps, with the exception of Telegram, had the ability to collect profile photos of the contact, if one had been saved.

Three apps developed specifically for children—Kelas Pintar (Indonesia), Shad (Iran), and Extramarks (South Africa)—do not disclose this practice in their privacy policies. Human Rights Watch found that this data was neither necessary for these apps to function, nor provided educational benefit to children.
These 18 apps may have granted access to their users’ contact data to 16 third-party companies.

<table>
<thead>
<tr>
<th>EdTech app</th>
<th>Country</th>
<th>Apparentlly designed for use by children?</th>
<th>Contacts’ details</th>
<th>Contacts’ photos</th>
<th>Ed Tech app may give access to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Teams</td>
<td>Australia: New South Wales, Germany: Bavaria, Republic of Korea, Spain, Taiwan, United Kingdom: England, US: Texas</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Crashes</td>
</tr>
<tr>
<td>Cisco Webex</td>
<td>Australia: Victoria, Japan, Poland, Spain, Republic of Korea, Taiwan, US: California</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Google Firebase Analytics, Google Crashlytics, Ampli-tude</td>
</tr>
<tr>
<td>Zoom</td>
<td>Australia: New South Wales, Cameroon, Kazakhstan, Republic of Korea, Romania, US: California</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Google Firebase Analytics</td>
</tr>
<tr>
<td>Remind</td>
<td>Colombia</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Google Firebase Analytics, Google Crashlytics, Braze, Pusher</td>
</tr>
<tr>
<td>Dropbox</td>
<td>Colombia</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Google Firebase Analytics, Adjust, Bugsnag</td>
</tr>
<tr>
<td>Padlet</td>
<td>Germany: Bavaria, Romania, Colombia</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Google Crashlytics, Google Firebase Analytics, Branch, Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Crashes</td>
</tr>
<tr>
<td>YouTube</td>
<td>India: Uttar Pradesh, Malaysia, Nigeria, United Kingdom: England</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Google Firebase Analytics, Google AdMob</td>
</tr>
<tr>
<td>WhatsApp</td>
<td>India: Uttar Pradesh, Cameroon</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Google Analytics</td>
</tr>
</tbody>
</table>
Kelas Pintar Indonesia Yes Yes Yes Google Crashlytics, Google Firebase Analytics, Google Analytics, Google Tag Manager, Facebook Analytics, Facebook Login, Facebook Share, Adjust

Shad Iran Yes Yes Yes Google Crashlytics, Google Firebase Analytics

LINE Japan, Taiwan No Yes Yes Google Analytics, Google AdMob, Facebook Login, Facebook Share

Telegram Nigeria No Yes No Google Firebase Analytics

Edmodo Nigeria, Egypt, Colombia, Ghana, Romania, Thailand Yes Yes Yes Google Crashlytics, Google Firebase Analytics, Google AdMob, JW Player, Matomo

Naver Band Republic of Korea No Yes Yes Google Firebase Analytics, Google AdMob, AppsFlyer, Facebook Analytics, Facebook Login, Facebook Share, InMobi, Moat

KakaoTalk Republic of Korea No Yes Yes Google Firebase Analytics, Google Crashlytics, AdFit

Extramarks South Africa Yes Yes Yes Google Analytics, Google Firebase Analytics, Google AdMob, Google Tag Manager, Adjust, Facebook Login, Facebook Places, Facebook Share

Google Meet Spain, Poland, Taiwan, US: California, Texas No Yes Yes Google Firebase Analytics

Facebook Taiwan No Yes Yes N/A

Tracking What Children Do in the Classroom

Human Rights Watch found that many governments enabled third-party companies to infringe on children’s privacy by allowing them to conduct unnecessary, disproportionate surveillance on what children do in their virtual classrooms. Using tracking technologies invisible to their users, many EdTech companies examined in this report collected and sent this data to AdTech and related companies, who in turn enabled a sprawling network of 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.
Children and parents were denied the knowledge or opportunity to challenge these practices. Most EdTech companies did not disclose their surveillance of children and their data; similarly, most governments did not provide notice of these practices and their risks to students or teachers when announcing their endorsements of EdTech platforms.

But even if children were aware of being surveilled in their virtual classrooms, they could not meaningfully opt out or refuse to provide their personal data to EdTech companies. The Council of Europe noted, “[A]s the education is compulsory and refusal or withdrawal of consent could be detrimental to the development of the child, children would not be in a position to consent freely, irrespective of the assistance by parents or legal representatives.”

This was particularly true in countries that provided most children's education solely through officially-endorsed EdTech platforms, as further discussed in Chapter 4.

**Websites: Ad Trackers**

Ad trackers identify and collect information about a person visiting a website. By scrutinizing a person’s every action and behavior, ad trackers use their presumed preferences to target them with specific ads, then measure how successful the ad has been at capturing the person’s attention or enticing them to click on it. Ad trackers usually take the form of JavaScript scripts or web beacons, which are near-invisible, 1x1 pixel images that are hidden on a website to silently record what users do, including when they visited the site and where they were physically located.
Human Rights Watch found that children’s educational websites installed as many third-party trackers on personal devices as do the world’s most popular websites aimed at adults. Out of a total 124 EdTech websites, 112 websites (90 percent) placed third-party trackers on devices and browsers used by children. In comparison, an investigation conducted by The Markup in September 2020 found that of the world’s over 80,000 most popular websites, a list that includes global e-commerce giants that deploy extensive advertising, 84.9 percent loaded third-party trackers on their website.\(^ {100}\)

Put another way, children are just as likely to be surveilled in their virtual classrooms as adults shopping in the world’s largest virtual malls, if not more so.

Children are also being tracked at dizzying scale. Human Rights Watch found 717 third-party trackers embedded in these EdTech websites; a child logging into a single one of these 112 platforms at the start of the school day could expect to be tracked by an average of 6 third-party trackers. One EdTech site, Z-kai, endorsed by the Japanese Education Ministry for all elementary, middle, and high school students in Japan to learn core subjects during Covid-19 school closures, embedded 54 ad trackers that were detected transmitting students’ data to 37 companies, predominantly in AdTech.

The number of advertising or other third-party companies receiving children’s data was discovered to be even greater than the number of EdTech companies sending this data to them. Human Rights Watch detected these 112 websites transmitting children’s data to 161 companies. Out of the 124 websites analyzed by Human Rights Watch, just 12 websites (10 percent) did not collect and transmit data about children through third-party trackers. These were: Juana Manso (Argentina), Stile Education (Australia: Victoria), Faso e-Educ@tion (Burkina Faso), Learn (Canada: Quebec), Biblioteca Digital Escolar (Chile), Jules (France), Ma classe à la maison (France), MaSpéMaths (France), Mebis (Germany: Bavaria), Visavid (Germany: Bavaria), NHK for School (Japan), and iEN (Saudi Arabia).\(^ {101}\) These sites point to an alternate vision of online education for children, one that preserves their privacy and does not surveil their students for profit.

---


\(^ {101}\) Human Rights Watch did not include Facebook in this list; while the website version of the product was not found with third-party ad trackers, the company relies on its own first-party tracking tools to collect and send its users’ data back to itself. See: Aaron Sankin and Surya Mattu, “I Scanned My Favorite Social Media Site on Blacklight and It Came Up Pretty Clean. What’s Going On?” *The Markup*, October 1, 2020, https://themarkup.org/ask-the-markup/2020/10/01/i-scanned-my-favorite-social-media-site-on-blacklight-and-it-came-up-pretty-clean-whats-going-on (accessed July 13, 2021).
II. HIDDEN SURVEILLANCE: CHILDREN’S DATA HARVESTED

102 Human Rights Watch interview with Jae-kuk H., 14, Seoul, South Korea, June 6, 2020.


Case Study: EBS, Republic of Korea

At the beginning of the pandemic, the Republic of Korea (South Korea)’s Education Ministry suspended all in-person learning and committed to providing online classes for all primary and secondary school students in the country. Jae-kuk H., a 14-year-old boy in Seoul, told Human Rights Watch at the time: “I feel like the earth has just stopped.” By April 20, 2020, the website of the national educational public broadcaster, Korea Educational Broadcasting System (EBS), received on average over 2.1 million users every day.103

Human Rights Watch notes that during Covid-19 school closures, the Korean education ministry recommended watching TV broadcast lessons on EBS, and to re-watch recordings of those lessons on the EBS sites. EBS’ home page is the primary gateway to access EBS’ educational offerings, much of which are directed towards children.104 Human Rights Watch also notes that it analyzed, among others, specific webpages that the Korean education ministry recommended for primary school students’ use.105

When a child opens up EBS’ home page, or its main page for primary school students, to log into school for the day, a swarm of trackers get to work. Within milliseconds, 24 ad trackers begin to suck up a child’s every movement and interaction within the virtual classroom and transmit this information to 15 advertising companies. A few of these recipients are large data brokers, companies that compile digital dossiers about people from information obtained from public, private, online, and offline sources.

EBS Sent Children’s Data to 15 AdTech Companies

<table>
<thead>
<tr>
<th>AdTech Company</th>
<th>AdTech Domain Receiving Children’s Data</th>
<th>How the AdTech company uses the data it receives, based on its marketing materials</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADPIE</td>
<td>adpies.com</td>
<td>“Generate amazing ad revenue like never before.”106</td>
</tr>
<tr>
<td>Appier</td>
<td>appier.net</td>
<td>“Achieve hyper-personalization and deliver 1:1 recommendations … Engage your customers with real-time notifications triggered by their behavior.”107</td>
</tr>
<tr>
<td></td>
<td></td>
<td>“[U]nifies and enriches existing customer data to help you better understand your audience and run AI models to easily predict their future actions.”108</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>BizSpring</th>
<th>bizspring.net</th>
<th>“BizSpring provides a variety of data solutions for MarTech/AdTech,” “Integrate' and 'connect' all behavioral data centered on 'people.' Predict user intentions with big data in which each individual’s behavioral patterns are alive and deliver a message that can directly increase conversion performance.”</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>“We build a single customer profile by integrating all data about the customer, including the movements and paths they take in an app or website … and even behavioral data from 3rd parties. Customers with specific behavioral tendencies can be easily identified at the level of each ‘person,’ and target segments can be extracted in the form of a list according to the purpose and utilized in various marketing activities.”</td>
</tr>
</tbody>
</table>

| Logger | logger.co.kr | “Logger™ provides data that can maximize marketing performance by tracking … every action that occurs on your website,” “Track your visitor’s clickstream to understand performance: … tracks all of the activities of visitors online and provides analysis data that can determine ROI.” |

<table>
<thead>
<tr>
<th>Criteo</th>
<th>criteo.com, criteo.net</th>
<th>“2.5 billion users … active in 100+ countries: a global perspective of consumers and commerce.”</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>“Pooled identity data within Criteo Shopper Graph ensures accurate cross-device identification from the billions of active online shoppers who use multiple devices to shop, and the tens of thousands of websites worldwide that continuously share their data with us. Stitch together device identifiers across billions of user timelines. Find patterns of behavior and listen to signals of intent.”</td>
</tr>
</tbody>
</table>

| Dable | dable.io | “Improve traffic and advertising earnings with the best personalization platform in Asia,” “consider personalization technology and native ads as effective profit models in increasing preference and user attention. Detailed targeting by interest, region, medium, time of day, etc.” |

| Enliple | mediacategory.com | “Enliple’s advertising solution differentiator is to analyze customer behavior data through Big Data-based customer insight and to deliver more personalized predictive analytics and maximize user’s ROI by automatically learning real-time customer behavior.” |

---


II. HIDDEN SURVEILLANCE: CHILDREN’S DATA HARVESTED

<table>
<thead>
<tr>
<th>Company</th>
<th>Website/Platform</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>facebook.com, facebook.net</td>
<td>“We will use Business Tool Data ... to match the Contact Information against user IDs,” “to prepare reports on your behalf on the impact of your advertising campaigns and other online content (“Campaign Reports”) and (b) to generate analytics and insights about people and their use of your apps, websites, products and services,” “to target your ad campaigns to people who interact with your business,” “use the Matched User IDs and associated Event Data to help you reach people with transactional and other commercial messages on Messenger and other Facebook Company Products,” and “to improve ad delivery, personalize features and content and to improve and secure the Facebook products.”</td>
</tr>
<tr>
<td>Google</td>
<td>google-analytics.com, doubleclick.net, googleadservices.com, googletagmanager.com, google.com</td>
<td>“Easily integrate and access your data to gain a deeper understanding of your customers and identify your most valuable audiences.” “Drive engagement with richer, more relevant ads. Thanks to Google’s unique understanding of customer intent, you’ll be able to show more relevant, meaningful ads to people when they’re most interested to learn more about your products and services.”</td>
</tr>
<tr>
<td>IPONWEB GmbH</td>
<td>bidswitch.net</td>
<td>“BidSwitch creates value for the Ad Tech ecosystem ... provides the underlying infrastructure that normalizes the connections between different programmatic technology platforms.... BidSwitch is continuously processing, filtering for fraud &amp; classifying inventory opportunities, layering on data and other services, then intelligently distributing it to relevant buyers across more than 130 Demand Side Technology platforms – all in real-time.” “Features: User &amp; ID syncing, Centralized cookie syncing and ID tables.”</td>
</tr>
<tr>
<td>Kakao</td>
<td>daum.net</td>
<td>“With Kakao’s technology, it finds suitable users and displays advertisements by capturing the moments when advertisements are needed. Experience a variety of sophisticated targeting, such as demographics, audience behavior, interests, Kakao services, and current location.”</td>
</tr>
</tbody>
</table>

---


128 Ibid.

<table>
<thead>
<tr>
<th>Company</th>
<th>Website/URL</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>MediaMath</td>
<td>mathtag.com</td>
<td>“MediaMath is the demand-side platform that offers the most powerful off-the-shelf and custom capabilities for brands to reach and influence customers and prospects on any screen. The digital advertising platform offers ... different targeting to drive a variety of goals/KPIs: audience, contextual, ... location.”</td>
<td></td>
</tr>
<tr>
<td>Oracle</td>
<td>bkrtx.com, bluekai.com</td>
<td>See below.</td>
<td></td>
</tr>
<tr>
<td>SK Communications</td>
<td>nate.com</td>
<td>“Based on users’ data, intensively focus on your key targets by: gender, age, location, and time.”</td>
<td></td>
</tr>
<tr>
<td>Co. Ltd</td>
<td></td>
<td>“Collect data that can identify people’s tendencies, such as their internet searches, news/posts browsed, shopping, videos viewed, memberships, etc., to find your targets for selective exposure.”</td>
<td></td>
</tr>
<tr>
<td>WiderPlanet</td>
<td>widerplanet.com</td>
<td>See below.</td>
<td></td>
</tr>
</tbody>
</table>

Among these, Human Rights Watch detected EBS transmitting children’s data to Oracle’s BlueKai Data Management Platform, a data broker that has amassed one of the world’s largest troves of data on people online.125 The company helps advertisers build even more extensive profiles on their users with the “actionable audience data” it has on billions of people, including billions of daily location signals acquired from other data brokers.126

In June 2020, TechCrunch reported that BlueKai had left one of its servers unprotected, spilling data on billions of records on people—names, home addresses, other personally identifiable data—out onto the open web for anyone to find.127 It was considered one of the most significant data security incidents of 2020, due to the immense size of the exposed database.128 Human Rights Watch detected EBS sending children’s data to Oracle’s BlueKai through its ad trackers bluekai.com and bkrtx.com, both before and after the reported data breach.
When reached for comment, Oracle confirmed the data leak, and said that an investigation it conducted in 2020 did not uncover evidence that data relating to children were involved. Oracle stated that any receipt of data related to children would be a violation of Oracle’s agreements and policy, and did not address whether it had nonetheless received child users’ data from six EdTech websites, including EBS. The company did not address whether data received from EBS were exposed as part of the 2020 security breach, and whether it had informed EBS or the other EdTech websites about the security breach.129

EBS also sent information about children’s behavior in its virtual classrooms to WiderPlanet, a Korean AdTech company. WiderPlanet advertises its “targeted advertising service” powered by the personal data they hold on “99% of Korean internet users” and information on what they do online. The company also claims it can uniquely identify 43 million people, “their interests and demographic types.”130 Given that 96 percent of Korea’s population uses the internet, this claim would mean that WiderPlanet holds the personal data of almost the entire country’s population.

WiderPlanet did not respond to our request for comment.

EBS’ privacy policy notes that it collects and uses its users’ personal information for “marketing and advertising,” including “demographic analysis, analysis of service visits and usage records, and provision of customized services based on personal information and interests.”131 It does not disclose the use of ad trackers on the site. Nor are the AdTech companies detected by Human Rights Watch to receive children’s data disclosed in the list of third parties officially recognized as processors of EBS users’ personal data.132

In their response to Human Rights Watch, EBS noted that EBS’ home page, “while it offers some paid subscription services such as health sciences and cooking classes for adults, mainly functions as a gateway to various Internet education websites of EBS.” EBS also stated that, of the user data it sends AdTech companies, it does not send information that would identify children. EBS pointed to a website, EBS Online Class, that it opened with support from the government and provided free education during the Covid-19 pandemic, and stated that this website, which Human Rights Watch did not analyze, as it required a student login, did not share users’ data with third-party companies.133

### Websites: Session Recording, Key Logging

Some EdTech websites are even more intrusive, embedding a tracking technology known as session recording that allows a third party to watch and record all of a user’s behavior on a web page.134 That includes mouse movements, clicks, movements around the page, and anything a user types into the page, even if they don’t click submit. The collection of such data minutiae is the digital equivalent of logging video surveillance each time a child scratches their nose or grasps their pencil in class.

Typically, these data would then be scrutinized by the third-party companies that offer session recording services on behalf of the website using their services in order to guess at a child’s personality, their preferences, and what they’re likely to do next.

---

129 Human Rights Watch email correspondence with Dorian Daley, Executive Vice President and General Counsel of Oracle, April 15, 2022.


132 Ibid., sections 4 and 5.

133 Human Rights Watch email correspondence with Suh Dong Won, Policy Planning Center Public Relations Manager of EBS, May 20, 2022.

Human Rights Watch found 23 EdTech websites, endorsed by eight governments, using session recorders. For all but one, their own materials describe and appear to market them for children’s use in education. Most transmitted children’s data to the third-party companies Hotjar or Yandex. Hotjar describes itself as a “Product Experience Insights software company”. Yandex, a technology company that describes itself as a “technology company that builds intelligent products powered by machine learning,” including search and information services, navigation products, and other mobile applications, claims that “clicks, scrolls, keystrokes, and mouse movements are all recorded in a single informative movie... Never miss something interesting with up to 150,000 recordings per day.”

When reached for comment, both Hotjar and Yandex answered without responding to our questions. Amazon, who owns cloudfront.net, did not respond to a request for comment.

<table>
<thead>
<tr>
<th>EdTech Product</th>
<th>Country</th>
<th>Apparently designed for use by children?</th>
<th>Session recorders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Descomplica</td>
<td>Brazil: São Paulo</td>
<td>Yes</td>
<td>script.hotjar.com, static.hotjar.com</td>
</tr>
<tr>
<td>DragonLearn</td>
<td>Brazil: São Paulo</td>
<td>Yes</td>
<td>mc.yandex.ru/webvisor/, mc.yandex.ru/metrika/watch.js</td>
</tr>
<tr>
<td>Manga High</td>
<td>Brazil: São Paulo</td>
<td>Yes</td>
<td>script.hotjar.com, static.hotjar.com</td>
</tr>
<tr>
<td>Stoodi</td>
<td>Brazil: São Paulo</td>
<td>Yes</td>
<td>script.hotjar.com, static.hotjar.com</td>
</tr>
<tr>
<td>WorkFlowy</td>
<td>Colombia</td>
<td>Yes</td>
<td>script.hotjar.com, static.hotjar.com</td>
</tr>
<tr>
<td>iMektep</td>
<td>Kazakhstan</td>
<td>Yes</td>
<td>mc.yandex.ru/webvisor/, mc.yandex.ru/metrika/watch.js</td>
</tr>
<tr>
<td>Kundelik</td>
<td>Kazakhstan</td>
<td>Yes</td>
<td>mc.yandex.ru/metrika/tag.js, mc.yandex.ru/metrika/watch.js</td>
</tr>
<tr>
<td>Daryn Online</td>
<td>Kazakhstan</td>
<td>Yes</td>
<td>mc.yandex.ru/webvisor/, mc.yandex.ru/metrika/watch.js</td>
</tr>
<tr>
<td>sooballov</td>
<td>Kazakhstan</td>
<td>Yes</td>
<td>mc.yandex.ru/webvisor/, mc.yandex.ru/metrika/watch.js</td>
</tr>
<tr>
<td>iTest</td>
<td>Kazakhstan</td>
<td>Yes</td>
<td>mc.yandex.ru/webvisor/, mc.yandex.ru/metrika/watch.js</td>
</tr>
<tr>
<td>ExamenulTau</td>
<td>Romania</td>
<td>Yes</td>
<td>script.hotjar.com, static.hotjar.com</td>
</tr>
<tr>
<td>Miro</td>
<td>Romania</td>
<td>No</td>
<td>script.hotjar.com, static.hotjar.com</td>
</tr>
<tr>
<td>ȘcoalaIntuitext</td>
<td>Romania</td>
<td>Yes</td>
<td>script.hotjar.com, static.hotjar.com</td>
</tr>
<tr>
<td>My School is Online</td>
<td>Russia</td>
<td>Yes</td>
<td><a href="https://mc.yandex.ru/webvisor">https://mc.yandex.ru/webvisor</a>, mc.yandex.ru/metrika/tag.js</td>
</tr>
<tr>
<td>Digital Lessons</td>
<td>Russia</td>
<td>Yes</td>
<td><a href="https://mc.yandex.ru/webvisor">https://mc.yandex.ru/webvisor</a>, mc.yandex.ru/metrika/tag.js</td>
</tr>
<tr>
<td>SberClass</td>
<td>Russia</td>
<td>Yes</td>
<td><a href="https://mc.yandex.ru/webvisor">https://mc.yandex.ru/webvisor</a>, mc.yandex.ru/metrika/tag.js</td>
</tr>
</tbody>
</table>

A related technique is key logging, a particularly invasive procedure that surreptitiously captures personal information that people enter on forms, like names, phone numbers, and passwords, before they hit submit. This technique has been used for a variety of purposes, including identifying anonymous web users by matching them to postal addresses and real names, before they can consent to anything.\(^{137}\)

Human Rights Watch detected 16 websites deploying key logging techniques to send users’ names, usernames, passwords, and other information to first- and third-party companies. All of these websites, save one, are products whose own materials describe and appear to market them for children’s use for education.

<table>
<thead>
<tr>
<th>EdTech Product</th>
<th>Country</th>
<th>Apparently designed for use by children?</th>
<th>Key loggers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education Perfect:</td>
<td>Australia: Victoria</td>
<td>Yes</td>
<td>hsforms.com</td>
</tr>
<tr>
<td>Science</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Descomplica</td>
<td>Brazil: São Paulo</td>
<td>Yes</td>
<td>hsforms.com</td>
</tr>
<tr>
<td>Manga High</td>
<td>Brazil: São Paulo</td>
<td>Yes</td>
<td>mangahigh.com</td>
</tr>
<tr>
<td>Stoodi</td>
<td>Brazil: São Paulo</td>
<td>Yes</td>
<td>veinteractive.com, stooicl.com.br</td>
</tr>
<tr>
<td>Aprendo en Línea</td>
<td>Chile</td>
<td>Yes</td>
<td>nullcurriculumnacional.cl</td>
</tr>
<tr>
<td>Educar Ecuador</td>
<td>Ecuador</td>
<td>Yes</td>
<td>recursos.educarecuaedor.gob.ec</td>
</tr>
<tr>
<td>Mineduc Digital</td>
<td>Guatemala</td>
<td>Yes</td>
<td>mineduc.gob.gt</td>
</tr>
<tr>
<td>Daryn Online</td>
<td>Kazakhstan</td>
<td>Yes</td>
<td>yandex.com</td>
</tr>
<tr>
<td>Notesmaster</td>
<td>Malawi</td>
<td>Yes</td>
<td>youtube.com</td>
</tr>
<tr>
<td>EBS Online Classes</td>
<td>Republic of Korea</td>
<td>Yes</td>
<td>nullebs.co.kr</td>
</tr>
<tr>
<td>Miro</td>
<td>Romania</td>
<td>No</td>
<td>realtimeboard.com</td>
</tr>
</tbody>
</table>

---


II. HIDDEN SURVEILLANCE: CHILDREN’S DATA HARVESTED

---

...
For example, Stoodi, an educational website recommended by Brazil’s São Paulo Education Ministry, was found using key logging to capture children’s names and what they searched for inside of Stoodi. Even if children changed their minds and decided not to submit their personal information, the captured data was still automatically sent to a third-party advertising company, Ve Global. Stoodi did not disclose in its privacy policy that children’s data would be captured through key logging, or that it would be sent to a third-party company for commercial use.

Evidence of Stoodi deploying key logging to send user data to Ve Global, captured in real time. Here, “Idaaaa Tarbell” is the first and last name of a fictional student interested in signing up for Stoodi’s services. Once a child types in their name into Stoodi’s website, Stoodi immediately captures their name (as seen here under “filter”) and sends it to the web address “https://dtrcusa.veinteractive.com/FormMappings.” The domain veinteractive.com is owned by the company Ve Global. © 2022 Hye Jung Han/Human Rights Watch

When contacted for comment, Ve Global acknowledged that Stoodi was a former client, and confirmed that Stoodi still had Ve Global’s active tracking tags embedded on its website. Ve Global confirmed that it had subsequently disabled the content of the tag. This renders the tracker unusable for Stoodi to continue sending user data to Ve Global.

Stoodi did not respond to our request for comment.


139 Human Rights Watch email correspondence with Barbara Lacourt, Director, Global Head of Legal, Ve, March 24, 2022.
II. HIDDEN SURVEILLANCE: CHILDREN’S DATA HARVESTED

Apps: Software Development Kits (SDKs)

For children who attend online classes using their mobile phones, companies are able to track what they do by embedding software development kits (SDKs) in their apps. Much like building blocks in a toy set, SDKs are blocks or libraries of code written by a third-party company that perform defined functions—like a login page, or notification popups—that app developers can conveniently use when building their app without having to create the functionality from scratch. SDKs are the primary means for app developers to enable an app to work with third-party services.

While some SDKs provide core functionality that is needed for an app to work or to improve its technical performance, others are designed solely for advertising—to track users’ actions within the app, guess at their preferences, and display the most persuasive ad at the most persuasive time. Still other SDKs provide tracking services that are designed to secretly collect data about the user that can later be compiled and sold. What an SDK does, once implemented in an app, will depend on how it was designed by the third party. SDKs do not fall into neat categories at the time of this writing; for example, an SDK for an analytics company may also facilitate the preparation of user profiles, and an SDK for an advertising company may provide reporting and analytics capabilities.

When a child installs an app for school, the SDKs that the developer embedded in the app also receive the same access as the app to the mobile phone’s data and system resources; this facilitates the transmission of the child’s personal data directly to the third-party company that owns that SDK. Human Rights Watch identified 243 SDKs embedded within 66 apps, giving access to a significant array of children’s personal data to 33 third-party companies, many of which appear to have primary businesses in advertising and the monetization of users’ personal data. It is not possible for Human Rights Watch to reach definitive conclusions as to the companies’ motivations in embedding these SDKs, beyond reporting on what it observed in the data and the companies’ and governments’ own statements.

In the table below, Human Rights Watch lists the third-party SDKs found embedded in each EdTech app, and the “dangerous” permissions and sensitive user data to which they were granted access.

Human Rights Watch notes that it does not conclusively determine how any given SDK is used by a specific app, and that some SDKs may provide multiple capabilities in addition to advertising. Human Rights Watch also notes that the use of “dangerous” permissions to access sensitive data is not inherently unsafe, but poses risks to users’ privacy if there are no safeguards that protect against the abuse of such access by the host app or its embedded third-party SDKs.
<table>
<thead>
<tr>
<th>EdTech app</th>
<th>Country</th>
<th>SDKs</th>
<th>EdTech app may give a third-party company access to a user's:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Teams</td>
<td>Australia: New South Wales, Germany: Bavaria, Republic of Korea, Spain, Taiwan, United Kingdom: England, US: Texas</td>
<td><strong>Microsoft</strong>: Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Crashes</td>
<td>Precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts’ information (contacts, contacts’ photo), call log, camera, microphone</td>
</tr>
<tr>
<td>Adobe Connect</td>
<td>Australia: New South Wales</td>
<td><strong>Google</strong>: Google Analytics</td>
<td>Phone number</td>
</tr>
<tr>
<td>Minecraft: Education Edition</td>
<td>Australia: Victoria</td>
<td><strong>AppsFlyer</strong>: AppsFlyer, <strong>Braze</strong>: Braze, <strong>Google</strong>: Google Firebase Analytics</td>
<td>Persistent identifiers (Android Advertising ID, Wi-Fi MAC)</td>
</tr>
<tr>
<td>Centro de Mídias da Educação de São Paulo</td>
<td>Brazil: São Paulo</td>
<td><strong>Google</strong>: Google Crashlytics, Google Firebase Analytics</td>
<td>Camera, microphone</td>
</tr>
<tr>
<td>Descomplica</td>
<td>Brazil: São Paulo</td>
<td><strong>Google</strong>: Google Crashlytics, Google Firebase Analytics, Google AdMob</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
</tr>
<tr>
<td>Explicaê</td>
<td>Brazil: São Paulo</td>
<td><strong>Google</strong>: Google Crashlytics, Google Firebase Analytics</td>
<td>Camera</td>
</tr>
<tr>
<td>Stoodi</td>
<td>Brazil: São Paulo</td>
<td><strong>Google</strong>: Google Crashlytics, Google Firebase Analytics, Google Tag Manager, Google Analytics</td>
<td>Persistent identifiers (Android Advertising ID, IMEI)</td>
</tr>
<tr>
<td>Math Kids</td>
<td>Canada: Quebec</td>
<td>None</td>
<td>N/A</td>
</tr>
<tr>
<td>Prof Multi</td>
<td>Canada: Quebec</td>
<td><strong>Microsoft</strong>: Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Crashes</td>
<td>Microphone</td>
</tr>
<tr>
<td>Storyline Online</td>
<td>Canada: Quebec</td>
<td><strong>Google</strong>: Google Firebase Analytics</td>
<td>Persistent identifiers (Android Advertising ID)</td>
</tr>
<tr>
<td>App</td>
<td>Country</td>
<td>Google: Google Crashlytics, Google Firebase Analytics, Google Analytics</td>
<td>Persistent identifiers (Android Advertising ID), contacts' information (contacts, contacts' photo), camera</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Biblioteca</strong></td>
<td>Chile</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Digital Escolar</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Dropbox</strong></td>
<td>Colombia</td>
<td><strong>Google</strong>: Google Firebase Analytics</td>
<td>Persistent identifiers (Android Advertising ID), contacts' information (contacts, contacts' photo), camera</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Adjust</strong>: Adjust</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Bugsnag</strong>: Bugsnag</td>
<td></td>
</tr>
<tr>
<td><strong>Remind</strong></td>
<td>Colombia</td>
<td><strong>Google</strong>: Google Crashlytics, Google Firebase Analytics</td>
<td>Persistent identifiers (Android Advertising ID), contacts' information (contacts, contacts' photo), call log, camera, microphone</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Braze</strong>: Braze</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Pusher</strong>: Pusher</td>
<td></td>
</tr>
<tr>
<td><strong>WorkFlowy</strong></td>
<td>Colombia</td>
<td><strong>Google</strong>: Google Firebase Analytics</td>
<td>Camera, microphone</td>
</tr>
<tr>
<td><strong>Jules</strong></td>
<td>France</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Jitsi</strong></td>
<td>Germany: Baden-Württemberg</td>
<td><strong>Google</strong>: Google Crashlytics, Google Firebase Analytics</td>
<td>Camera, microphone</td>
</tr>
<tr>
<td></td>
<td>Germany: Bavaria</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Threema Work</strong></td>
<td>Germany: Baden-Württemberg, Germany: Bavaria</td>
<td><strong>None</strong></td>
<td>Precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), camera, microphone</td>
</tr>
<tr>
<td><strong>Moodle</strong></td>
<td>Germany: Baden-Württemberg, Germany: Romania, Kazakhstan</td>
<td><strong>Google</strong>: Google Firebase Analytics</td>
<td>Precise location (GPS, time of current location, last known location), coarse location, camera, microphone</td>
</tr>
<tr>
<td><strong>IServ</strong></td>
<td>Germany: Bavaria</td>
<td><strong>Google</strong>: Google Firebase Analytics</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>itslearning</strong></td>
<td>Germany: Bavaria</td>
<td><strong>Google</strong>: Google Crashlytics, Google Firebase Analytics</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
</tr>
<tr>
<td><strong>SchoolFox</strong></td>
<td>Germany: Bavaria</td>
<td><strong>Google</strong>: Google Firebase Analytics</td>
<td>Persistent identifiers (Android Advertising ID)</td>
</tr>
<tr>
<td><strong>Padlet</strong></td>
<td>Germany: Bavaria, Romania, Colombia</td>
<td><strong>Google</strong>: Google Crashlytics, Google Firebase Analytics</td>
<td>Persistent identifiers (Android Advertising ID, Wi-Fi MAC), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), phone number, camera, microphone</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Microsoft</strong>: Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Crashes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Branch</strong>: Branch</td>
<td></td>
</tr>
<tr>
<td><strong>Ghana Library App</strong></td>
<td>Ghana</td>
<td><strong>Google</strong>: Google Crashlytics, Google Firebase Analytics</td>
<td>Persistent identifiers (Android Advertising ID), camera, microphone</td>
</tr>
<tr>
<td>App</td>
<td>Country</td>
<td>Developers</td>
<td>Data Collected</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------</td>
<td>--------------------------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>YouTube</td>
<td>India: Uttar Pradesh, Malaysia, Nigeria, United Kingdom: England</td>
<td>Google: Google Firebase Analytics, Google AdMob</td>
<td>Persistent identifiers (Wi-Fi MAC), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts’ information (contacts, contacts’ photo), camera, microphone</td>
</tr>
<tr>
<td>e-Balbharti</td>
<td>India: Maharashtra</td>
<td>None</td>
<td>Phone number</td>
</tr>
<tr>
<td>Learning Outcomes</td>
<td>India: Maharashtra</td>
<td>Google: Google Firebase Analytics</td>
<td>None</td>
</tr>
<tr>
<td>Smart Q</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diksha</td>
<td>India: National</td>
<td>Google: Google Crashlytics, Google Firebase Analytics</td>
<td>Persistent identifiers (Android Advertising ID), precise location (GPS, time of current location, last known location), camera, microphone</td>
</tr>
<tr>
<td>ePathshala</td>
<td>India: National</td>
<td>Google: Google Crashlytics, Google Firebase Analytics</td>
<td>Persistent identifiers (Android Advertising ID)</td>
</tr>
<tr>
<td>Top Parent</td>
<td>India: Uttar Pradesh</td>
<td>Google: Google Crashlytics, Google Firebase Analytics, Google AdMob</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Facebook: Facebook Login, Facebook Share, Facebook Places</td>
<td>CleverTap: CleverTap</td>
</tr>
<tr>
<td>WhatsApp</td>
<td>India: Uttar Pradesh, Cameroon</td>
<td>Google: Google Analytics</td>
<td>Precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts’ information (contacts, contacts’ photo), phone number, SMS logs, camera, microphone</td>
</tr>
<tr>
<td>Khan Academy</td>
<td>India: Uttar Pradesh, Pakistan, Nigeria, South Africa</td>
<td>Google: Google Firebase Analytics</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Facebook: Facebook Analytics, Facebook Login, Facebook Share</td>
<td></td>
</tr>
<tr>
<td>Kelas Pintar</td>
<td>Indonesia</td>
<td>Google: Google Crashlytics, Google Firebase Analytics, Google AdMob, Google Analytics, Google Tag Manager</td>
<td>Persistent identifiers (Android Advertising ID, IMEI), contacts’ information (contacts, contacts’ photo), camera</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Facebook: Facebook Analytics, Facebook Login, Facebook Share</td>
<td>Adjust: Adjust</td>
</tr>
</tbody>
</table>

II. HIDDEN SURVEILLANCE: CHILDREN’S DATA HARVESTED
<table>
<thead>
<tr>
<th>App</th>
<th>Country</th>
<th>Google</th>
<th>Facebook</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quipper</td>
<td>Indonesia</td>
<td>Google Crashlytics,</td>
<td>Facebook Analytics,</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Google Firebase Analytics, Google Analytics</td>
<td>Facebook Login, Facebook Share</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Facebook Analytics, Facebook Login, Facebook Share</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Brightcove</td>
<td>UXCam</td>
<td>Wotric: Wotric</td>
</tr>
<tr>
<td>Ruangguru</td>
<td>Indonesia</td>
<td>Google Crashlytics,</td>
<td>Facebook Analytics, Facebook Login, Facebook Places, Facebook Share</td>
<td>Persistent identifiers (Android Advertising ID), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, call logs, camera, microphone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Google Firebase Analytics</td>
<td>Facebook Analytics, Facebook Login</td>
<td>AppsFlyer: AppsFlyer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Facebook Share</td>
<td>OneSignal: OneSignal</td>
</tr>
<tr>
<td>Rumah Belajar</td>
<td>Indonesia</td>
<td>Google Crashlytics,</td>
<td>Facebook Analytics, Facebook Login</td>
<td>Persistent identifiers (Android Advertising ID), precise location (GPS, time of current location, last known location), coarse location, camera</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Google Firebase Analytics</td>
<td>Facebook Share</td>
<td></td>
</tr>
<tr>
<td>Sekolah.mu</td>
<td>Indonesia</td>
<td>Google Crashlytics,</td>
<td>Facebook Analytics, Facebook Login</td>
<td>Precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, camera, microphone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Google Firebase Analytics</td>
<td>Facebook Share</td>
<td></td>
</tr>
<tr>
<td>Snowplow</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zenius</td>
<td>Indonesia</td>
<td>Google Crashlytics,</td>
<td>Facebook Analytics, Facebook Login</td>
<td>Camera, microphone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Google Firebase Analytics</td>
<td>Facebook Share</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AppsFlyer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shad</td>
<td>Iran</td>
<td>Google Crashlytics,</td>
<td></td>
<td>Persistent identifiers (Android Advertising ID), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts’ information (contacts, contacts’ photo), camera, microphone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Google Firebase Analytics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Newton</td>
<td>Iraq</td>
<td>Google AdMob</td>
<td></td>
<td>Persistent identifiers (Android Advertising ID)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>App</td>
<td>Country</td>
<td>Google Services</td>
<td>Additional Permissions</td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>------------------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>WeSchool</td>
<td>Italy</td>
<td>Google: Google Firebase Analytics</td>
<td>Persistent identifiers (Android Advertising ID), microphone</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Huawei: Huawei Mobile Services (HMS Core)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OneSignal: OneSignal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NHK for School</td>
<td>Japan</td>
<td>None</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>schoolTakt</td>
<td>Japan</td>
<td>Google: Google Crashlytics, Google Firebase Analytics</td>
<td>Persistent identifiers (Android Advertising ID)</td>
<td></td>
</tr>
<tr>
<td>Study Sapuri</td>
<td>Japan</td>
<td>Google: Google Crashlytics, Google Firebase Analytics, Google Analytics, Google AdMob</td>
<td>Persistent identifiers (Android Advertising ID)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AppsFlyer: AppsFlyer</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Keen: Keen</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Repro: Repro</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LINE</td>
<td>Japan, Taiwan</td>
<td>Google: Google Analytics, Google AdMob</td>
<td>Persistent identifiers (aaaaaWiFi MAC, IMEI), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), phone number, call logs, camera, microphone, flashlight, fingerprint</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Facebook: Facebook Login, Facebook Share</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bilimland</td>
<td>Kazakhstan</td>
<td>Google: Google Crashlytics, Google Firebase Analytics</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Facebook: Facebook Analytics, Facebook Login, Facebook Share</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Daryn Online</td>
<td>Kazakhstan</td>
<td>Amplitude: Amplitude</td>
<td>Persistent identifiers (Android Advertising ID), camera, microphone</td>
<td></td>
</tr>
<tr>
<td>Kundelik</td>
<td>Kazakhstan</td>
<td>Google: Google Crashlytics, Google Firebase Analytics, Google AdMob</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AppMetrica: AppMetrica</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>VKontakte: VKontakte SDK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yandex</td>
<td></td>
<td>Yandex: Yandex Ad</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TelmideTICE</td>
<td>Morocco</td>
<td>None</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Telegram</td>
<td>Nigeria</td>
<td>Google: Google Firebase Analytics</td>
<td>Precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts), phone number, call logs, camera, microphone</td>
<td></td>
</tr>
<tr>
<td>App</td>
<td>Country</td>
<td>Google: Google Crashlytics, Google Firebase Analytics, Google AdMob</td>
<td>Persistent identifiers (Android Advertising ID), contacts’ information (contacts, contacts’ photo), phone number, call logs, camera, microphone</td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------</td>
<td>---------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Edmodo</td>
<td>Nigeria, Egypt, Colombia, Ghana, Romania, Thailand</td>
<td>JW Player: JW Player</td>
<td>Matomo (Piwik): Matomo</td>
<td></td>
</tr>
<tr>
<td>Learn Smart</td>
<td>Pakistan</td>
<td>Google: Google Firebase Analytics</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Muse</td>
<td>Pakistan</td>
<td>Google: Google Crashlytics, Google Firebase Analytics</td>
<td>Persistent identifiers (Android Advertising ID, Wi-Fi MAC), microphone</td>
<td></td>
</tr>
<tr>
<td>Facebook</td>
<td>Facebook Analytics, Facebook Login, Facebook Share</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Taleemabad</td>
<td>Pakistan</td>
<td>Google: Google Crashlytics, Google Firebase Analytics</td>
<td>Persistent identifiers (Android Advertising ID, IMEI), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location</td>
<td></td>
</tr>
<tr>
<td>Facebook</td>
<td>Facebook Analytics, Facebook Login, Facebook Share</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KakaoTalk</td>
<td>Republic of Korea</td>
<td>Google: Google Crashlytics, Google Firebase Analytics</td>
<td>Persistent identifiers (Android Advertising ID, Wi-Fi MAC, IMEI), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts’ information (contacts, contacts’ photo), phone number, call logs, SMS logs, camera, microphone</td>
<td></td>
</tr>
<tr>
<td>AdFit</td>
<td>AdFit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Naver Band</td>
<td>Republic of Korea</td>
<td>Google: Google Firebase Analytics, Google AdMob</td>
<td>Persistent identifiers (Android Advertising ID), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts’ information (contacts, contacts’ photo), camera, microphone</td>
<td></td>
</tr>
<tr>
<td>Facebook</td>
<td>Facebook Analytics, Facebook Login, Facebook Share</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AppsFlyer</td>
<td>AppsFlyer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>InMobi</td>
<td>InMobi</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moat</td>
<td>Moat</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edpuzzle</td>
<td>Romania</td>
<td>Google: Google Crashlytics, Google Firebase Analytics</td>
<td>Phone number</td>
<td></td>
</tr>
<tr>
<td>Kinderpedia</td>
<td>Romania</td>
<td>Google: Google Crashlytics, Google Firebase Analytics</td>
<td>Persistent identifiers (Android Advertising ID), phone number, call logs, camera, microphone</td>
<td></td>
</tr>
<tr>
<td>Huawei</td>
<td>Huawei Mobile Services (HMS) Core</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OneSignal</td>
<td>OneSignal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Country</td>
<td>Google:</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------</td>
<td>------------------------------</td>
<td>--------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Miro</td>
<td>Romania</td>
<td>Google Crashlytics,</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Google Firebase Analytics,</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Google AdMob</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td>Branch</td>
<td></td>
<td></td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td>Moscow</td>
<td>Russia</td>
<td>Google Crashlytics,</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td>Electronic School</td>
<td></td>
<td>Google Firebase Analytics</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td>My Achievements</td>
<td>Russia</td>
<td>Google Crashlytics</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Facebook Analytics,</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Facebook Login, Facebook</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Share</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Flurry:</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Flurry</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>VKontakte:</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>VKontakte SDK</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td>iEN</td>
<td>Saudi Arabia</td>
<td>Google Crashlytics</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Google Firebase Analytics</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td>African</td>
<td>South Africa</td>
<td>None</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td>Storybook</td>
<td></td>
<td>N/A</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td>Extramarks</td>
<td>South Africa</td>
<td>Google Crashlytics,</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Google Firebase Analytics</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Google AdMob, Google Tag</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Manager</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Facebook Places, Facebook</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Login, Facebook Share</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adjust:</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adjust</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td>Google Meet</td>
<td>Spain, Poland,</td>
<td>Google Firebase Analytics</td>
<td>Contacts' information (contacts, contacts' photo), camera, microphone</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Taiwan, US:</td>
<td></td>
<td>Contacts' information (contacts, contacts' photo), camera, microphone</td>
<td></td>
</tr>
<tr>
<td></td>
<td>California,</td>
<td></td>
<td>Contacts' information (contacts, contacts' photo), camera, microphone</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Texas</td>
<td></td>
<td>Contacts' information (contacts, contacts' photo), camera, microphone</td>
<td></td>
</tr>
<tr>
<td>Nenasa</td>
<td>Sri Lanka</td>
<td>Google Crashlytics,</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Google Firebase Analytics</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Google Analytics,</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Google Tag Manager</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Facebook Analytics,</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Facebook Login, Facebook</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Share, Facebook Places</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AppsFlyer:</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AppsFlyer</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td>Facebook</td>
<td>Taiwan</td>
<td>None</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>PaGamO</td>
<td>Taiwan</td>
<td>Google Crashlytics,</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Google Firebase Analytics</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Facebook Analytics,</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Facebook Login, Facebook</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Share</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Amplitude:</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Amplitude</td>
<td>Persistent identifiers (Android Advertising ID), camera</td>
<td></td>
</tr>
</tbody>
</table>
Without significant technical expertise, children cannot know whether third-party SDK integrations are present in their EdTech app. But even if they were aware, none of the 66 apps analyzed by Human Rights Watch allowed their users to decline access to their data by a third-party company.

When reached for comment, Cisco stated that Webex does not share user data with Google Crashlytics or Google Firebase Analytics, as it has disabled data collection for those SDKs.

Five apps did not embed any SDKs, demonstrating that it is possible to build an app without sending children’s personal information to a third-party company, and without the ability to collect information about children that is unnecessary to provide them with education. These apps, and the governments that recommended them, are: Math Kids (Canada: Quebec), Jules (France), NHK for School (Japan), TelmideTICE (Morocco), and African Storybook (South Africa).\(^\text{143}\)

---

\(^{143}\) While the Facebook app was also found without third-party SDKs, Meta is an AdTech company that relies on its own first party tracking technologies to collect and send its users’ data to itself. See: Aaron Sankin and Surya Mattu, “I Scanned My Favorite Social Media Site on Blacklight and It Came Up Pretty Clean. What’s Going On?” The Markup, October 1, 2020, https://themarkup.org/ask-the-markup/2020/10/01/i-scanned-my-favorite-social-media-site-on-blacklight-and-it-came-up-pretty-clean-whats-going-on (accessed July 13, 2021).
II. HIDDEN SURVEILLANCE: CHILDREN’S DATA HARVESTED

Ruangguru, an EdTech app recommended by Indonesia’s Ministry of Education and Culture. Built by an Indonesian EdTech company of the same name, the company successfully completed a tenth round of funding in April 2021 after the pandemic drove significant growth in user volume and revenue and led to the company’s first fiscal year of profitability since its founding in 2014. The app is widely used by children in Indonesia. Ruangguru reported that it had 22 million users in 2020, and that a free version of its product offered during the pandemic was used by over 10 million students in Indonesia. The company also stated that “we have also been trusted to partner with 32 (out of 34) Provincial Governments and 326 City and District Governments in Indonesia.”

Forensic analysis found that Ruangguru collects personal data from its students, including their location, Android Advertising ID, information about the device they use, and in-app navigation, and transmits this to two companies: AppsFlyer and Facebook.

When a child opens up Ruangguru on their phone, the app immediately begins to track what they do in its virtual classrooms, compiling a log of everything the child does and sees in what is known as “in-app navigation.” This log is continually updated and transmitted not just to Ruangguru, via the domain tracker.ruangguru.com, but also to Facebook via the domain graph.facebook.com.

Ruangguru may surveil its virtual classrooms to target children with behavioral advertising. Ruangguru discloses in its privacy policy that it “may collect interaction information on the page (such as scrolling, clicks, or mouse movement),” for which “we’ll use this information to measure and understand the effectiveness of the advertising we do to you and other parties, and to serve advertisements for products and services that are relevant to you.” Ruangguru also notes that it may share this intimate information with “[a]dvertisers and ad networks that require data to select and offer relevant advertisements to you and other users,” and that “[w]e may use the personal data we collect to fulfill advertisers’ requests by showing their ads to that target audience,” though it does not disclose the identity of the advertisers and third-party companies that receive children’s data.

However, Ruangguru misleadingly states that it does “not disclose information about identifiable individuals, but we may provide them with aggregated information about our users.” However, forensic testing proves otherwise. Human Rights Watch and the Defensive Lab Agency found Ruangguru transmitting its students’ Android Advertising ID to AppsFlyer and to Facebook.

Ruangguru also tags its students’ devices with an additional, proprietary identifier and
II. HIDDEN SURVEILLANCE: CHILDREN'S DATA HARVESTED


149 Ibid.

150 Ibid. “We may combine information we receive from other sources with information you provide and information we collect. We may use this information as well as the combined information for the purposes set out above.”

151 Human Rights Watch email correspondence with Miranda Sissons, Director, Human Rights Policy, Meta, April 15, 2022; and with Danielle Blumenstyk Peterman, Head of Corporate Comms, AppsFlyer, April 6, 2022.


MUSE’s privacy policy discloses that the app “may collect ... the type of mobile device you use, your mobile device unique ID, the IP address of your mobile device, your mobile operating system, the type of mobile internet browser you use, unique device identifiers and other diagnostic data.” However, it does not disclose the data practices observed by Human Rights Watch.

When contacted for comment, MUSE stated that it did not believe that it has “collected children specific data from the app,” and doesn’t maintain “any repository of children’s data.” MUSE also confirmed that the app included “data sharing SDKs.” In later correspondence, MUSE also stated that “the data is collected of the user so we can better understand what content items were viewed more than others,” and that “Google and Facebook SDKs collect this data without sharing any data about a specific user – rather it collects the data of each user as a data point to understand overall usage.”

In its response to Human Rights Watch, Meta (Facebook) did not address whether it was receiving children’s user data from MUSE. Google did not respond to our request for comment.

### Tracking Children Outside of the Classroom

My teacher makes me download Facebook, BiP, and WhatsApp for school. I don’t like these apps, because they understand and see everything that I do. They read my messages. They see everything that I do on my phone. This makes me feel bad.

—Rodin R., a nine-year old student in Istanbul, Turkey

Many children are tracked and surveilled even after they leave the virtual classroom. Human Rights Watch identified companies that track children online, outside of school hours, deep into their private lives, and over time.

### Websites: Cookies

A cookie is a small piece of data that companies store in a person’s web browser in order to uniquely identify that person. While not all cookies are trackers, third-party cookies are generally used by advertising and tracking companies to watch what people do online, infer their characteristics and interests, and deliver customized ads that then follow them around the internet.
Human Rights Watch found that children’s educational websites inserted as many third-party cookies on personal devices as do the world’s most popular websites aimed at adults. Out of a total 124 EdTech websites, Human Rights Watch detected 66 EdTech websites that had a total of 470 third-party cookies embedded in them. A child logging into a single one of these 66 platforms might be tracked on average by seven cookies or encounter a median of three cookies. Meanwhile, an investigation conducted by The Markup in September 2020 found that of the world’s over 80,000 most popular websites, a list that includes global e-commerce giants that deploy extensive advertising, a site loaded a median of three third-party cookies.

Put another way, children are surveilled in their virtual classrooms and followed long after they leave, outside of school hours and across the internet, at a similar rate as adults shopping in the world’s largest virtual malls.

The number of AdTech or other third-party companies receiving children’s data was discovered to be even greater than the number of EdTech sites sending this data to them.

Human Rights Watch detected 66 websites transmitting children’s data to 85 AdTech or third-party companies.

Some EdTech sites installed dozens of cookies. Human Rights Watch found 76 cookies installed on Z-kai, recommended by the Japanese government and noted earlier in this chapter as having installed the highest number of ad trackers amongst the EdTech websites analyzed by Human Rights Watch. These cookies trailed students even after they left Z-kai’s website to go elsewhere on the web, sending their whereabouts and activities to 31 AdTech companies.

**Case study: 100Ballov, Kazakhstan**

Some EdTech sites chose to install cookies by AdTech companies that engage in particularly deceptive practices. On April 3, 2020, children in Kazakhstan began logging into their first day of online classes, in accordance with their government’s pivot to online learning. Many of these children opened up 100Ballov, endorsed by the Education Ministry and adopted by schools as the “educational portal for schoolchildren and students.”

Human Rights Watch detected 100Ballov sending information about its students to AddThis, a marketing company acquired by Oracle in 2016. AddThis offers a set of social media share buttons that allows website users to easily share interesting content on social media.

But AddThis does much more than encourage social media traffic. Whether or not a person clicks on the “share” button, AddThis instantly loads dozens of cookies and tracking pixels on website visitors’ browsers, like nesting dolls, each collecting and sending user data to Oracle and to dozens of other AdTech companies to profile and target a person or a child with behavioral advertising that follows them across the internet.

AddThis’ privacy policy states:

> The AddThis Tools also incorporate Cookies and Pixels from Oracle partners to enable the synchronization of unique identifiers between Oracle and our third-party partners to facilitate online behavioral advertising across the online advertising ecosystem.

Human Rights Watch found six AddThis cookies on 100Ballov, which in turn loaded four other trackers by AddThis’ advertising partners: two cookies pointing to DoubleClick, Google’s advertising division, and two to Tapad. Tapad, an AdTech company, describes its services as “enabling marketers to identify a brand customer or related household across multiple devices, unlocking key use cases across programmatic targeting, media measurement, attribution, and personalization globally.”

100Ballov did not disclose this practice on its website; it does not have a privacy policy at all. AddThis’ button is not visible on any of 100Ballov’s webpages, indicating that AddThis and its nested cookies were harvesting children’s data without even providing its purported social media functionality, as well as denying children knowledge of these tracking practices.
In response to our request for comment, Oracle stated that any receipt of children’s data through its AddThis tools is a violation of Oracle’s policies, which prohibit advertising partners and website publishers from sending personal information from sites directed to children under 16 years old, or from consumers these companies know to be under 16 years old. Oracle did not address whether it had received children’s data from 100Ballov.

100Ballov did not respond to our request for comment.

---


III. Hidden Manipulation: How Children’s Data Are Used

These companies, they don’t let us know. They’re not transparent with us, saying that this is exactly where your data goes, and this is exactly what happens with it. We’re trusting them blindly without knowing what’s going on. And us kids won’t doubt it at all—we won’t even think that something bad is happening behind our backs. The amount that we’ve shared, all that we’ve done online, that it’s all gone to some strange person … The whole idea starts haunting you, and you get really scared.

—Priyanka S., 16, Uttar Pradesh, India

Profiled and Targeted

Most online learning platforms used during the pandemic secretly harvested vast amounts of data from children, piecing them together to deduce each child’s characteristics, behaviors, and interests. Combined in this way, personal data can uniquely identify a child; algorithms can mine this data to guess at a child’s identity, location, interests, emotions, health, and relationships, and use these inferences to predict what a child might do next, or how they might be influenced.

Profiling and targeting children on the basis of their actual or inferred characteristics not only infringes on their privacy, but also risks abusing or violating their other rights, particularly when this information is used to anticipate and guide them toward outcomes that are harmful or not in their best interest.
Such practices also play an enormous role in shaping children’s online experiences and determining the information they see, which can influence, shape, or modify children’s opinions and thoughts in ways that exploit their lack of understanding, affect their ability to make autonomous choices, and limit their opportunities or development. Such practices may also have adverse consequences that continue to affect children at later stages of their lives.170

The United Nations Committee on the Rights of the Child has warned that such processing and use of children’s data “may result in violations or abuses of children’s rights,” and has called on states to “prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling.”171

The Office of the High Commissioner for Human Rights has stated more broadly that the mass collection and processing of fine-grained information about people’s lives to infer their physical and mental characteristics, profile, and make decisions about them “carries risks for individuals and societies that can hardly be overestimated,”172 with implications for people’s access to health care, financial services, and due process rights, among others. In guidelines issued to its member states, the Council of Europe stated: “Profiling of children, which is any form of automated processing of personal data which consists of applying a ‘profile’ to a child, particularly in order to take decisions concerning the child or to analyse or predict his or her personal preferences, behaviour and attitudes, should be prohibited by law.”173

Below, we discuss the different ways in which user profiles on children can be misused. Human Rights Watch found that EdTech’s profiling and targeting of children did not yield any educational benefit to children; furthermore, the invasiveness of these data practices stands in sharp contrast to the strict limits and laws that governments place on the collection, sharing, and use of student data by schools.

### Behavioral Advertising

Children are particularly susceptible to advertising, due to their still-developing cognitive abilities and impulse inhibition. Research on children’s cognitive development in relation to television commercials has demonstrated that younger children, particularly those under 7 years old, cannot identify ads or understand their persuasive intent; children at 12 years and older begin to distinguish between organic content and advertisements, though this does not translate into their ability to resist marketing.174

On the internet, much like adults, many older children and teenagers struggle with understanding the opaque supply chain of commercial activity in which their personal data are valued, traded, and used.175

---


Children are at even greater risk of manipulation by behavioral advertising online. When children’s data are collected for advertising, sophisticated algorithms extract and analyze overwhelming amounts of children’s personal data for the purpose of tailoring ads accurately. These ads are embedded in personalized digital platforms that further blur the distinctions between organic and paid content. In doing so, behavioral advertising capitalizes on children’s disabilities to identify or critically think about persuasive intent, potentially manipulating them toward outcomes that may not be in their best interest.

Behavioral advertising is even more egregious when targeted at children in settings where they cannot realistically refuse it. In the absence of alternatives, children faced a singular choice whether they were aware of it or not: attend school and use an EdTech product that infringes upon their privacy, or forgo the product altogether, be marked as absent, and be forced to drop out of school during the pandemic. Furthermore, as children spent a considerable amount of their childhood online in virtual classrooms during Covid-19 lockdowns, they were maximally exposed to the risks of collection and exploitation of their personal data.

The Committee on the Rights of the Child has stated that countries “should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling.” In a statement issued to pediatric health care providers, industry, and policy makers, the American Academy of Pediatrics raised concerns “about the practice of tracking and using children’s digital behavior to inform targeted marketing campaigns, which may contribute to health disparities among vulnerable children or populations.”

Human Rights Watch found that 199 third-party companies, most of them AdTech companies, received children’s personal data from just 145 EdTech products. Put another way, the number of advertising companies receiving children’s data vastly outnumber the number of EdTech companies collecting children’s data.

Most EdTech companies concealed their data surveillance practices. Of the total 163 EdTech products reviewed by Human Rights Watch, only 35 disclosed in their privacy policies that their users’ data was used for behavioral advertising. Of these, 23 products were developed with children as their primary users in mind, suggesting that behavioral advertising to children was an intended feature of the EdTech product.
Case Study: ȘcoalaIntuitext, Romania

Recommended by Romania’s Education Ministry, ȘcoalaIntuitext discloses in its privacy policy that it installs 23 marketing cookies in order to target its students with behavioral advertising across the internet.

Excerpt from ȘcoalaIntuitext’s Privacy Policy, as seen on May 2, 2022.180

Marketing cookies are used to track users from one site to another. The intent is to show relevant and engaging ads to individual users, so they are more valuable to advertising agencies and third parties dealing with advertising.

<table>
<thead>
<tr>
<th>Name</th>
<th>Provider</th>
<th>Purpose</th>
<th>Expiry</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>_zlcmid</td>
<td>Zendesk</td>
<td>Preserves users states across page requests.</td>
<td>1 year</td>
<td>HTTP cookie</td>
</tr>
<tr>
<td>_fbp</td>
<td>Meta Platforms, Inc.</td>
<td>Used by Facebook to deliver a series of advertising products such as real time bidding from third party advertisers.</td>
<td>3 months</td>
<td>HTTP cookie</td>
</tr>
<tr>
<td>_gcl_au</td>
<td>Google</td>
<td>Used by Google AdSense for experimenting with advertisement efficiency across websites using their services.</td>
<td>3 months</td>
<td>HTTP cookie</td>
</tr>
<tr>
<td>_hjRecording-Enabled</td>
<td>Hotjar</td>
<td>This cookie is used to identify the visitor and optimize ad-relevance by collecting visitor data from multiple websites – this exchange of visitor data is normally provided by a third-party data-center or ad-exchange.</td>
<td>Session</td>
<td>HTML Local Storage</td>
</tr>
<tr>
<td>ads/ga-audiences</td>
<td>Google</td>
<td>Used by Google AdWords to re-engage visitors that are likely to convert to customers based on the visitor’s online behaviour across websites.</td>
<td>Session</td>
<td>Pixel Tracker</td>
</tr>
<tr>
<td>fr</td>
<td>Meta Platforms, Inc.</td>
<td>Used by Facebook to deliver a series of advertisement products such as real time bidding from third party advertisers.</td>
<td>3 months</td>
<td>HTTP Cookie</td>
</tr>
<tr>
<td>IDE</td>
<td>Google</td>
<td>Used by Google DoubleClick to register and report the website user’s actions after viewing or clicking one of the advertiser's ads with the purpose of measuring the efficacy of an ad and to present targeted ads to the user.</td>
<td>1 year</td>
<td>HTTP Cookie</td>
</tr>
</tbody>
</table>

When contacted for comment, Softwin, the Romanian EdTech company that operates ȘcoalaIntuitext, said that the product is “actually dedicated first to teachers/educators and only in a subsidiary way to children or their parents.” The company acknowledged that it sends user data through marketing cookies, Facebook Pixel, and Google Analytics’ ‘remarketing audiences’ feature, and that it does so to target adults “in the places where our main customers (teachers/educators) are active,” including on Facebook and on Google. Softwin responded that, “To be clear no children’s data collected by ScoalaIntuitext.ro is used for advertising, behavioral advertising, or any other commercial purposes.”

---

It denied that it sends children’s data to third parties or AdTech companies and said that the children’s data it collects is not used for advertising, behavioral advertising, or user profiling.\textsuperscript{181}

However, ŞcoalaIntuitext is marketed for children’s use. Its home page features a marketing message directed at students that explains the benefits of the product.\textsuperscript{182} Another page on the website, titled “Children,” is directed to would-be child users and states that, “ŞcoalaIntuitext is an educational platform ... intended for primary school students (Preparatory classes – IV), their parents and primary school teachers.”\textsuperscript{183}

The page also asks students to advertise ŞcoalaIntuitext to their teacher: “Share with your teacher that you have discovered this useful application and enjoy the benefits of ŞcoalaIntuitext TOGETHER,” and features four share buttons which, when clicked, opens a social media platform or new email message and prompts the student user to log in to share pre-populated text inviting the recipient, presumably their teacher, to use ŞcoalaIntuitext.\textsuperscript{184}

Human Rights Watch found that ŞcoalaIntuitext embedded tracking technologies on pages that were likely to be accessed by children, including the page titled “Children,” and observed ŞcoalaIntuitext sending user data to AdTech companies through the third-party marketing cookies, Facebook Pixel and Google Analytics’ ‘remarketing audiences’ feature that it acknowledged. The company did not acknowledge its use of ad trackers and session recording.\textsuperscript{185} Human Rights Watch did not find evidence that these data practices were limited to adults.
Human Rights Watch also found that five governments directly built and offered EdTech products for which they disclosed, through their privacy policies, that they use children’s personal data to target behavioral advertising back at them.

<table>
<thead>
<tr>
<th>Country</th>
<th>EdTech Product</th>
<th>Privacy Policy</th>
</tr>
</thead>
</table>
| Canada        | CBC Kids       | “The data collected when you visit our website or click on our digital ads is used to show you future ads that match your interests. Ad targeting is used to create larger group profiles and larger audience segments made of users across Canada that share common interests.”

“Our advertising partners use cookies to show you ads. They’ll look at the cookies you already have on your browser and decide whether and which ad they want to place on our site for you to see.”  

| Ghana         | Ghana Library Mobile Application | “We may use information collected about you via the Application to ... Deliver targeted advertising, coupons, newsletters, and other information regarding promotions and the Application to you” and “Offer new products, services, mobile applications, and/or recommendations to you.”

“We may share your information with third parties for marketing purposes ... Additionally, we may use third-party software to serve ads on the application, implement email marketing campaigns, and manage other interactive marketing initiatives. This third-party software may use cookies or similar tracking technology to help manage and optimize your online experience with us.”  

| Indonesia     | Rumah Belajar   | “We may share Your information with Our business partners to offer You certain products, services or promotions.”

“We may share Your personal information with Service Providers to ... show advertisements to You to help support and maintain Our Service, to contact You, to advertise on third party websites to You after You visited our Service.”

“The information gathered via these Cookies may directly or indirectly identify you as an individual visitor. This is because the information collected is typically linked to a pseudonymous identifier associated with the device you use to access the Website. We may also use these Cookies to test new advertisements ... to see how our users react to them.”

| Republic of Korea | EBS       | “(Korea Education Broadcasting Corporation) processes personal information for the following purposes: Use for marketing and advertising. Personal information is processed for the purpose of developing new services (products) and providing customized services, providing event and advertising information.”

“The company uses cookies for the following purpose: to provide targeted marketing and personalized services by analyzing the frequency and time of visits by members and non-members, identifying, tracing, and tracking users’ preferences and interests, and identifying the degree of participation in various events and the number of visits, etc.”


**South Africa**  Ministry of Education’s website

“National Department of Basic Education also uses your personally identifiable information to inform you of other products or services available from National Department of Basic Education and its affiliates.”

“National Department of Basic Education may, from time to time, contact you on behalf of external business partners about a particular offering that may be of interest to you.”

“National Department of Basic Education keeps track of the Web sites and pages our customers visit within National Department of Basic Education … This data is used to deliver customized content and advertising within National Department of Basic Education to customers whose behavior indicates that they are interested in a particular subject area.”

**Case Study: CBC Kids, Canada**

When a child opens CBC Kids, offered by the Canadian Broadcasting Corporation and recommended by Canada’s Quebec Education Ministry for pre-primary and primary school-aged children’s learning, the first thing they see on the page are large, brightly colored tiles. In July 2021, the first tile featured a photo marked by a heart emoji and captioned, “AWW: Check out these cute baby animals.” Another tile was filled with brightly colored characters and titled “MONSTER MATH! Are you a math wizard? Let’s find out.” The front page also offered the newest episode of “The Adventures of Paddington;” the link was decorated with the smiling face of the famous fictional bear, waving his paw at the viewer.
At the same time, when the child opens up the website, an invisible swarm of ad trackers and cookies get to work. Human Rights Watch found 29 third-party trackers collecting and sending data about children to 18 companies, mostly AdTech, and another 15 third-party cookies sending children's data to nine companies, mostly AdTech. To put this into perspective, this is more than five times the median number of three cookies and more than four times the median of seven ad trackers installed on the world's most popular internet sites—sites that include heavily trafficked e-commerce sites with explicit business interests in marketing.  

15 third-party cookies on CBC Kids collected and sent children's data to 9 companies

<table>
<thead>
<tr>
<th>AdTech company</th>
<th>Receiving domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe</td>
<td>demdex.net, dpm.demdex.net</td>
</tr>
<tr>
<td>Bombora</td>
<td>ml314.com</td>
</tr>
<tr>
<td>Google</td>
<td>doubleclick.net</td>
</tr>
<tr>
<td>LiveRamp</td>
<td>rlcdn.com, rlcdn.com</td>
</tr>
<tr>
<td>Lotame</td>
<td>crwdcntrl.net, crwdcntrl.net, crwdcntrl.net, crwdcntrl.net, crwdcntrl.net</td>
</tr>
<tr>
<td>Neustar</td>
<td>agkn.com</td>
</tr>
<tr>
<td>Piano</td>
<td>cxense.com</td>
</tr>
<tr>
<td>The Trade Desk</td>
<td>adsrvr.org</td>
</tr>
<tr>
<td>WarnerMedia</td>
<td>adnxs.com</td>
</tr>
</tbody>
</table>

29 ad trackers on CBC Kids collected and sent children's data to 18 companies

<table>
<thead>
<tr>
<th>AdTech company</th>
<th>Receiving domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe</td>
<td>adobedtm.com, demdex.net, everesttech.net, omtrdc.net</td>
</tr>
<tr>
<td>Akamai Technologies</td>
<td>akstat.io, edgekey.net, go-mpulse.net</td>
</tr>
<tr>
<td>Amplitude</td>
<td>amplitude.com</td>
</tr>
<tr>
<td>Bombora</td>
<td>ml314.com</td>
</tr>
<tr>
<td>Chartbeat</td>
<td>chartbeat.com, chartbeat.net</td>
</tr>
<tr>
<td>Cheetah Digital (formerly Wayin)</td>
<td>wayin.com</td>
</tr>
<tr>
<td>comScore</td>
<td>scorecardresearch.com</td>
</tr>
<tr>
<td>Conductrics</td>
<td>conductrics.com</td>
</tr>
<tr>
<td>Facebook</td>
<td>facebook.com, facebook.net</td>
</tr>
<tr>
<td>Google</td>
<td>google-analytics.com, googlesyndication.com, googletagmanager.com, googletagservices.com, doubleclick.net</td>
</tr>
<tr>
<td>LiveRamp</td>
<td>rlcdn.com</td>
</tr>
<tr>
<td>Lotame</td>
<td>crwdcntrl.net</td>
</tr>
<tr>
<td>Neustar</td>
<td>agkn.com</td>
</tr>
<tr>
<td>Oracle</td>
<td>bluekai.com</td>
</tr>
<tr>
<td>Piano</td>
<td>cxense.com</td>
</tr>
<tr>
<td>Skimbit</td>
<td>skimresources.com</td>
</tr>
<tr>
<td>The Nielsen Company</td>
<td>exelator.com</td>
</tr>
<tr>
<td>Throttle</td>
<td>thrtle.com</td>
</tr>
</tbody>
</table>

Altogether, 20 companies involved in advertising and marketing received data about children from CBC Kids. Of these, six AdTech companies receiving data from CBC Kids—Adobe, Facebook, Google, LiveRamp, Piano, The Trade Desk—offer services to match website visitors to personally identifiable information sourced from other online and offline records, including physical addresses, location data, and credit scores, building or enhancing a comprehensive profile about that person that can be used and sold to “serve targeted advertising and content to the right audience” (Adobe) or to “understand and influence customer behavior” (Piano).

Of the 20 companies, seven companies—comScore, LiveRamp, Lotame, Neustar, Oracle, The Nielsen Company, and Throtle—have formally registered themselves with the California Data Broker Registry as data brokers, that is, companies whose primary business is the packaging and selling of people’s personal data.

Lotame, for instance, bills itself as the “World’s Largest 2nd and 3rd Party Data Marketplace” and “supplies real-time access to a firehose of raw behavioral data from billions of consumer profiles” which can be used to create user profiles. The company assures advertisers that they “can add demographic, behavioral, geographic, and other types of data to learn more about your customers and find new ways to monetize those audiences.” Human Rights Watch detected CBC Kids sending children’s data to Lotame through five cookies and an ad tracker.


Human Rights Watch detected CBC Kids sending children’s data to Lotame through five cookies and an ad tracker.
Human Rights Watch also found CBC Kids sending data about children to The Nielsen Company, which claims that it can “understand the personality of your customers and prospects to effectively forecast behavior with the largest personality database in the world.” Specifically, Human Rights Watch observed CBC Kids transmitting kids’ data through the ad tracker exelator.com, which then feeds into the eXelate data pool, “Nielsen’s proprietary and highly curated mix of offline and online data,” which Nielsen can sell to other companies to “help [them] win the battle for consumer attention.”

CBC Kids is covered by the privacy policy of its parent site, CBC, which reassures users that, “The vast majority of the information you create doesn’t have any indicator of who you are, personally.” However, Human Rights Watch observed CBC Kids sending children’s data to companies that claim to connect real people’s offline identity records to their online activities. One such company, LiveRamp, claims to “deterministically merg[e] offline PII (personally identifiable information, such as email address, name, postal address, and phone number) and matching to cookies, mobile device IDs, and proprietary platform IDs,” into what the company calls RampID. The company draws upon “a multi-billion record set” that includes public record data, publicly available data, and self-reported information.

LiveRamp promises its clients “real-time people-based insights … and build a mapping over time,” once clients place the company’s Real-Time Identity Service pixel and cookie on their website or advertisement. The pixel is programmed to send user information to LiveRamp’s domain rlcdn.com.

Human Rights Watch found CBC Kids sending data about the children visiting its website to LiveRamp through two embedded cookies and an ad tracker pointing to the domain rlcdn.com, none of which were disclosed in CBC’s privacy policy or cookie policy.

CBC discloses in its privacy policy that it engages in user profiling and behavioral advertising (see table above), but does not disclose the identity of these companies and data brokers that receive children’s data, or explain how they might use it. On a child-friendly webpage titled “How to Manage Your Cookies,” CBC Kids discloses that it uses “strictly necessary cookies … needed for CBC Kids to work,” “functionality cookies … needed for specific features of CBC Kids to work,” and “performance cookies [that] help us understand how well the CBC Kids sites are working.” However, CBC Kids does not disclose the presence of marketing cookies or ad trackers on its site, or that such tracking technologies are used to send children’s data to AdTech companies and data brokers. Moreover, children who accessed this webpage to learn how to opt out of being tracked by cookies were in turn surveilled, and their personal data transmitted, to six AdTech companies. Human Rights Watch detected cookies and ad trackers embedded in the “How to Manage Your Cookies” webpage sending children’s data to Adobe, ChartBeat, comScore, Cxense, Google, and Oracle.


When reached for comment, CBC said that it “explicitly prohibit[s] targeting on both our traditional and online platforms” and that “[t]he CBC.ca/kids [CBC Kids] section is ad free.” CBC confirmed the presence of 13 trackers on CBC Kids, of which 8 trackers—Adobe, Akamai, Amplitude, Chartbeat, comScore, Conductrics, Piano, Wayin—were used for site performance, functionality, and safety. The company said that another 4 trackers—Lotame, Oracle, Facebook, and Neustar—were inactive, and that trackers from Google were primarily restricted to product performance, though CBC had discovered a Google cookie that it planned to check.

As noted in the methodology of this report, Human Rights Watch conducted the primary phase of its investigation between May and August 2021, and conducted further checks in November 2021 to verify its findings. Human Rights Watch captured evidence, in real time, of CBC Kids transmitting data through the 29 ad trackers and 15 third-party cookies embedded on the site and listed in the tables above. These included the trackers that CBC acknowledged were present but inactive on the site.

While Human Rights Watch could not corroborate CBC’s statement that 8 trackers were used to enable core site functionality, other trackers were found sending data to domains explicitly owned by AdTech companies and used for their advertising businesses, including Google’s doubleclick.net.

When reached for comment, Akamai Technologies did not answer our questions regarding CBC Kids. Adobe, Cheetah Digital, Meta, and Oracle did not acknowledge that they receive data from CBC Kids, and said that it was their customers’ responsibility to comply with their policies and applicable laws that prohibit the collection of children’s data. LiveRamp said that it was not aware of a contractual or other relationship between LiveRamp and CBC Kids, and requested additional details. LiveRamp had not replied to Human Rights Watch’s April 13, 2022 correspondence sharing further technical evidence at the time of this writing.

Bombora denied that it receives data from CBC Kids, but acknowledged that it receives data from CBC’s parent site, cbc.ca. However, Human Rights Watch notes that its investigation focused on analyzing the data that was sent from eleven web pages from the CBC Kids domain (cbc.ca/kids).

In a statement, Piano said that it provided services to CBC Kids for the optimization of CBC Kids’ search engine, which did not involve the collection of children’s data from CBC Kids.

Amplitude did not respond to our questions on CBC Kids. comScore, Google, Lotame, Neustar, and Throtle did not respond to a request for comment.
Influencing Information, Shaping Beliefs

The use of children’s personal information to deliver highly targeted content and advertisements that follow them across the internet plays an enormous role in shaping children’s experiences and what they see online. This can influence, modify, and manipulate their thoughts and beliefs, nudging them to particular outcomes and possibly affecting their ability to make autonomous choices.217

Every child has the right to freedom of thought, and the right to access to information.218

Unlike the rights to freedom of expression, association, and assembly, which can be limited, freedom of thought is an absolute right. International human rights law protects children’s freedom of thought unconditionally from interference from any lawful or unlawful measure.219 While the law on this right is underdeveloped, some experts have recently argued that targeted behavioral advertising that manipulates people’s thoughts may threaten this right for all people, and particularly for children.220

The UN Committee on the Rights of the Child has noted that the digital environment “provides a unique opportunity for children to realize the right to access to information…. States parties should ensure that children have access to information in the digital environment and that the exercise of that right is restricted only when it is provided by law and is necessary.”221

The UN Committee on the Rights of the Child has noted that many automated processes shaping online experiences “may result in violations or abuses of children’s rights, including through advertising design features that anticipate and guide a child’s actions toward more extreme content […] or the use of a child’s personal information or location to target potentially harmful commercially driven content.”222

As such, governments “should ensure that all children are informed about, and can easily find, diverse and good quality information online, including content independent of commercial and political interests.” Governments should also “ensure that automated search and information filtering, including recommendation systems, do not prioritize paid content with a commercial or political motivation over children’s choices or at the cost of children’s right to information.”223

When these automated processes affect the quality of information that children can easily find online, they risk interfering with children’s right to freedom of thought.224

Because children are at high risk of manipulative interference at a time when their capacities are evolving, they may be particularly vulnerable when they come into contact with algorithms that
can be used to target and influence their thoughts, opinions, and beliefs through the curated display of content.  

As a result, the UN Committee on the Rights of the Child has urged governments to identify, define and prohibit practices that “manipulate or interfere with” children’s freedom of thought. It has also said that governments should ensure that “automated processes of information filtering systems, profiling, marketing and decision-making do not supplant, manipulate or interfere with children’s ability to form and express their opinions in the digital environment.”

The majority of government-endorsed EdTech apps and websites examined by Human Rights Watch sent information about children to Google and Facebook, two companies that not only dominate the advertising and analytics industries, but also serve as primary channels to the internet for much of the world and whose algorithms determine what many people—and children—see online.

### SDKs that Human Rights Watch observed most commonly embedded in EdTech apps

<table>
<thead>
<tr>
<th>SDK</th>
<th>Parent company</th>
<th>EdTech App Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Firebase Analytics</td>
<td>Google</td>
<td>56</td>
</tr>
<tr>
<td>Google Crashlytics</td>
<td>Google</td>
<td>40</td>
</tr>
<tr>
<td>Facebook Login</td>
<td>Facebook</td>
<td>20</td>
</tr>
<tr>
<td>Facebook Share</td>
<td>Facebook</td>
<td>17</td>
</tr>
<tr>
<td>Facebook Analytics</td>
<td>Facebook</td>
<td>16</td>
</tr>
<tr>
<td>Google AdMob</td>
<td>Google</td>
<td>13</td>
</tr>
<tr>
<td>Google Analytics</td>
<td>Google</td>
<td>11</td>
</tr>
<tr>
<td>AppsFlyer</td>
<td>AppsFlyer</td>
<td>6</td>
</tr>
<tr>
<td>Facebook Places</td>
<td>Facebook</td>
<td>5</td>
</tr>
<tr>
<td>Google Tag Manager</td>
<td>Google</td>
<td>5</td>
</tr>
</tbody>
</table>

### Third-party companies that Human Rights Watch observed most commonly receiving children’s data from EdTech websites through trackers

<table>
<thead>
<tr>
<th>Parent company</th>
<th>Number of trackers found in EdTech websites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>315</td>
</tr>
<tr>
<td>Facebook</td>
<td>71</td>
</tr>
<tr>
<td>Twitter</td>
<td>59</td>
</tr>
<tr>
<td>Adobe</td>
<td>34</td>
</tr>
<tr>
<td>Microsoft</td>
<td>34</td>
</tr>
<tr>
<td>HubSpot</td>
<td>20</td>
</tr>
<tr>
<td>New Relic</td>
<td>18</td>
</tr>
<tr>
<td>Hotjar</td>
<td>16</td>
</tr>
<tr>
<td>Naver</td>
<td>15</td>
</tr>
<tr>
<td>Yandex</td>
<td>15</td>
</tr>
</tbody>
</table>

---

225 The Council of Europe’s Committee of Ministers warned that “fine grained, sub-conscious and personalized levels of algorithmic persuasion may have significant effects on the cognitive autonomy of individuals and their right to form opinions and take independent decisions.” See: “Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes,” Decl (13/02/2019), February 13, 2019, https://search.coe.int/cm/pages/result_details.aspx?Objectid=090000168092dd4b (accessed July 22, 2021), para. 9.

226 In 2018, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression also noted that the “intersection of technology and content curation raises novel questions about the types of coercion or inducement that may be considered an interference with the right to form an opinion,” and that “[c]ommercial advertising has also sought to induce favourable opinions of and cultivate desire for particular products and services.” He concludes that “[c]ompanies should, at the very least, provide meaningful information about how they develop and implement criteria for curating and personalizing content on their platforms, including policies and processes for detecting social, cultural or political biases in the design and development of relevant artificial intelligence systems.” See UN General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/73/348, August 29, 2018, https://www.un-docs.org/A/73/348 (accessed July 22, 2021), paras. 24, 36.

226 CRC, General Comment No. 25, Children’s Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), paras. 61-62.
Third-party companies that Human Rights Watch observed most commonly receiving children’s data from EdTech websites through cookies

<table>
<thead>
<tr>
<th>Parent company</th>
<th>Number of cookies found in EdTech websites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>98</td>
</tr>
<tr>
<td>Microsoft</td>
<td>46</td>
</tr>
<tr>
<td>Mail.Ru Group, OOO</td>
<td>25</td>
</tr>
<tr>
<td>Pipefy</td>
<td>16</td>
</tr>
<tr>
<td>The Trade Desk</td>
<td>16</td>
</tr>
<tr>
<td>WiderPlanet</td>
<td>16</td>
</tr>
<tr>
<td>LiveRamp</td>
<td>10</td>
</tr>
<tr>
<td>Oracle</td>
<td>10</td>
</tr>
<tr>
<td>tawk.to</td>
<td>10</td>
</tr>
</tbody>
</table>

In countries and contexts where these companies are viewed as indistinguishable from the internet, the existence of behavioral advertising aimed at children and fueled by data collected in educational contexts risks affecting children’s rights to access diverse and good quality information online, including content independent of commercial interests.

**Facebook (Meta)**

Facebook, which rebranded itself as Meta in October 2021, is the world’s dominant social media company. It owns four of the world’s biggest social media platforms, and reported over 3.51 billion monthly users across all of its products in the second quarter of 2021. In 2014, Iris Oriss, Facebook’s head of localization and internationalization, wrote, “Awareness of the Internet in developing countries is very limited. In fact, for many users, Facebook is the internet, as it’s often the only accessible application.”

Due to Facebook’s ubiquity, its News Feed algorithm, which determines what each of its 2.9 billion users see every day by providing them with a personalized, constantly updated stream of content and advertisements, plays a significant role in influencing people’s opinions and beliefs by shaping the information they see online.

Facebook uses the vast amounts of data it has on people to continually train its News Feed algorithm to choose and show content that each person is most likely to engage with. In an internal report from 2018, Facebook found that its recommendation algorithm stoked polarization. “Our algorithms exploit the human brain’s attraction to divisiveness,” read a slide from the 2018 presentation. “If left unchecked,” it warned, Facebook would feed users “more and more divisive content in an effort to gain user attention & increase time on the platform.”
This became reality in Myanmar, “a context where, for most users, Facebook is the Internet.”

Given its prominence as the online population’s primary source of information, Facebook’s failure to prevent the spread of hate speech and disinformation that violated its policies on its platform resulted in the company playing what a UN-backed fact-finding mission later called “a determining role” in inciting real world violence in 2018.

In September 2021, a trove of internal documents leaked by the whistleblower Frances Haugen and first published in the Wall Street Journal indicated that over three years, the company’s researchers documented Instagram harming the mental and emotional health of a significant number of its child users. Instagram’s recommendation algorithm and the negative social comparisons that it stoked made body image issues worse for one in three girls, according to the documents; one slide from a 2019 presentation read, “Teens blame Instagram for increases in the rate of anxiety and depression. This reaction was unprompted and consistent across all groups.”

In response, Facebook’s Vice President of Global Affairs, Nick Clegg, said that the Wall Street Journal’s reporting “contained deliberate mischaracterizations of what we are trying to do, and conferred egregiously false motives to Facebook’s leadership and employees,” and suggested that they “need[ed] more evidence to understand social media’s impact on people.”

Nine days later, Facebook paused the development of an Instagram Kids service for children ages 13 and under.

Facebook uses its insights into its users to help advertisers target advertising to people in ways that are optimized to be persuasive to them. This significantly affects what people see on the platform. Over time, Facebook has increased the prevalence of advertising in its News Feed; a 2021 Wall Street Journal analysis of Facebook’s investor calls found that the company had increased the number of ads served on its platforms by a quarterly average of nearly 30 percent year on year since the third quarter of 2015. Simultaneously, Facebook has also increased the visual prominence and space taken up by ads in the News Feed, continually revising its ad formats to not only make them more prominent and attractive for users, but to integrate them to further blur the lines between advertisements and organic content.


As described in the previous section, children are at heightened risk of being influenced by behavioral advertising on social media sites like Facebook, where the lines between organic and commercial content are blurred and advertisements take up significant real estate in the News Feed.

In April 2021, Reset Australia, an advocacy group, reported that Facebook offered advertisers the ability to target their ads to approximately 740,000 children in Australia, and to target children as young as 13 determined by Facebook to be interested in smoking, extreme weight loss, and gambling, for as little as AU$3.03.240 A Facebook spokesperson said that the company reviews all ads before and after they run, and that advertisers must comply with Facebook’s policies and local laws.241

The news outlet the Australian reported in 2017 that a leaked Facebook document showed the company telling advertisers that it could judge when teenagers were feeling “insecure” and “worthless,” and offering advertisers the ability to target ads at the moment when young people “need a confidence boost.” The document, which stated that the company held data on 1.9 million Australian high schoolers, included an analysis on how young people express their emotions at different points during the week.242 In response, Facebook first released a statement to the Australian in which it apologized and said it would undertake disciplinary measures;243 it released a second statement that said the article’s premise was misleading, that it does not offer tools to target people based on their emotional state, and that the document was commissioned research that was never used to target ads and was based on anonymous and aggregated data.244

Not including Facebook’s own app and website, Human Rights Watch detected 62 EdTech products with embedded Facebook tracking technologies.245 Of these, 22 apps had installed Facebook’s SDKs, giving the company the ability to access children’s personal data, and 37 websites were found transmitting children’s data to Facebook through ad trackers, third-party cookies, and the Facebook Pixel.

**Facebook Pixel**

Human Rights Watch found 30 EdTech websites sending their users’ data to Facebook through a specific tracking technology known as the Facebook Pixel. This technology collects information about what students and teachers do on these sites and sends this data back to Facebook. This can be used by the EdTech website to later target them with ads on Facebook and Instagram.

Facebook can also retain and use this data for its own advertising purposes, although it is not always clear what these purposes are.246 The Facebook Pixel allows Facebook to track people across the internet, and build user profiles on people — even matching them and their data to their respective Facebook or Instagram profiles, if they have one, and even if they are not logged into Facebook at the time when they were accessing a website with an embedded Facebook Pixel.247 As noted previously in this report, the Facebook Pixel could also enable the company to collect personal data and create shadow profiles on people who have never used their services or signed up for an account.

---


Of the 30 EdTech websites found by Human Rights Watch to be sending data to Facebook through Facebook Pixel, 27 are websites specifically designed for use by children, and all were government-recommended for online learning. Facebook could use such data to profile children and target behavioral advertisements at them.

<table>
<thead>
<tr>
<th>Product</th>
<th>Country</th>
<th>Child specific?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Educ.ar</td>
<td>Argentina</td>
<td>Yes</td>
</tr>
<tr>
<td>Education Perfect: Science</td>
<td>Australia: Victoria</td>
<td>Yes</td>
</tr>
<tr>
<td>DragonLearn</td>
<td>Brazil: São Paulo</td>
<td>Yes</td>
</tr>
<tr>
<td>Mangahigh</td>
<td>Brazil: São Paulo</td>
<td>Yes</td>
</tr>
<tr>
<td>Descomplica</td>
<td>Brazil: São Paulo</td>
<td>Yes</td>
</tr>
<tr>
<td>Escola Mais</td>
<td>Brazil: São Paulo</td>
<td>Yes</td>
</tr>
<tr>
<td>Explicaê</td>
<td>Brazil: São Paulo</td>
<td>Yes</td>
</tr>
<tr>
<td>Stoodi</td>
<td>Brazil: São Paulo</td>
<td>Yes</td>
</tr>
<tr>
<td>StoryWeaver</td>
<td>Canada: Quebec</td>
<td>Yes</td>
</tr>
<tr>
<td>CBC Kids</td>
<td>Canada: Quebec</td>
<td>Yes</td>
</tr>
<tr>
<td>Dropbox</td>
<td>Colombia</td>
<td>No</td>
</tr>
<tr>
<td>Khan Academy</td>
<td>India: Uttar Pradesh, Pakistan, Nigeria, South Africa</td>
<td>Yes</td>
</tr>
<tr>
<td>WeSchool</td>
<td>Italy</td>
<td>Yes</td>
</tr>
<tr>
<td>Study Sapuri</td>
<td>Japan</td>
<td>Yes</td>
</tr>
<tr>
<td>Z-kai</td>
<td>Japan</td>
<td>Yes</td>
</tr>
<tr>
<td>eboard</td>
<td>Japan</td>
<td>Yes</td>
</tr>
<tr>
<td>Asahi Shimbun</td>
<td>Japan</td>
<td>No</td>
</tr>
<tr>
<td>Daryn Online</td>
<td>Kazakhstan</td>
<td>Yes</td>
</tr>
<tr>
<td>iTest</td>
<td>Kazakhstan</td>
<td>Yes</td>
</tr>
<tr>
<td>Learn Smart Pakistan</td>
<td>Pakistan</td>
<td>Yes</td>
</tr>
<tr>
<td>Sabaq Foundation</td>
<td>Pakistan</td>
<td>Yes</td>
</tr>
<tr>
<td>EBS</td>
<td>Republic of Korea</td>
<td>Yes</td>
</tr>
<tr>
<td>ExamenulTau</td>
<td>Romania</td>
<td>Yes</td>
</tr>
<tr>
<td>Kinderpedia</td>
<td>Romania</td>
<td>Yes</td>
</tr>
<tr>
<td>Miro</td>
<td>Romania</td>
<td>No</td>
</tr>
<tr>
<td>ȘcoalaIntuitext</td>
<td>Romania</td>
<td>Yes</td>
</tr>
<tr>
<td>Moscow Electronic School</td>
<td>Russia</td>
<td>Yes</td>
</tr>
<tr>
<td>Siyavula</td>
<td>South Africa</td>
<td>Yes</td>
</tr>
<tr>
<td>PaGamO</td>
<td>Taiwan</td>
<td>Yes</td>
</tr>
<tr>
<td>ST Math</td>
<td>US: Texas</td>
<td>Yes</td>
</tr>
</tbody>
</table>
In July 2021, Facebook announced that advertisers would no longer be able to use Facebook’s full suite of detailed targeting capacities when targeting children; instead, advertisers would be limited to targeting children based on their age, gender, and location. The announcement came two months after 44 state attorneys general in the US wrote to Facebook CEO Mark Zuckerberg asking him to abandon his plans to create an Instagram service for children under the age of 13, citing social media’s detrimental effect on the health and well-being of children and the company’s track record of having “historically failed to protect the welfare of children on its platforms.”

Facebook did not commit to limiting its own collection, profiling, and targeting of children for its own purposes. Its new policy does not protect children from advertisements targeted to people “living in this location,” “recently in this location,” or “traveling in this location,” as well as to infer further sensitive information about children as described in Chapter 2.

When reached for comment, Facebook did not acknowledge that they receive data from the EdTech products listed by Human Rights Watch, and said that it was their customers’ responsibility to comply with their policies and applicable laws that prohibit the collection of children’s data.

For children aged 13-17 with a user account with one of Facebook’s services, the company said that it “does not use data from our advertisers’ and partners’ websites and apps to personalize [ads] to people under 18,” and also confirmed that advertisers can only target ads to children aged 13-17 based on age, gender, and location. Facebook also said that children under 13 were not authorized to sign up for an account to use its products, and therefore if the company “were to inadvertently receive data relating to a child under 13, there would not be an authorized Meta user account for that child to which the data could be connected.”

An internal document written by Facebook’s privacy engineers on the Ad and Business Product team and published by Vice in April 2022 suggests that the company struggles to understand and track how people’s data are shared and used inside of its own systems. “We do not have an adequate level of control and explainability over how our systems use data, and thus we can’t confidently make controlled policy changes or external commitments such as ‘we will not use X data for Y purpose,’” the document said. In response to the internal document, Facebook said that the document did not demonstrate non-compliance with privacy regulations, because it did not describe the company’s processes and controls to comply with privacy regulations.
Google

Mr. Google has sucked in a beastly amount of information during these days.

—Pere Nieto, primary school teacher, Barcelona, Spain

Google holds unparalleled dominance over the world’s digital advertising market. According to public data, the company has been the global market leader in online advertising for over a decade, commanding a 27.5 percent share of digital ad spending in 2021. In turn, advertising contributes to the majority of Google’s business; in 2020, it reported that 80 percent of its total annual revenue, or US$147 billion, was earned by its ads business.

Google’s considerable control over online advertising is reinforced by the overwhelming market dominance of its other services, which have become essential to how most people participate in life online. Google is by far the most widely used search engine in the world; over 92 percent of all internet queries worldwide are done through Google, and to “Google” something is synonymous with online search itself. As such, the company’s algorithms determine what most people see when they search for information on the internet, as well as the digital ads displayed alongside their search results.

Nine of the company’s products—Android, Chrome, Gmail, Google Drive, Google Maps, Google Play Store, Google Photos, Google Search, and YouTube—have more than a billion users each. Each of these products provides vast amounts of user data back to Google, which analyzes this data to create new insights and information about people that can then be sold to advertisers.

The company collects data not just from people directly using their services, but from anyone who encounters their tracking technologies embedded across the internet. Google offers infrastructure and developer tools that are popularly used by other companies to build their own websites and apps; many of these tools offer multiple capabilities, including advertising. When using Google’s services, developers provide Google with their users’ data. Google offers developers the ability to collect users’ data through its non-advertising specific tools and integrate it later with its advertising services.


For example, Google Firebase Analytics offers developer tools for building and maintaining apps. It was the most prevalent SDK found in EdTech apps analyzed by Human Rights Watch, and is similarly ubiquitous in Android apps worldwide. Firebase also offers developers the capability to use their users’ personal data to “gain insight into who your users are, and what actions they’re taking inside your app,” and to “apply the power of machine learning to predict future user behavior.” Once collected and analyzed by Firebase, users’ personal data can be sent to and integrated with Google’s other advertising services, including Google Ads, AdMob, and Google Marketing Platform.

Google’s advertising ecosystem is opaque, and even experts struggle to understand how its algorithms use the data they collect or receive about people to decide what to show them online.\(^{264}\) It is difficult to know how personal data is used within Google’s ecosystem once it is collected, and difficult to distinguish between “where Google as a service provider ends, and where Google as an advertising service begins.”\(^{265}\)

Of the 163 EdTech products examined by Human Rights Watch, 131 products (80 percent) were found with embedded tracking technologies built by Google.\(^{266}\) Of these, 63 Android apps (86 percent of the total 73 apps examined) were found with at least one embedded Google SDK, giving the company the ability to access children’s personal data based on the Android permissions also granted to the app. Human Rights Watch observed 100 websites (81 percent of the total 124 websites examined) transmitting children’s data to Google through ad trackers, third-party cookies, and Google Analytics’ ‘remarketing audiences’ feature.

Human Rights Watch also further identified instances in which EdTech products sent or granted access to children’s data directly to Google’s advertising divisions, which Google may use for its own purposes.\(^{267}\)

For example, Google Analytics is popularly used for both its analytics and advertising capabilities. Human Rights Watch examined websites identified to be using a tool offered by Google Analytics, called its ‘remarketing audiences’ feature, that allows developers to make custom audience lists based on user behavior and then target ads to those users across the internet using Google Ads and Display & Video.\(^{360}\)

### EdTech products sent or granted access to children’s data to Google, using Google’s advertising-specific tracking technologies

<table>
<thead>
<tr>
<th>EdTech Type</th>
<th>Tracker</th>
<th>Receiving Domain</th>
<th>Number of EdTech products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apps</td>
<td>SDK</td>
<td>Google AdMob</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>SDK</td>
<td>Google Tag Manager</td>
<td>5</td>
</tr>
<tr>
<td>Websites</td>
<td>Ad Tracker</td>
<td>googletagmanager.com</td>
<td>64</td>
</tr>
<tr>
<td></td>
<td>Ad Tracker</td>
<td>doubleclick.net</td>
<td>63</td>
</tr>
<tr>
<td></td>
<td>Ad Tracker</td>
<td>googleadservices.com</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>Ad Tracker</td>
<td>googleoptimize.com</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Cookie</td>
<td>doubleclick.net</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>Cookie</td>
<td>10499192.fls.doubleclick.net</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Google Analytics’ ‘remarketing audiences’ feature</td>
<td>stats.g.doubleclick</td>
<td>52</td>
</tr>
</tbody>
</table>

Of the 73 EdTech apps reviewed in this report, Human Rights Watch found that 17 apps (23 percent) had installed one of Google’s ad-specific SDKs; likewise, out of the total 124 EdTech websites reviewed, 82 websites (66 percent) were found transmitting children’s personal data to Google’s advertising businesses.\(^{269}\)
For example, Human Rights Watch found 14 apps granting access to their users’ data to Google AdMob by installing the AdMob SDK, “one of the largest global ad networks” that “helps you monetize your mobile app through in-app advertising.” Ten out of the 14 are apps designed specifically for children’s use in education, and their data sharing practices directly impacted children. Google’s advertising policies prohibit targeting children under 13 with behavioral advertising or collection of their personal information for that purpose. However, the company did not preclude advertisers from continuing to use location data to infer sensitive information and target ads to children. The company also did not comment on the massive amounts of children’s personal data that it has received to date, nor did it commit to limiting its own collection of children’s data or its profiling and targeting of children.

In August 2021, Google announced that it would no longer allow advertisers to target personalized advertising to children based on their age, gender, or interests. However, the company did not preclude advertisers from continuing to use location data to infer sensitive information and target ads to children. The company also did not comment on the massive amounts of children’s personal data that it has received to date, nor did it commit to limiting its own collection of children’s data or its profiling and targeting of children.

Through dynamic analysis, Human Rights Watch detected one EdTech app, e-Pathshala, transmitting details about what children search for within the app to Google. The Indian Education Ministry, who built the app, does not notify its child users that the app is sending what information children seek within their virtual classroom to Google. Indeed, the app has no privacy policy at all.

Neither Google nor e-Pathshala responded to our request for comment.

In 2018, an AP investigation concluded that Google collects location data from Android users, even if users had set their privacy settings to prevent Google from doing so. The Attorney General of the US state of Arizona subsequently filed a consumer fraud lawsuit against Google in May 2020; newly unredacted documents in May 2021 revealed testimony from Jack Menzel, Google’s former Vice President of Product for Maps and current Vice President of Product for ads, that Google infers a user’s home and work locations without consent, even when a user has turned off all of their device’s location-related settings, and that the only way for Google not to infer a user’s home and work locations is to insert “arbitrary locations.” Karin Hennessy, Google’s product manager for ads privacy and safety, similarly noted during deposition that even if a user opts out of ads personalization, Google still uses the user’s real-time location to serve ads to them. See: Ryan Nakashima, “AP Exclusive: Google tracks your movements, like it or not,” Associated Press, August 13, 2018; https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d41b3ac257a07c1a80eb4 (accessed August 11, 2021); State of Arizona Attorney General, Mark Brnovich v. Google LLC, The Superior Court of the State of Arizona In and For The County of Maricopa, Complaint, May 2021, https://www.azag.gov/sites/default/files/2021-05/Complaint%20%28redacted%29.pdf (accessed August 11, 2021), paras. 93, 99; Google, “Personalized Advertising,” https://web.archive.org/web/20210811183214/https://support.google.com/adspolicy/answer/143465 (accessed August 11, 2021).
IV. Failure to Protect

This is scary. Especially us kids, we blindly trust our country, the whole education system, because we don’t question these things yet. We don’t have enough experience.... As kids, we feel powerless. What can I even do as a kid to stop these companies? That idea itself hurts a lot.

—Priyanka S., 16, Uttar Pradesh, India

Companies’ and Governments’ Child Rights Responsibilities

Companies have a responsibility to respect all children’s rights, wherever they operate in the world and throughout their operations. This is a widely recognized standard of expected corporate conduct, as set out in international human rights standards including the United Nations Guiding Principles on Business and Human Rights, and by the UN Committee on the Rights of the Child.

Companies’ responsibilities encompass preventing their services from being used in ways that cause or contribute to violations of children’s rights, even if they were not directly involved in perpetrating abuses. These responsibilities hold even when a national government lacks the necessary laws and regulations to sanction such abuses, or is unable or unwilling to protect children’s rights.

Governments are responsible for ensuring that businesses meet these responsibilities. They have a duty to protect children and their rights, and so should prevent, monitor, investigate, and punish child rights abuses by businesses. Governments are themselves also held responsible for violating children’s rights if they have failed to take necessary, appropriate, and reasonable measures to prevent and remedy such violations, or otherwise tolerated or contributed to these violations.
When children’s rights are violated in an environment of opaque digital systems, businesses’ global operations, and complex flows of data and technology between actors and across jurisdictions, children face immense challenges in finding justice. It is difficult for children, much less adults, to obtain evidence, identify perpetrators, or to even know what their rights are and when they have been abused—particularly if they have to act individually and expose themselves to scrutiny to get action from digital service providers.

Governments are obligated to provide effective remedies for violations of children’s rights, and companies have a responsibility to put in place processes to remedy rights abuses which they caused or to which they contributed. Remedies should be widely known and readily available to all children; they should involve prompt, thorough, and impartial investigation of alleged violations, and should be capable of ending ongoing violations.

Child Data Protection Laws

The United Nations Convention on the Rights of the Child recognizes that children need special safeguards and care, including legal protections, at all stages of their lives.

Even as more children spend increasing amounts of their childhood online, most countries in the world do not have modern child data protection laws that would provide protections to children in complex online environments. For example, of the 49 countries examined by Human Rights Watch in this report, 14 countries had no data protection laws at all. Twenty-four countries possessed data protection laws that contained references to children, but these were restricted to the question of who may provide consent to the processing of children’s data. Some of these were written at a time when digital technologies and data practices described in this report did not exist. For example, the United States’ Children’s Online Privacy Protection Act, signed into law in 1998 and subsequently amended, does not provide protections to children aged 13 to 18, nor restrict companies from collecting and using children’s data for purposes not in the best interest of the child, including commercial interests and behavioral advertising. This domestic law has impacted children’s digital experiences worldwide due to the fact that many of the largest and most influential technology companies that provide global services—including the majority of AdTech companies covered in this report—are headquartered in the US.

As a result, technology companies have faced little regulatory pressure or incentive to prioritize the safety and privacy of children in the design of their services. Most online service providers do not offer specific, age-appropriate data protections to children, and instead treat their child users as if they were adults.

The majority of EdTech products examined by Human Rights Watch did not offer data protections specific to children, nor did they provide a high level of privacy by design and default. As noted in this report, of the 163 EdTech products reviewed, 145 (89 percent) engaged in data practices that put children’s rights at risk, contributed to undermining them, or actively infringed on these rights.

Of the 74 AdTech companies that responded to Human Rights Watch’s request for comment, an overwhelming majority did not state that they had operational procedures in place to prevent the ingestion or processing of children’s data, or to verify that the data they did receive comply with their own policies and applicable child data protection laws. Absent effective protections, AdTech companies appear to routinely ingest and use children’s data in the same way they do adults’ data.
The UN Committee on the Rights of the Child states that governments “should review, adopt and update national legislation” to ensure that the digital environment protects children’s rights, and that such legislation “should remain relevant, in the context of technological advances and emerging practices.”

287 Laws should be updated to specifically support enforcement and compliance in digital environments.

### Education

Every child has the right to education. International human rights law makes clear that governments are responsible for ensuring free and compulsory primary education, and governments must fulfill an “unequivocal” requirement to ensure the availability of primary education without charge to children, their parents or guardians, and eliminate all direct and indirect costs to children’s education. Governments must make secondary education progressively available and accessible to all children. Human Rights Watch calls on states to take immediate measures to ensure that secondary education is available and accessible to all, free of charge. Human Rights Watch also calls on states to make education compulsory through the end of lower secondary school, in line with the Sustainable Development Goals and the political commitments made by all United Nations member states to provide 12 years of free primary and secondary education, with 9 compulsory years of education.

Education offered to children needs to “promote the realization of the child’s other rights,” placing the best interests of students as a “primary consideration.” As digital technologies can be used to support children’s access to education, the Committee on the Rights of the Child has stated that governments “should ensure that the use of those technologies is ethical and appropriate for educational purposes and does not expose children to … misuse of their personal data, commercial exploitation or other infringements of their rights.”

The Abidjan Principles on the human rights obligations of states to provide public education and to regulate private involvement in education, which are guiding principles adopted in 2019 by a group of independent experts from around the world, state that governments should regulate companies providing ancillary services that enable learning to ensure that their actions facilitate, not obstruct, the right to education. They further call on governments to “ban commercial advertising and marketing in public and private instructional educational institutions, and ensure that curricula and pedagogical methodologies and practices are not influenced by commercial interests.” Where children rely on services from the private market to access their right to education, states should also ensure that private actors do not infringe on children’s other rights, including their rights to privacy; to play; to seek, receive, and impart information; to freedom of expression; and to freedom of thought.

As described in this chapter, some governments made it compulsory for students and teachers to use government-built or endorsed EdTech products during the pandemic. This not only subjected them to the data practices and privacy protections—or lack thereof—of those products, but also made it impossible for children to protect themselves by opting for alternative means to access their right to education.
Students, Parents, and Teachers Operating in Blind Faith

Children, parents, and teachers operated on blind faith that their governments would protect children’s rights when providing education online during Covid-19 school closures.

Many children and parents told Human Rights Watch that they did not recall ever being asked for their consent, much less informed how their rights might be protected or affected, when told to adopt specific EdTech products for school.299 Hayley John, a mother of two in Murwillumbah, Australia, said: “I just trusted the school had looked into it. What would we do about it anyway?... We were worried about the tension and uncertainty around this pandemic, so we were trying to make things work.”300

But teachers told Human Rights Watch that they were also not informed how the EdTech products they were told to use would protect their students’ privacy or told to explain and seek consent from children or their parents.301 One secondary school teacher in London, United Kingdom, was told by his school to begin teaching in Google Classroom. But regarding the protection of his students’ privacy, he said: “I’m not sure what the school has done. [...] I’m not aware that any student has signed any kind of waiver or consent form. I certainly haven’t.”302

Asked whether she had been instructed to seek consent from students and parents, Marie-Therese Exler, a 6th grade teacher in Schleswig-Holstein, Germany, said: “No. I assumed it would be fine and someone else decided over this.”303 A secondary school teacher in Bilbao, Spain, said simply, “If the school’s IT team says to use it, it is supposed to be fine.”304

Some teachers told Human Rights Watch that their government created accounts for them and their students on EdTech platforms without asking for consent or informing them of the products’ privacy practices. Fifth-grade teacher Daniela Andrea Ribeiro Espinoza, in Santiago, Chile, said: “The platforms were activated from the Huechuraba education department. They activated everything and sent us an institutional email, no more. We have never been asked to sign or accept anything.”305 When asked whether he was asked to explain or seek consent from his students and their parents, one teacher in Hesse, Germany said: “No. We just got the access code [for the software] and that was it.”306

“We don’t really understand what’s going on with data protection,” said a primary school teacher in Barcelona, Spain. “The teachers at my school have accepted it, but it is the feeling that the students and teachers know everyone’s home, as they have entered them virtually ... I don’t know how it would have worked if someone hadn’t wanted to [use the EdTech platform]. Being an extraordinary situation, people have accepted it.... There have been zero clear guidelines from the government or the Department of Education.”307

Some teachers expressed concern for their students’ data privacy.308 Abby Rufer, an algebra teacher in Texas, US, said that her school district initially did not implement protections for students’ privacy. “Teachers were using [an online platform] which has no privacy protection. I was worried because, especially for our kids, this is not safe for them. Sixty to seventy percent of our kids had one primary family member that had been deported or was currently in ICE [US Immigration and Customs Enforcement] holding. So, this is unacceptable, and it is a dangerous situation to put these kids in.”309
Companies Failed to Protect

Human Rights Watch found that the data practices of an overwhelming majority of EdTech companies and their products risked or infringed on children’s rights. As noted above, companies are responsible for preventing and mitigating abuses of children’s rights, including those they indirectly contribute to through their business relationships. Out of 94 EdTech companies, 87 (93 percent) directly sent or had the capacity to grant access to children’s personal data to 199 companies, overwhelmingly AdTech, as described in Chapters 2 and 3. In many cases, this enabled the commercial exploitation of children’s personal data by third parties, including AdTech companies and advertisers, and put children’s rights at risk or directly infringed upon them.310

The majority of these companies—79—built and offered educational products designed specifically for children’s use. In each of these 80 products apparently designed for use by children, the EdTech company implemented tracking technologies to collect and to allow AdTech companies to collect personal data from children.

Most EdTech companies did not inform children and their parents of how children were secretly surveilled by the online learning platforms they used daily for school. As described in Chapter 2, companies failed to disclose data practices that risked or infringed on children’s privacy; 18 companies did not provide a privacy policy at all. 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, these companies also impeded children’s access to justice and remedy.

Case Study: Daryn Online, Kazakhstan

Flush with new users and a captive audience during Covid-19 school closures, EdTech companies faced financial incentives to commercialize children’s data and their attention. This was exemplified by Daryn Online, an educational website built by a Kazakh startup, Bugin Soft, which offers classes for students in grades 1 to 12 and claims to be the “Number 1 educational ecosystem in Kazakhstan.”

On March 20, 2020, the Kazakhstan Ministry of Education recommended Daryn Online for children’s learning during Covid-19 school closures, working with the country’s telecommunications providers to zero-rate the website—that is, not charging users for data use when accessing that specific website—to allow students to use it for free.311 Within days, the website was overwhelmed by 1.5 million new users.312 In an interview with Forbes Kazakhstan, 27-year old founder Aibek Kuatbaev said, in astonishment, “we could not imagine such an explosive growth,” and that this “organic growth took place with the support of the state.”313

By April 1, 2020, the founder sought to monetize the attention of his newfound user base by posting a “Price List for Advertising” on Daryn Online’s home page, offering advertisers the opportunity to advertise to his students.314 An advertiser could purchase the ability to display an ad banner on the login and registration page—which students had to pass through in order to get to their classes—for 70,000 KZT (US$164) a day, or 420,000 KZT (US$985) for a whole week. Advertisers could also purchase the ability to send out a push notification that would appear on the phones of 800,000 users of Daryn Online’s study app for 900,000 KZT (US$2,112).
Human Rights Watch also detected Daryn Online transmitting children’s personal data to Google, CloudFlare, Yandex, and Facebook, and found that the website engaged in intrusive surveillance of its students by installing session recorders and key logging.

Daryn Online discloses in their privacy policy that they may use information about a child and what they do in class—including their search history, messages, and comments to teachers, classmates, or written on their homework—for advertising and sponsorship purposes, and provide “anonymous” data to “third parties, as well as to partners and advertisers.” The company also “reserves the right to download advertisements of other organizations on Daryn.online without the User’s consent.”

Daryn Online did not respond to our request for comment.

Governments Failed to Protect

Because Spain was in a state of emergency, the Ministry of Education communicated [to teachers] that consent for privacy, or data protection, was no longer required ... Privacy and all that has gone into the background completely, but we have done it because the Ministry has said so.

—Secondary school science teacher, Madrid, Spain

With the exception of a single government—Morocco—all governments reviewed in this report failed to protect children’s right to education. Human Rights Watch found that every government endorsed or procured at least one EdTech product that appeared to put at risk or infringed on children’s rights. Similarly, the majority of EdTech products endorsed by governments—145 out of 163, or 89 percent—engaged in data practices that appeared to put children’s rights at risk or directly infringed on them.

Most EdTech products were marketed as free and provided to governments at no direct financial cost. In the process of endorsing these and promoting their wide adoption by schools, teachers, and students, governments offloaded the true costs of providing education online onto children, who were forced to pay for their learning with their fundamental rights to privacy, access to information, and their freedom of thought.

Most governments failed to take measures to prevent or mitigate children’s rights abuses by companies. Few governments appear to have taken child data privacy into consideration in their endorsements of EdTech products. At time of writing, no government reviewed in this report was found to have undertaken a technical privacy evaluation of the EdTech products they recommended after the declaration of the pandemic in March 2020.
One government, Australia (New South Wales), conducted assessments for two of its three EdTech recommendations in June 2020 and October 2021. These assessments rely on a self-reported questionnaire completed by an EdTech company, and reviewed by a non-profit company owned by state, territory, and Australian Government education ministers.

Human Rights Watch found that two national education ministries and two state-level ministries—Republic of Korea, Australia (Victoria), Germany (Bavaria), and Poland—provided general data privacy guidance to schools relating to online learning.

Governments that did not carry out children’s rights due diligence passed onto children the risks and harms associated with the misuse and exploitation of their personal data, which include security breaches, commercial exploitation, and the use of children’s data by governments, law enforcement, and other actors for purposes that are not directly relevant, necessary, or proportionate to children’s education or their best interests.

As noted in Chapter 2, for example, Oracle’s BlueKai was reported to have exposed billions of people’s personal data in one of the largest data security breaches in 2020. Human Rights Watch detected four EdTech products—CBC Kids (Canada), Z-kai (Japan), Notesmaster (Malawi), and EBS (Republic of Korea)—transmitting their students’ data to BlueKai through ad trackers and cookies pointing to the domains bluekai.com and bkrtx.com, both prior to, and after, the reported data breach.

317 Human Rights Watch email correspondence with Sandie Matthews, Chief Information and Data Officer, New South Wales Department of Education, April 14, 2022.


320 For further examples, please refer to chapter 2 of this report.
Governments Directly Engage in Rights Violations

Many governments directly built and offered their own EdTech products that violated or put at risk children's rights.

Out of the 42 governments that provided online education to children during the pandemic by directly building and offering their own EdTech products, 39 governments produced products that handled children's personal data in ways that may have put at risk or violated their rights, as described in chapters 2 and 3.

Put another way, out of a total 65 EdTech products built or financed by governments, the majority—56, or 86 percent—were found transmitting children's data to AdTech companies.

56 government-built EdTech products sent children’s data to AdTech companies

<table>
<thead>
<tr>
<th>Government</th>
<th>EdTech Product</th>
<th>Has Privacy Policy?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Argentina</td>
<td>Educ.ar</td>
<td>Yes</td>
</tr>
<tr>
<td>Brazil (Minas Gerais)</td>
<td>Estude em Casa</td>
<td>No</td>
</tr>
<tr>
<td>Brazil (São Paulo)</td>
<td>Centro de Mídias da Educação de São Paulo</td>
<td>Yes</td>
</tr>
<tr>
<td>Burkina Faso</td>
<td>Faso e-Educ@tion</td>
<td>No</td>
</tr>
<tr>
<td>Cameroon</td>
<td>Distance Learning</td>
<td>No</td>
</tr>
<tr>
<td>Canada (Quebec)</td>
<td>CBC Kids</td>
<td>Yes</td>
</tr>
<tr>
<td>Canada (Quebec)</td>
<td>Mathies</td>
<td>No</td>
</tr>
<tr>
<td>Canada (Quebec)</td>
<td>PBS Learning</td>
<td>Yes</td>
</tr>
<tr>
<td>Chile</td>
<td>Aprender en Línea</td>
<td>Yes</td>
</tr>
<tr>
<td>China</td>
<td>Eduyun</td>
<td>No</td>
</tr>
<tr>
<td>Colombia</td>
<td>Aprender Digital</td>
<td>No</td>
</tr>
<tr>
<td>Côte d’Ivoire</td>
<td>Mon école à la maison</td>
<td>No</td>
</tr>
<tr>
<td>Ecuador</td>
<td>Educa Contigo</td>
<td>No</td>
</tr>
<tr>
<td>France</td>
<td>Deutsch für Schulen</td>
<td>Yes</td>
</tr>
<tr>
<td>France</td>
<td>English for Schools</td>
<td>Yes</td>
</tr>
<tr>
<td>Ghana</td>
<td>Ghana Library App</td>
<td>Yes</td>
</tr>
<tr>
<td>Guatemala</td>
<td>Mineduc Digital</td>
<td>Yes</td>
</tr>
<tr>
<td>India (Maharashtra, National, Uttar Pradesh)</td>
<td>Diksha</td>
<td>Yes</td>
</tr>
<tr>
<td>India (Maharashtra, National, Uttar Pradesh)</td>
<td>e-Pathshala</td>
<td>Yes</td>
</tr>
<tr>
<td>India (Maharashtra)</td>
<td>e-Balbhari</td>
<td>Yes</td>
</tr>
<tr>
<td>Indonesia</td>
<td>Rumah Belajar</td>
<td>Yes</td>
</tr>
<tr>
<td>Iran</td>
<td>Shad</td>
<td>No</td>
</tr>
<tr>
<td>Iraq</td>
<td>Newton</td>
<td>No</td>
</tr>
<tr>
<td>Kenya</td>
<td>Kenya Education Cloud</td>
<td>No</td>
</tr>
<tr>
<td>Malawi</td>
<td>Notesmaster</td>
<td>Yes</td>
</tr>
<tr>
<td>Country</td>
<td>Platform/Website</td>
<td>Status</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Malaysia</td>
<td>DELiMa</td>
<td>No</td>
</tr>
<tr>
<td>Mexico</td>
<td>@prende 2.0</td>
<td>Yes</td>
</tr>
<tr>
<td>Nepal</td>
<td>Learning Portal</td>
<td>No</td>
</tr>
<tr>
<td>Peru</td>
<td>Aprendo en Casa</td>
<td>No</td>
</tr>
<tr>
<td>Poland</td>
<td>E-podręczniki</td>
<td>Yes</td>
</tr>
<tr>
<td>Republic of Korea</td>
<td>EBS</td>
<td>Yes</td>
</tr>
<tr>
<td>Republic of Korea</td>
<td>KERIS edunet</td>
<td>Yes</td>
</tr>
<tr>
<td>Republic of Korea</td>
<td>Wedorang</td>
<td>Yes</td>
</tr>
<tr>
<td>Russian Federation</td>
<td>Moscow Electronic School</td>
<td>Yes</td>
</tr>
<tr>
<td>Russian Federation</td>
<td>My Achievements</td>
<td>Yes</td>
</tr>
<tr>
<td>Russian Federation</td>
<td>My School is Online</td>
<td>No</td>
</tr>
<tr>
<td>Russian Federation</td>
<td>Digital Lessons</td>
<td>Yes</td>
</tr>
<tr>
<td>Russian Federation</td>
<td>Russia Electronic School</td>
<td>Yes</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>iEN</td>
<td>Yes</td>
</tr>
<tr>
<td>South Africa</td>
<td>Department of Basic Education website</td>
<td>Yes</td>
</tr>
<tr>
<td>Spain (Andalusia)</td>
<td>eAprendizaje</td>
<td>Yes</td>
</tr>
<tr>
<td>Spain (Catalonia)</td>
<td>EDU365.cat</td>
<td>Yes</td>
</tr>
<tr>
<td>Spain (Catalonia)</td>
<td>Super3</td>
<td>Yes</td>
</tr>
<tr>
<td>Spain (National)</td>
<td>Aprendo en Casa</td>
<td>Yes</td>
</tr>
<tr>
<td>Sri Lanka</td>
<td>e-Thaksalawa</td>
<td>No</td>
</tr>
<tr>
<td>Sri Lanka</td>
<td>Nenasa</td>
<td>Yes</td>
</tr>
<tr>
<td>Taiwan</td>
<td>Education Cloud</td>
<td>Yes</td>
</tr>
<tr>
<td>Taiwan</td>
<td>Kaohsiung Daxuetang</td>
<td>Yes</td>
</tr>
<tr>
<td>Taiwan</td>
<td>Taipei CooC Cloud</td>
<td>Yes</td>
</tr>
<tr>
<td>Thailand</td>
<td>DEEP</td>
<td>Yes</td>
</tr>
<tr>
<td>Turkey</td>
<td>Eğitim Bilişim Ağıt</td>
<td>No</td>
</tr>
<tr>
<td>Turkey</td>
<td>Özelim Eğitimdeyim</td>
<td>Yes</td>
</tr>
<tr>
<td>Venezuela</td>
<td>Cada Familia Una Escuela</td>
<td>No</td>
</tr>
<tr>
<td>Vietnam</td>
<td>OLM</td>
<td>No</td>
</tr>
<tr>
<td>Zambia</td>
<td>e-Learning portal</td>
<td>No</td>
</tr>
<tr>
<td>Zambia</td>
<td>Smart Revision</td>
<td>No</td>
</tr>
</tbody>
</table>

Only nine government EdTech products—Edu.ar (Argentina), CBC Kids (Canada), PBS Learning (Canada), Ghana Library App (Ghana), Rumah Belajar (Indonesia), South Africa’s Ministry of Education website (South Africa), EBS (Republic of Korea), KERIS edunet (Republic of Korea), and Wedorang (Republic of Korea)—disclosed in their privacy policies that they collect and use students’ data for advertising. Of these, four government products—Rumah Belajar, the Education Ministry of South Africa’s own website, CBC Kids, and Ghana Library App—explicitly disclosed that they use their students’ data for behavioral advertising purposes.
Furthermore, Human Rights Watch identified 22 government EdTech products that failed to offer any privacy policy at all, thus keeping their students in the dark about how their governments were handling their intimate data and their privacy.

In contrast, only eight government-built products were found to protect children’s data by not installing any tracking technologies. These were: Juana Manso (Argentina), Biblioteca Digital Escolar (Chile), Jules, MaSpéMaths, and Ma classe à la maison (France), mebis (Germany: Bavaria), NHK for Schools (Japan), and TelmidTICE (Morocco). While few in number, these nine products demonstrate that it is possible for governments to uphold their obligation to protect and promote children’s rights by building and offering digital educational services to children that do not compromise their data and their privacy.

Case Study: Zambia

Children with access to connectivity and capable devices, or whose families made sacrifices to ensure their access, relied on EdTech to attend school online during the pandemic. The economic incentives to monetize their captive attention were illustrated in Zambia, a country which legally guarantees free basic education to every child and has committed to provide free and compulsory primary and secondary education, or grades 1 to 12, in its national education plans.321

Human Rights Watch found that the Zambian government charged primary and secondary students for the online education it provided during Covid-19 school closures. On April 20, 2020, Zambia’s Ministry of General Education launched two websites: the first, e-Learning Portal, offered courses in core subjects for students grades 7 to 12; the second, Smart Revision, provided practice tests to help students in grades 7, 9, and 12 prepare for national examinations.322

Both websites required children to pay a monthly subscription fee before they could access learning content. Each course on e-Learning Portal costed ZMW 5 (US$0.26), although students were nudged by the website’s design toward subscription bundles that were progressively more expensive at higher grades.323 For example, the website advertised the option to “Subscribe To All At K35 Only” (at a cost of US$1.84) for students in grades 10-12, even though only three subjects were available to take—Biology, Chemistry, and Mathematics—that would have costed much less to purchase separately.324 Smart Revision featured similarly tiered pricing, and charged a monthly fee of ZMW 10 (US$0.53) for students in grade 7, ZMW 20 (US$1.06) for grade 9 students, and ZMW 30 (US$1.58) for students in grade 12.325

---


These fees constituted a direct cost and a financial barrier to education, in addition to the high costs of internet access and devices that students and their families had to pay for before they could even access either of the government’s websites. Access to the internet in Zambia is prohibitively expensive for many, especially for the poorest children and those living in rural areas. According to the Inclusive Internet Index report, Zambia ranks 98 out of 120 countries surveyed in the cost of internet access relative to income. In 2015, 57.5 percent of Zambia’s population lived below the international poverty line of US$1.90 per day; poverty is estimated to have increased with widespread job losses and rising prices during the pandemic, making the internet even less affordable for most children and their families.

Human Rights Watch also detected e-Learning Portal transmitting its students’ personal data to PushEngage, a company offering push notification services “so you can unlock maximum revenue from each visitor,” and Tawk.to, a live chat service, even though the latter function was neither visible nor available for use on e-Learning Portal’s website. Human Rights Watch detected Smart Revision sending students’ personal data to Facebook.

For students relying on these websites to learn core content and prepare for high-stakes national examinations during Covid-19 school closures, submitting to these data practices was an indirect cost levied on them in exchange for their education.

The Zambian government, e-Learning Portal, PushEngage, and Smart Revision did not respond to a request for comment. Tawk.to and Facebook did not acknowledge Human Rights Watch’s finding that they were receiving data from either of these websites, or respond to questions about it.

No Choice

As noted in Chapter 3, this data collection and surveillance took place in virtual classrooms and educational settings where children could not reasonably object to such surveillance. Most government-built EdTech platforms did not allow their users to decline to be tracked; most of this surveillance happened secretly, without the child’s knowledge or consent. In such cases, it was impossible for children to opt out of such surveillance and data exploitation without opting out of school and giving up on formal learning altogether during the pandemic.

Some governments made it compulsory for students and teachers to use government-built EdTech platforms, not only subjecting them to the data practices and privacy protections—or lack thereof—of those products, but also making it impossible for children to protect themselves by opting for alternative means to access their right to education.

Teachers in Iran told Human Rights Watch that the government compelled those in public schools to use Shad, an app built by Iran’s Education Ministry for online learning during Covid-19. One teacher said: “The principal called and said that if I do not install the Shad app, I would be recorded as absent. The authorities do not accept teaching in Telegram and WhatsApp.… Students have also been told that if you are not in this app, your score will not be approved and will not be sent to the [school].” In October 2021, the Iranian government reported more than 18 million active users of Shad.
Technical analysis of Shad’s code by Human Rights Watch found that the app can collect children’s precise location data, the time of their current location, the child’s last known location, their Wi-Fi SSID, IP address, the child’s contacts, and any saved photos of their contacts.

Iran does not have a data protection law. A Personal Data Protection and Safeguarding Draft Act (“Draft Act”) was first proposed on July 26, 2018, and is still pending review from the Islamic Parliament of Iran as of September 2021; the Draft Act does not contain specific protections for children.333

In Turkey, one mother of a 9-year-old child, Rodin, told Human Rights Watch: “Rodin’s teacher forced all these 8-year-old kids to use Facebook. He made Rodin, who was 8 at the time, open a Facebook account, and told him to upload his homework there. Now, the teacher is forcing the kids to use Facebook when they’re taking tests.”334 Facebook’s terms of service prohibit children under 13 years old from using its services. 335

She continued, “The teacher also asked me to download BiP [a government-mandated messaging app for government and school use during the pandemic] to communicate with him. I’d heard that the app was not secure in terms of data privacy, so I said no. The teacher said, ‘Well, then you can’t communicate with me.’ I didn’t want to download the app, so I told him, ‘I don’t have space on my phone.’ The teacher said, ‘Well, you can’t communicate with me,’ and blocked us all on WhatsApp to prevent all parents from contacting him on secure apps. So, I haven’t been able to talk to him since.”336

As noted in Chapter 2, the Indian government offered Diksha, an app that claimed to deliver education to over 10 million students in the early days of the pandemic. To drive further adoption, some state-level education ministries set quotas for government teachers to compel a minimum number of students to download the app.337

Human Rights Watch found that Diksha collects children’s precise location data, including the time of their current location and their last known location. Human Rights Watch also observed Diksha collecting and transmitting children’s AAID to Google, which demonstrates that Diksha shares children’s personal data with Google for advertising purposes.

In these countries, children could not give valid, meaningful consent for the processing of their data by government-mandated EdTech platforms—even if they had been asked—because they could not refuse to use them freely without detrimental effect, and there were no alternative means to access their education.
Acknowledgments

This report was researched and written by Hye Jung Han, researcher and advocate in the children’s rights division at Human Rights Watch, who also conducted technical static analysis of all EdTech apps, technical analysis of EdTech websites, and data analysis of all EdTech products.

Technical analysis of EdTech websites was also conducted by Gabi Ivens, head of open source research at Human Rights Watch, and guided by Surya Mattu, Senior Data Engineer and Investigative Data Journalist of The Markup. We are particularly grateful to Surya Mattu for his work in building Blacklight, the real-time website privacy inspector built for The Markup, and for his generous assistance and invaluable insights in adapting the tool for Human Rights Watch’s website analysis.

Additional technical analysis—both static and dynamic—of eight EdTech apps was conducted by Esther Onfroy, founder of Defensive Lab Agency, who also conducted additional dynamic analysis and ran the data experiments with four children located in Indonesia, India, South Africa, and Turkey. We are extremely grateful to Esther Onfroy for her work, as well as for her generous technical advice and expertise.

Additional interviews were conducted by Marlene Auer, former associate, Europe and Central Asia (ECA); Martha Bernild, associate, Development and Global initiatives; Hanna Darroll, former senior associate, Development and Global Initiatives; Tayla Hall, senior coordinator, Development and Global Initiatives; Anjelica Jarrett, former coordinator, LGBT rights; Aya Majzoub, researcher, Middle East and North Africa (MENA); Devin Milroy, former associate, Global IT; Elin Martínez, senior researcher, children’s rights; Seung Kyung Noh, former senior associate, Operations; Catherine Pilishvili, senior coordinator, ECA; Marina Riera Rodoreda, former coordinator, International Justice; Anna Salami, officer, Development and Global initiatives; Kristen Scott, senior associate, Development and Global initiatives; Delphine Starr, former senior coordinator, children’s rights; Svetlana Stepanova, senior manager, Development and Global initiatives; Behrouz Tehrani, consultant, MENA; Agnes Tkotz, associate director, Development and Global initiatives; Nicole Tooby, officer, Asia; Frances Underhill, senior manager, Film Festival; and Tenzin Wangmo, officer, General Counsel.

This report was edited by Bede Sheppard, children’s rights deputy director at Human Rights Watch. Maria McFarland Sánchez-Moreno, senior legal advisor, and Tom Porteous, deputy program director, provided legal and program reviews. Expert reviews were provided by: Ilaria Allegrozzi, senior researcher, Africa; Jayshree Bajoria, senior researcher, Asia; Julia Bleckner, Asia researcher and health editor; Deborah Brown, senior researcher and advocate, technology and human rights; Eva Cossé, researcher, ECA; Farida Deif, Canada director; Corinne Dufka, associate director, Africa; Anietie Ewang, researcher, Africa; Elvire Fondacci, coordinator, France; Lydia Gall, senior researcher, ECA; Abir Ghattas, director, Information Security; Andreas Harsono, senior researcher, Asia; Saroop Ijaz, senior researcher, Asia; Paula Ini, senior research assistant, Americas; Gabi Ivens, head of open source research; Teppel Kasai, officer, Asia; Chloe King, researcher, MENA; Anastasila Kruope, assistant researcher, ECA; Linda Lakhdhir, legal advisor, Asia; Elin Martínez, senior researcher, children’s rights; Tyler Mattiace, researcher, Americas; Sophie McNeill, researcher, Asia; Santiago Menna, research assistant, Americas; César Muñoz, senior researcher, Americas; Otsieno Namwaya, senior researcher, Africa; Juan Pappier, senior researcher, Americas; Laura Pitter, deputy director, United States; Sunai Phasuk, senior researcher, Asia; Martina Rapido Ragozzino, senior research assistant, Americas; Kartik Raj, researcher, ECA; Mihra Rittmann, senior researcher, ECA; Tara Sepehri Far, senior researcher, MENA; Mary Smith, researcher, Asia; Judith Sutherland, associate director, ECA; Tamara Taraciuk Broner, acting director, Americas; Nathalye Cotrino Villarreal, senior research assistant, Americas; Maya Wang, senior researcher, Asia; Belkis Wille, senior researcher, crisis and conflict; Lina Yoon, senior researcher, Asia; and Hiba Zayadin, senior researcher, MENA.
Acknowledgments

Additional colleagues provided expert review for this report but are not named here for security reasons.

We are grateful to Esther Onfroy and Surya Mattu for providing external expert technical review.

External legal review was provided by Elizabeth Wang, founder of Elizabeth Wang Law Offices.

Sakae Ishikawa, senior video editor at Human Rights Watch, Liliana Patterson, senior editor, and Christina Curtis, multimedia deputy director, produced and edited one of the accompanying videos. Priya Sanghvi, content and production strategist, managed the production of a second accompanying video, which was produced and edited by Alejandro Norman, Patrick Scerri, Andrea Devia-Nuño, Erik Righetti, Hanna Lau-Walker, and Min Liu at Hero Studios.

Production assistance was provided by Katherine La Puente, associate, children’s rights; Travis Carr, senior publications coordinator; and Fitzroy Hepkins, senior administrative manager. Content strategy, branding, and design was provided by Deroy Peraza, Izabella Stern, Lauren Jones, Pauline Shin, and Rima Desai of Hyperakt; and illustration was provided by Andrea Devia-Nuño at Hero Studios. Design direction and operational support was provided by Grace Choi, director of publications and information design; Les Lim, developer; and Christina Rutherford; senior digital manager.

The campaign supporting this project was led by Amanda Alampi, deputy director, Campaigns and Public Engagement; Ziva Luddy Juneja, acting digital campaigner; Bronte Price, digital engagement strategist; Nailah Ali, senior graphic designer, public engagement; and supported by Andrea Zita, associate; and Naimah Hakim, senior coordinator. Emma Daly, head of the Collaboratory, provided support and guidance.

We thank the four children and their parents who were willing to test out specific EdTech apps recommended by their government in order to verify our findings, and shared their stories with us.

Human Rights Watch thanks the Novo Nordisk Foundation for their support of this project.
“How Dare They Peep into My Private Life?”

Children’s Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic

“How Dare They Peep into My Private Life?: Children’s Rights Violations by Governments that Endorsed Online Learning during the Covid-19 Pandemic,” is a global investigation of the education technology (EdTech) endorsed by 49 governments for children’s education during the pandemic. Based on technical and policy analysis of 164 EdTech products, Human Rights Watch finds that the majority of these online learning platforms put at risk or infringed upon children’s privacy and other rights, for purposes unrelated to their education.

These products monitored children, harvesting personal data such as who they are, where they are, what they do in the classroom, who their family and friends are, and what kind of device their families could afford for them to use. Children, parents, and teachers were largely kept in the dark about these data surveillance practices.

The report finds that governments failed to protect children’s right to education. By endorsing and enabling the wide adoption of EdTech products without adequate safeguards or oversight, governments offloaded the true costs of providing online education onto children, who were unknowingly forced to pay for their learning with their rights to privacy and access to information, and potentially their freedom of thought.

Children’s reliance on digital services that enable their education will likely continue long after the end of the pandemic. Governments should adopt modern child data protection laws to protect children online. Companies should immediately stop collecting, processing, and sharing children’s data in ways that risk or infringe on their rights.