Read Me

Methodology,
Technical Evidence

Context

The Human Rights Watch report, "'How Dare They Peep into My Private Life?': Children's Rights Violations by Governments that Endorsed Online Learning during the Covid-19 Pandemic," covers 49 countries that recommended 163 educational technology (EdTech) products for children to use for online learning during Covid-19 school closures.

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.

A detailed methodology can be found in the report.

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 εxodus by εxodus 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 εxodus 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.

For readers looking to recreate Human Rights Watch's static analysis for apps, please refer to the relevant privacy snapshot to find the version of the app analyzed by Human Rights Watch and its release date.

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. The technical evidence found in this data repository are results generated by Blacklight for the websites covered in the research.

Blacklight emulates how a user might be surveilled while browsing the web. 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.

Blacklight exists in two formats: as a user-friendly interface on The Markup's website, and as an open source command-line tool. 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.

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.

Blacklight results are unavailable for four websites—Distance Learning (Cameroon), Eduyun (China), Smart Revision (Zambia), and e-learning portal (Zambia)—as the 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. As a result, Human Rights Watch conducted manual analysis of these four websites, following the same methodology used by Blacklight. Please refer to the respective privacy snapshot for the date of Human Rights Watch's analysis.