Moscow Electronic School

(“Московская электронная школа”)

Recommended by:
Russia

Developer's Description:

[translation] “Moscow Electronic School" is a combination of educational activities with information technology, which improves the learning process of children [...].”[1]

Information

Type: App, Website

Apparently designed for children? Yes

Developer: Government

Analyzed by Human Rights Watch

Version: v.2.24.0

Release date: February 20, 2021

Estimated users[2]**:** 100,000+

URL at the time of analysis:
Link 1, Link 2

Was there a publicly available privacy policy at the time of analysis? Yes. Link

HUMAN RIGHTS WATCH

STUDENTS NOT PRODUCTS

Website Analysis

This website collected and sent the following data about users to third-party companies[3]**:**

To track the user | 4 ad trackers sent data about users to third-party companies

2 ad trackers sent users' data to **Facebook** through the domains facebook.com, facebook.net
1 ad tracker sent users' data to **Mail.Ru Group OOO** through the domain vk.com
1 ad tracker sent users' data to **Yandex** through the domain yandex.ru

To watch and record the user

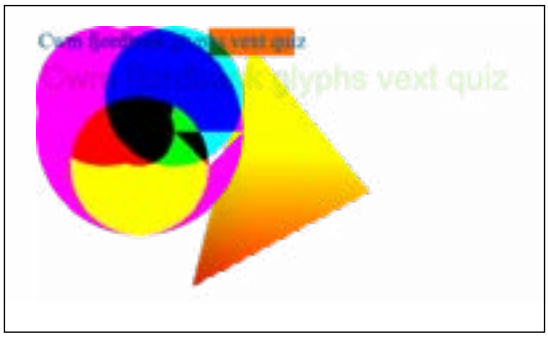
This site used **session recording** to record what users did on this website, including clicks and mouse movements around the page, and sent the recording to **Yandex t**hrough the domains mc.yandex.ru/webvisor, mc.yandex.ru/metrika/watch.js, mc.yandex.ru/metrika/tag.js

To capture what users type, before they hit send

This site used **key logging** to capture text typed by users, before they hit send, and sent it to **Yandex** through the domain yandex.ru

To find out who the user is

This site used **canvas fingerprinting** to identify users and their online behavior by invisibly drawing the following image and text on their browsers, and sending their data to the **Mayor of Moscow's Office, mos.ru,** through the domain https://stats.mos.ru/ss2.min.js



To track the user across the internet

Third-party cookies were not detected on this site.

1 Translation provided by Google Translate. See: Moscow Electronic School, “What is Moscow Electronic School?” (“Что такое Московская электронная школа?”) https://web.archive.org/web/20211103003530/https://school.mos.ru/help/stats/whatismes/ (accessed November 2, 2021)

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

3 A technical analysis does not definitively determine the intent of any particular tracking technology, or how the collected d``ata is used. For example, an EdTech product can include third-party tracking 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 for advertising or other marketing purposes.

This website collected and sent users' data through these tracking technologies:

Facebook Pixel[4] | was detected on this site sending data about users to Facebook. This allows this website to later target its users with ads on Facebook and Instagram. Facebook can also retain and use this data for its own advertising purposes.

Google Analytics' 'remarketing audiences' | was not detected on this site.

App Analysis (static)

This app did not include code that has the capability to collect the following personal data[5]:

To find out who the user is:
This app does not collect users' persistent identifiers.

To track where the user is:
This app does not collect users' location data.

To track who the user knows, and with whom they talk:
This app does not collect contacts' information, phone number, call or SMS logs.

To track what the user does:
This app does not access users' camera or microphone.

This app requested access to the following sensitive data on the user's device[6]:

"Dangerous" (as defined by Android) Permissions requested:

READ_EXTERNAL_STORAGE
WRITE_EXTERNAL_STORAGE
SYSTEM_ALERT_WINDOW

This app embedded the following third-party code, which the app may permit to collect and send users' data to that third-party company[7]:

2 Software Development Kits (SDKs) were found embedded in this app.

Google Firebase Analytics
Google CrashLytics

---

4 Facebook rebranded itself to Meta in October 2021. This privacy profile refers to Facebook as both the platform and the parent company, for consistency across the timeline of Human Rights Watch's investigation.

5 As noted in the report, this type of analysis observes whether the code is capable of collecting specific types of personal data, but not whether it is being collected, or how it is being used. Put another way, an app may not use all of the programmed functionalities of which it is capable.

6 Android labels permissions as "dangerous" when granting that permission to an app can "potentially affect the user's privacy or the device's normal operation," because the app "wants data or resources that involve the user's private information, or could potentially affect the user's stored data or the operation of other apps." 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. See: Android Developers, "Permissions overview," May 7, 2020, https://web.archive.org/web/20200712090715/https://developer.android.com/guide/topics/permissions/overview (accessed April 24, 2022).

7 Human Rights Watch does not conclusively determine whether, or how, any given SDK is used by a specific app, and notes that some SDKs may provide multiple capabilities in addition to advertising.