Stoodi

Recommended by:
Brazil: São Paolo

Developer's Description:

[translation] "Stoodi is the only platform that organizes your daily life and tells you exactly what to study until ENEM. We help you maintain a study routine. We provide video lessons, exercises and summaries in the most organized way for every moment of your study journey."[1]

Information

Type: App, Website

Apparently designed for children? Yes

Developer: Stoodi Ensino e Formação à Distancia SA

Analyzed by Human Rights Watch

Version: v. 2.2.3

Release date: February 19, 2021

Estimated users[2]**:** 1,000,000+

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

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

Website Analysis

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

To track the user | 24 ad trackers sent data about users to third-party companies

3 ad trackers sent users' data to **Google** through the domains google-analytics.com, double-click.net, googleadservices.com, googletagmanager.com, youtube.com
2 ad trackers sent users' data to **Facebook** through the domains facebook.com, facebook.net
2 ad trackers sent users' data to **Mixpanel** through the domains mixpanel.com, mxpnl.com
2 ad trackers sent users' data to **Datadog** through the domains datadoghq-browser-agent.com, datadoghq.com
1 ad tracker sent users' data to **Microsoft** through the domain bing.com
1 ad tracker sent users' data to **Crazy Egg** through the domain crazyegg.com
1 ad tracker sent users' data to **Cloudflare** through the domain cloudflareinsights.com
1 ad tracker sent users' data to **Hotjar** through the domain hotjar.com
1 ad tracker sent users' data to **The Nielsen Company** through the domain exelator.com
1 ad tracker sent users' data to **Optomaton UG (haftungsbeschränkt)** through the domain volvelle.tech
1 ad tracker sent users' data to **RudderLabs** through the domain rudderlabs.com
1 ad tracker sent users' data to **Sales Analytics** through the domain salesanalytics.io
1 ad tracker sent users' data to **omguk.com** through the domain omguk.com
1 ad tracker sent users' data to **rtb123.com** through the domain rtb123.com
1 ad tracker sent users' data to **Awin** through the domain dwin1.com
1 ad tracker sent users' data to **Kenshoo TLD** through the domain xg4ken.com
1 ad tracker sent users' data to **Ve Global** through the domain veinteractive.com

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 **Hotjar** through the domains script.hotjar.com, static.hotjar.com

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 **Ve Global** through the domain veininteractive.com[4], and to **Stoodi** through stoodi.com.br.

1 Translation provided by Google Translate. See: Stoodi, "Stoodi," https://web.archive.org/web/20210313235601/https://www.stoodi.com.br/ (accessed March 13, 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 data 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.

4 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.

To find out who the user is

Canvas fingerprinting was not detected on this site.

To track the user across the internet | 21 third-party cookies were found on this site that tracked users across the internet

15 cookies sent users' data to **Pipefy** through the domains pipefy.com, app.pipefy.com
3 cookies sent users' data to **Google** through the domains doubleclick.net, youtube.com
2 cookies sent users' data to **Microsoft** through the domains bing.com, bat.bing.com
1 cookie sent users' data to **Ve Global** through the domain veinteractive.com

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

Facebook Pixel[5] **|** 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 detected on this site sending data about users to Google. This allows this website to target its users with ads across the internet.

5 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.

App Analysis (static)

This app included code that has the capability to collect the following personal data[6]:

To find out who the user is:
Android Advertising ID
IMEI

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[7]:

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

READ_EXTERNAL_STORAGE
WRITE_EXTERNAL_STORAGE
READ_PHONE_STATE

This app embedded the following third-party code, which the app may permit to collect and send users' data to that third-party company[8]:

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

Google Crashlytics

Google Firebase Analytics

Google Tag Manager

Google Analytics

Facebook Analytics

Facebook Login

Facebook Share

Segment

---

6 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.

7 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).

8 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.