Website Analysis

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

To track the user | 30 ad trackers sent data about users to third-party companies
---
6 ad trackers sent users’ data to Google through the domains google-analytics.com, double-click.net, googletagmanager.com, googleadservices, googleoptimize.com, youtube.com
2 ad trackers sent users’ data to Facebook through the domain facebook.com, facebook.net
3 ad trackers sent users’ data to Microsoft through the domains adsymptotic.com, licdn.com, bing.com
2 ad trackers sent users’ data to Criteo through the domain criteo.com, criteo.net
2 ad trackers sent users’ data to Hubspot through the domain hubspot.com, hs-analytics.net
2 ad trackers sent users’ data to Mixpanel through the domain mixpanel.com, mxpnl.com
2 ad trackers sent users’ data to Twitter through the domain twitter.com, t.co
1 ad tracker sent users’ data to WarnerMedia through the domain adnxs.com
1 ad tracker sent users’ data to Hotjar through the domain hotjar.com
1 ad tracker sent users’ data to OneSignal through the domain onesignal.com
1 ad tracker sent users’ data to Pinterest through the domain pinterest.com
1 ad tracker sent users’ data to Wingify through the domain visualwebsiteoptimizer.com
1 ad tracker sent users’ data to TikTok through the domain tiktok.com
1 ad tracker sent users’ data to Awin through the domain dwin1.com
1 ad tracker sent users’ data to getblue through the domain getblue.io
1 ad tracker sent users’ data to IP-API through the domain ip-api.com
1 ad tracker sent users’ data to Reyp through the domain omappapi.com
1 ad tracker sent users’ data to rtb123.com through the domain rtb123.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

Key logging was not detected on this site.

To find out who the user is

Canvas fingerprinting was not detected on this site.

---
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.
To track the user across the internet | 19 third-party cookies were found on this site that tracked users across the internet

10 cookies sent users’ data to **Microsoft** through the domains linkedin.com, ads.linkedin.com, bing.com, bat.bing.com
3 cookies sent users’ data to **Google** through the domains doubleclick.net, youtube.com
2 cookies sent users’ data to **WarnerMedia** through the domain adnxs.com
1 cookie sent users’ data to **Twitter** through the domain twitter.com
1 cookie sent users’ data to **getblue** through the domain getblue.io
1 cookie sent users’ data to **Meu Dim Dim** through the domain track.meudimdim.com.br
1 cookie sent users’ data to **Enviou** through the domain life.enviou.com.br

---

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

**Facebook Pixel** | 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.

---

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.
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.

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).

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.

---

**App Analysis (static)**

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

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

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

- To track what the user does:
  - Camera

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

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

- READ_EXTERNAL_STORAGE
- WRITE_EXTERNAL_STORAGE
- CAMERA

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

- Google Crashlytics
- Google Firebase Analytics
- Google AdMob
- Facebook Analytics
- Facebook Login
- Facebook Places
- Facebook Share
- MixPanel

---

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.