Android Data Collection

This article addresses the manner in which Android phones share personal user information with Google, usually in a complete user unaware and unapproved way, and the legal consequences Google has endured for deceptive practices in users' location tracking.

Background [edit | edit source]

Android, the global top mobile operating system,[1] is used to power billions of devices globally. Tests have shown that Android phones with Google services transmit user data to Google on multiple occasions even when users try to restrict sharing of data via settings. This has encouraged increasing alarm over user privacy, transparency, and personal data control.

A study found that data collection happens without any chance to opt out even before the user has even opened their first app.[2]

Moreover, most phone vendors do their own tracking on top and pre-install so-called bloatware in exchange for payment from the respective company, such as social media and shopping apps (Facebook, TikTok, Aliexpress, eBay, ...), which transmit data in the background without user consent even if the apps are never even opened and the user never agreed to their TOS.[3]

Data sharing with Google [edit | edit source]

A research examined the frequency of data sharing between Google and Android phones with Google services.[4] The research showed that even if an Android phone is set to minimal setting and left on its own, it shares data with Google on average every 4.5 minutes. The shared data includes sensitive information like:

- IMEI (International Mobile Equipment Identity)
- Hardware serial number
- SIM serial number and IMSI (International Mobile Subscriber Identity)
- Handset phone number

In addition, Google services on Android sends telemetry data to Google even when customers directly decline to have their data collected. For instance, each time a SIM card is inserted into the device, Google services sends its information to Google automatically.

Data exchanged with Google by Google Messages and Google Dialer applications on an Android smartphone was also researched.[5] These applications report to Google whenever messages are being sent/received or calls are being received/made. Precisely:

- Google Messages sends a message text hash so Google can match the sender and receiver in a message exchange.
- Google Dialer also transmits call time and call duration to Google for linking both devices for a call.
- Both of the apps forward phone numbers to Google.
- Both user interaction timing and duration with both apps are also forwarded to Google in addition to the above.

No exemption option exists in the data transmission. Data comes through two pathways:

1. The Google Play Services Clearcut logger.
2. Google/Firebase Analytics.

Location History Lawsuit [edit | edit source]

Google misled some Android users into thinking that the setting titled "Location History" was the only Google account setting that affected whether the company collected, kept and used personally identifiable data about their location. In fact, another account setting titled "Web & App Activity" also enabled Google to collect, store and use personally identifiable location data when it was turned on, and that setting was turned on by default.

For this, Google was sued in the United States[6] and in Australia.[7]

Privacy respecting alternatives [edit | edit source]

Not many alternatives are available to users for completely avoiding this data sharing. Attempts to disable data collection via settings, Android integration with Google services does make it impossible to fully discontinue the passing on of person and device details.[4]

The use of custom ROMs or privacy-focused applications, do cut down on sharing data, these are likely to require technical know-how and are not necessarily in the hands of the average user.

In general, Google services which are the source of most of the data collection serve two functions:

1. Application dependencies, like network location services, debugging tooling, advertising services etc.
2. Application distribution

A privacy replacing alternative should therefore have an alternative for these functions.

Perhaps the only Google -free alternate configuration comprises of MicroG applications, which is an open source reimplementation of Google services. It provides necessary dependencies so that most of the applications which depend on Google services can function on a device without those Google services.

As for application distribution, few alternate channels, such as F-droid and Aurora Store exists.

Murena, Fairphone and Iodé sells devices pre-installed with de-googled Android based on LineageOS and MicroG, making privacy friendly Android phones accessible to non-technical users. However, the operating system called /e/ on Murena devices has a history of not always addressing security vulnerabilities in a timely manner[8]. However the situation is still much better than the millions of phones in active use that no longer get manufacturer support.

References [edit | edit source]

1. ↑ "Mobile Operating System Market Share Worldwide". *StatCounter*. Retrieved 15 Mar 2025.
2. ↑ Jones, Connor (4 Mar 2025). "How Google tracks Android device users before they've even opened an app". *The Register*. Retrieved 2025-03-05.
3. ↑ Trinity College Dublin (October 11, 2021). "Study reveals scale of data-sharing from Android mobile phones". *TechXplore*. Retrieved 2025-03-05.
4. ↑ 4.0 4.1 Leith, Douglas J. (25 Mar 2021). "Mobile Handset Privacy: Measuring The Data iOS and Android Send to Apple And Google" (PDF). Retrieved 15 Mar 2025.
5. ↑ Leith, Douglas J. (28 Feb 2022). "What Data Do The Google Dialer and Messages Apps On Android Send to Google?" (PDF). Retrieved 15 Mar 2025.
6. ↑ Gatlan, Sergiu (14 Nov 2022). "Google will pay $391M to settle Android location tracking lawsuit". *BleepingComputer*. Retrieved 15 Mar 2025.
7. ↑ "Google LLC to pay $60 million for misleading representations". *ACCC*. 12 Aug 2022. Retrieved 15 Mar 2025.
8. ↑ Duval, Gael (Sep 2023). "Some clarification regarding security vs privacy in /e/OS". *e*. Retrieved 15 Mar 2025.

Categories: Android | Data collection