Dangerous Permissions

Location Tracking

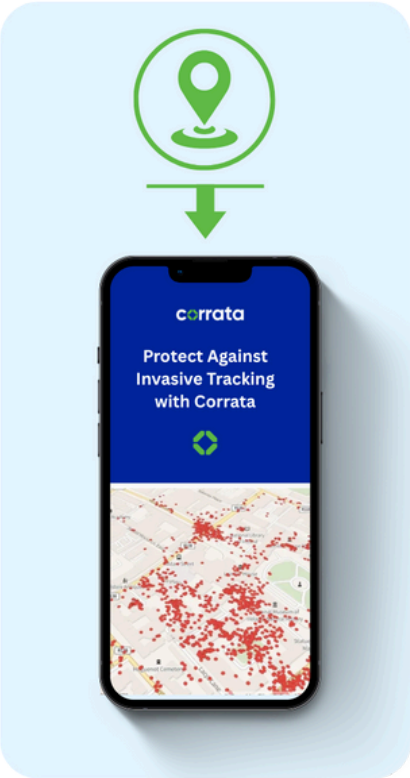
One of the most insidious aspects of the mobile advertising ecosystem is how app vendors exploit end-user trust. Apps that provide useful services often request a wide range of permissions - many only loosely connected to the app's core function - in order to harvest detailed data on user behavior.

The most egregious example is the monetization of GPS-level location data. Below we outline how this happens and how Corrata helps prevent employees from unknowingly sharing their movements in the so-called "data economy."

How Users Surrender Their Privacy

A wide variety of apps request access to device location, often under the guise of delivering a better experience. For example, a browser might claim to improve search results by using your current location. Yet in many cases, location data adds little real value to the user. Outside of location-centric apps like navigation, the benefit is negligible.

For app vendors, however, location data is highly lucrative. By collecting frequent "pings" and combining them with data from other apps and brokers, they can build a detailed picture of an individual's movements. This becomes even easier when background location tracking is enabled - recording a user's movements even when the app is not in use. While intended only for legitimate cases like navigation or exercise tracking, in practice this capability is often misused.



87%

percent of Android apps and 60% of iOS apps requested permissions that were not needed for their functions.

Source: NordVPN study 2023

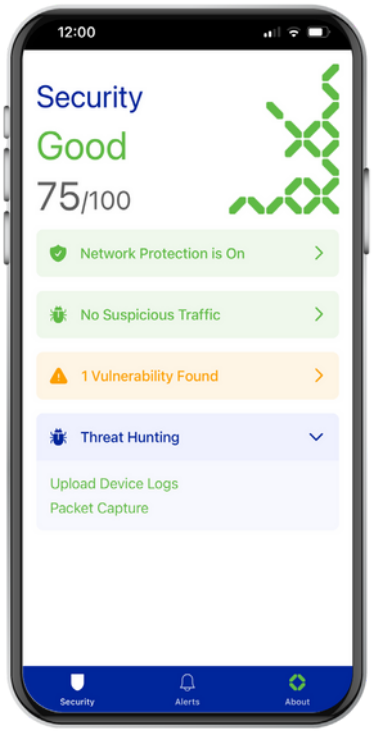
Protecting Against Invasive Tracking with Corrata

- You cannot rely on employees to always make the right choices when granting app permissions. Corrata provides technical safeguards to drastically reduce the risk of location data leakage.

- Our solution scans all apps on an employee's device to identify those with background location tracking enabled - part of a category of app permissions we classify as potentially dangerous.

- Once detected, Corrata alerts the user, and if the issue is not addressed, can quarantine the device until action is taken. Apps with a legitimate need for background location (e.g., navigation tools with strong privacy protections) can be allow-listed to prevent false positives.

- By giving organizations visibility of background location tracking, Corrata can ensure both the privacy and safety of employees and ensure that their location history never falls into the wrong hands.



CYBER|IRELAND
IRELAND'S CYBER SECURITY CLUSTER

FIRSTNET™
Built with AT&T

Member of
Microsoft Intelligent Security Association
Microsoft Security

corrata

Corrata provides endpoint threat detection and response for mobile devices. Our unique patented on-device technology delivers unprecedented visibility and protection, one-click deployment and the device experience and privacy employees expect. Corrata has customers across multiple verticals including healthcare, logistics, manufacturing and the public sector. Corrata is a proud member of the Microsoft Intelligent Security Association and Cyber Ireland and is verified for use with FirstNet, the US Government network for first responders powered by AT&T.

corrata.com