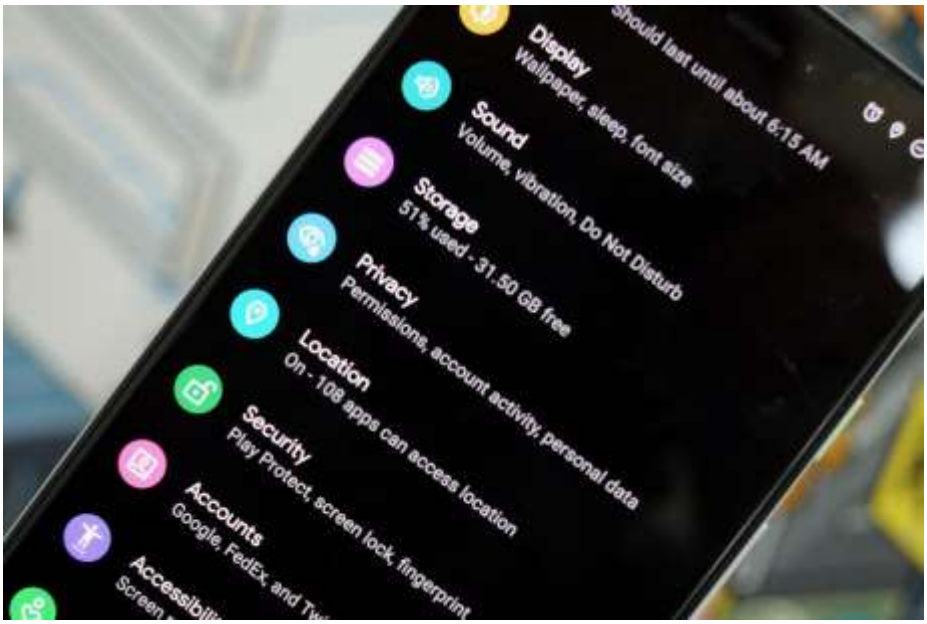
More than 1,000 Android apps harvest data even after you deny permissions

cnet.com/news/more-than-1000-android-apps-harvest-your-data-even-after-you-deny-permissions/

The apps gather information such as location, even after owners explicitly say no. Google says a fix won't come until Android Q.



More than 1,000 Android apps have been circumventing privacy permission settings, researchers found. Jason Cipriani/CNET

Permissions on Android apps are intended to be gatekeepers for how much data your device gives up. If you don't want a flashlight app to be able to read through your call logs, you should be able to deny that access. But even when you say no, many apps find a way around: Researchers discovered more than 1,000 apps that skirted restrictions, allowing them to gather precise geolocation data and phone identifiers behind your back.

The discovery highlights how difficult it is to stay private online, particularly if you're attached to your phones and mobile apps. Tech companies have mountains of personal data on millions of people, including where they've been, who they're friends with and what they're interested in.

Lawmakers are attempting to reel that in with privacy regulation, and app permissions are supposed to control what data you give up. Apple and Google have released new features to improve people's privacy, but apps continue to find hidden ways to get around these protections.

Researchers from the International Computer Science Institute found up to 1,325 Android apps that were gathering data from devices even after people explicitly denied them permission. Serge Egelman, director of usable security and privacy research at the ICSI, presented the study in late June at the Federal Trade Commission's PrivacyCon.

"Fundamentally, consumers have very few tools and cues that they can use to reasonably control their privacy and make decisions about it," Egelman said at the conference. "If app developers can just circumvent the system, then asking consumers for permission is relatively meaningless."

Egelman said the researchers notified Google about these issues last September, as well as the FTC. Google said it would be addressing the issues in Android Q, which is expected to release this year.

The update will address the issue by hiding location information in photos from apps and requiring any apps that access Wi-Fi to also have permission for location data, according to Google.

The study looked at more than 88,000 apps from the Google Play store, tracking how data transferred from the apps when they were denied permissions. The 1,325 apps that violated permissions on Android used workarounds hidden in its code that would take personal data from sources like Wi-Fi connections and metadata stored in photos.

Researchers found that Shutterfly, a photo-editing app, had been gathering GPS coordinates from photos and sending that data to its own servers, even when users declined to give the app permission to access location data.

Fundamentally, consumers have very few tools and cues that they can use to reasonably control their privacy and make decisions about it.
Serge Egelman, director at the International Computer Science Institute

A Shutterfly spokeswoman said the company would only gather location data with explicit permission, despite what researchers found.

"Like many photo services, Shutterfly uses this data to enhance the user experience with features such as categorization and personalized product suggestions, all in accordance with Shutterfly's privacy policy as well as the Android developer agreement," the company said in a statement.

Some apps were relying on other apps that were granted permission to look at personal data, piggybacking off their access to gather phone identifiers like your IMEI number. These apps would read through unprotected files on a device's SD card and harvest data they didn't have permission to access. So, if you let other apps access personal data, and they stored it in a folder on the SD card, these spying apps would be able to take that information.

While there were only about 13 apps doing this, they were installed more than 17 million times, according to the researchers. This includes apps like Baidu's Hong Kong Disneyland park app, researchers said.

Baidu and Disney didn't respond to requests for comment.

There are 153 apps that have that capability, researchers found, including Samsung's Health and Browser apps, which are installed on more than 500 million devices.

Samsung didn't respond to a request for comment.

Other apps were gathering location data by connecting to your Wi-Fi network and figuring out the router's MAC address. They found this on apps that functioned as smart remote controls, which didn't need your location information to function.

Egelman said he will be releasing details with a list of the 1,325 apps the researchers discovered when he presents the study at the Usenix Security conference in August.