www.eff.org /deeplinks/2022/05/how-disable-ad-id-tracking-ios-and-android-and-why-you-should-do-it-now

How to Disable Ad ID Tracking on iOS and Android, and Why You Should Do It Now

Bennett Cyphers ⋮ 8-10 minutes ⋮ 5/11/2022

The ad identifier - aka “IDFA” on iOS, or “AAID” on Android - is the key that enables most third-party tracking on mobile devices. Disabling it will make it substantially harder for advertisers and data brokers to track and profile you, and will limit the amount of your personal information up for sale.

This post explains the history of device ad identifiers and how they have enabled persistent tracking, identification, and other privacy invasions.

But first things first. Here’s how to revoke tracker access to your ad ID right now:

On Android

With the release of Android 12, Google began allowing users to delete their ad ID permanently. On devices that have this feature enabled, you can open the **Settings** app and navigate to **Privacy** > **Ads**. Tap “**Delete advertising ID**,” then tap it again on the next page to confirm. This will prevent any app on your phone from accessing it in the future.

The Android opt out should be available to most users on Android 12, but may not available on older versions. If you don't see an option to "delete" your ad ID, you can use the older version of Android's privacy controls to reset it and ask apps not to track you, shown below:

Source

On iOS

Apple requires apps to ask permission before they can access your IDFA. When you install a new app, it may ask you for permission to track you.

Source

Select “**Ask App Not to Track**” to deny it IDFA access.

To see which apps you have previously granted access to, go to **Settings** > **Privacy** > **Tracking**. The menu should look like this:

Here you can disable tracking for individual apps that have previously received permission. Only apps that have permission to track you will be able to access your IDFA.

You can set the “**Allow apps to Request to Track**” switch to the “**off**” position (the slider is to the left and the background is gray). This will prevent apps from asking to track in the future. If you have granted apps permission to track you in the past, this will prompt you to ask *those* apps to stop tracking as well. You also have the option to grant or revoke tracking access on a per-app basis.

Apple has its own targeted advertising system, separate from the third-party tracking it enables with IDFA. To disable it, navigate to **Settings** > **Privacy** > **Apple Advertising**:

Source

Set the “**Personalized Ads**” switch to the “**off**” position to disable Apple’s ad targeting.

History

In the early days of smartphones, trackers used static device identifiers - the “Unique Device Identifier” (UDID) on iOS, and the “Android ID” on Android - to track users across apps. These identifiers were unique, permanent, and were frequently accessed by third parties without user knowledge or consent.

This was rightfully considered a problem for user privacy. A 2010 investigation by the Wall Street Journal exposed the extent of the issue, and in 2011, after a series of probing questions from US members of congress, Apple began restricting access to the UDID.

The industry had already begun to rely on data collection tied to UDID, and trackers scrambled to adapt to the change. Then, in 2012, Apple quietly introduced the Identifier for Advertisers (IDFA). IDFA was almost identical to the UDID it replaced: it was a globally unique identifier that was available to all apps by default. The biggest difference was that IDFA could be reset -- though this was only possible if users knew what to look for. Apple also allowed users to enable a setting called “Limit Ad Tracking.” This sent a signal to apps asking them not to track, but it did not actually affect the apps’ ability to access IDFA.

Android followed suit in 2013, introducing the Android Advertising Identifier (AAID). Like Apple, Google made its identifier available to all apps by default, without any special permission. It also allowed users to reset their ad identifier, but not restrict access to it or delete it.

In 2016, Apple updated Limit Ad Tracking to set the IDFA to a string of zeroes - effectively deleting it. This meant that for the first time, users had an effective, technical opt-out of IDFA tracking.

In 2021, Apple introduced App Tracking Transparency (ATT), which requires apps to get affirmative consent before they can track users with IDFA or any other identifier. This had an enormous impact on the tracking industry. While previously, about 20% of users chose to opt out of tracking (meaning 4 out of 5 were “opted in”), after the change, the vast majority of users have chosen *not* to allow tracking. Defaults matter.

Meanwhile, Android finally started rolling out a way for users to disable their ad ID.As of April 1, 2022, Android also requires developers to request a separate permission in order to access the ad ID. However, this is treated as a “normal” permission, meaning users don’t see any pop-up asking for their consent. Despite the ad ID’s central role in enabling third-party tracking, the developer documents explain that this kind of permission is for data that presents “very little risk to the user's privacy.” In other words, Android’s ad ID is still exposed on an opt-out basis, and users have to go out of their way to defend their privacy on the platform.

In February, Google also indicated that it may eventually phase out the ad ID altogether. It plans to bring a version of the Privacy Sandbox framework to mobile devices to support behavioral advertising “without reliance on cross-app identifiers.” But Google assured developers that it won’t change anything substantial about the ad ID for “at least two years.”

Why It Matters

The ad identifier is a string of letters and numbers that uniquely identifies your phone, tablet, or other smart device. It exists for one purpose: to help companies track you.

Third-party trackers collect data via the apps on your device. The ad ID lets them link data from different sources to one identity you. In addition, since every app and tracker sees the same ID, it lets data brokers compare notes about you. Broker A can buy data from broker B, then use the ad identifier to link those two datasets together. Simply, the ad ID is the key that enables a whole range of privacy harms: invasive 3rd-party profiling by Facebook and Google, pseudoscientific psychographic targeting by political consultants like Cambridge Analytica, and location tracking by the U.S. military.

Sometimes, participants in the data pipeline will argue that the ad ID is anonymous or pseudo-anonymous, not “personally identifying” information, and imply that it does not pose a serious privacy threat. This is not true in practice. First, the ad ID is commonly used to help collect data that is obviously personally identifiable, like granular location data. If you can see where a person works, sleeps, studies, socializes, worships, and seeks medical care, you don’t need their email address to help identify them. And second, an entire industry exists to help trackers link ad IDs to more directly identifying information, like email addresses and phone numbers. In a vacuum, the ad ID may be anonymous, but in the context of the tracking industry, it is a ubiquitous and effective identifier.

Disabling this ID makes it substantially harder for most advertisers and data brokers to track you. These industries process data from millions or billions of users every day, and they rely on convenient technologies like the ad ID to make that kind of scale possible. Removing this tool from their toolbox will result in substantially less data that can be associated with you in the wild. It is not only beneficial to your privacy, it also makes the surveillance advertising industry less profitable. And don't take our word for it: Facebook has said that Apple's App Tracking Transparency feature would decrease the company's 2022 sales by about $10 billion.

But although it's a good first step, removing your ad ID won't stop all tracking. If you are concerned about a specific privacy-related threat to yourself or someone you know, see our other resources, including Digital Security and Privacy Tips for Those Involved in Abortion Access. You can also check out EFF's guides to surveillance self-defense, including personal security plans, attending a protest, and privacy on mobile phones. These resources are organized into playlists such as this one for reproductive healthcare providers, seekers, and advocates.