Apple’s changes to IDFA in iOS 14

An overview of the changes and what they mean for in-app mobile advertising
What is the IDFA?

Apple’s identifier for advertisers (IDFA) is a unique string of random numbers and letters assigned to an iOS device (e.g. iPhones and iPads).

Here’s an example of what an IDFA looks like:

7D902I08D-7846-4CA4-TE6P-83369125YFDC
What is the IDFA used for?

The IDFA is used for ad targeting, measurement, and attribution in apps on iOS, iPadOS, and tvOS.

Unlike cookies in web browsers that can be blocked or deleted, the IDFA is persistent, meaning it will be associated with that device until a user changes their Apple device (e.g. iPhone or iPad) or manually resets the IDFA.
Apple’s IDFA vs Google’s AAID

Google’s Android also has an ID for advertisers called Android Advertising ID (AAID) and it works in the same way as Apple’s IDFA.

No changes have been proposed for Google’s AAID (yet).

In this presentation, we’ll just be focusing on Apple’s IDFA.
How is the IDFA used currently in mobile app advertising?

The IDFA is passed from the user’s device to AdTech platforms and mobile measurement platforms (MMPs).
But this is all about to change...

Apple Just Crippled IDFA, Sending An $80 Billion Industry Into Upheaval

John Koetsier  Senior Contributor  Consumer Tech
John Koetsier is a journalist, analyst, author, and speaker.

Apple killed the IDFA: A comprehensive guide to the future of mobile marketing

Posted on June 29, 2020 by Eric Benjamin Seufert
What privacy changes are coming with iOS 14?

Privacy

Privacy information on the App Store
A new section on each product page on the App Store helps you see a summary of the privacy practices of the app before you download it. Developers self-report their privacy practices, including data collected by the developer and used to track you across companies, in a simple, easy-to-read format.

Approximate location
A new setting lets you choose to share your approximate location, rather than your precise location, with an app.

Recording indicator
iOS displays an indicator whenever an app is using the mic or camera, both in the app and in Control Center.

App tracking controls and transparency
Developers are now required to get your permission before tracking you. See which apps you have given permission to track in Settings so you can change your preferences.

Limited Photos library access
You can choose to share only selected items with a developer who asks for access to your photos, or you can give access to your entire library.

Upgrade to Sign in with Apple
Developers can offer the option to upgrade existing app accounts to Sign in with Apple so users can enjoy improved privacy, security, and ease of use without setting up a new account.
App tracking controls and transparency

Before an app can access the IDFA and pass it to AdTech companies, **users will have to opt in**.

iOS 14 users will be presented with a message like the one in the image.

App developers will have to use the AppTrackingTransparency framework to access the IDFA.
AppTrackingTransparency

Request user authorization to access app-related data for tracking the user or the device.

Overview

Use the AppTrackingTransparency framework if your app collects data about end users and shares it with other companies for purposes of tracking across apps and web sites. The AppTrackingTransparency framework presents an app-tracking authorization request to the user and provides the tracking authorization status.

To use the AppTrackingTransparency framework:

1. Set up a `NSUserTrackingUsageDescription` to display a system-permission alert request for your app installed on end-user devices.

2. Call `requestTrackingAuthorization(completionHandler:)` to present the app-tracking authorization request to the end user.

IDFA: Now vs in iOS 14

How IDFA is accessed currently.

How IDFA can be accessed in iOS 14.
Will ads still be shown to users and how will ad targeting work in iOS 14?

Yes, ads can still be shown to iOS users, but apps won’t be able to display targeted or retargeted ads to users based on their IDFA, unless they opt in.
How will ad measurement and attribution work?

Via Apple’s SKAdNetwork

Attributing App Installations

SKAdNetwork allows registered advertising networks to attribute app installations to a particular campaign by receiving a signed signal from Apple. This enables them to verify how many installations occurred from an advertisement and measure which campaigns are most effective while maintaining user privacy.

Beginning this fall, advertising networks using SKAdNetwork will have access to Source App information, which identifies the specific app from which an installation occurred. This allows advertising networks who run advertisements on apps they don’t own to identify which app should be credited with initiating the download. SKAdNetwork will also identify re-downloads, which helps advertising networks measure the success of re-engagement campaigns. If you’re an advertising network and would like to use SKAdNetwork for managing advertising attribution, contact us.

A few more words about SKAdNetwork

1. App install attribution data will pass through SKAdNetwork and then onto ad networks.

2. **No user-level or device-level data will be passed** to AdTech platforms or MMPs.

3. Campaign IDs are limited to 100 per ad network.
FAQs
When will these changes to IDFA be released?

iOS 14 will likely be released in September 2020.

Although these changes to IDFA were supposed to be released with iOS 14, Apple have decided to delay the release of these changes until early 2021.
What will happen to apps running in iOS 14 that haven’t implemented the AppTrackingTransparency framework?

Apps will need to publish an update once these changes are released to include the AppTrackingTransparency API.

If an app running on iOS 14 doesn’t have this API, then they won’t have access to the IDFA (it will be zeroed out) and won’t be able to ask users to opt in via the pop-up message.
When will users see the opt-in message and how often?

Only once, unless the user deletes the app and then reinstalls it.

It looks like app developers can choose when to show the message to users, but they won’t have access to the IDFA until the users opt in.

The `requestTrackingAuthorization(completionHandler:)` is the one-time request to authorize or deny access to app-related data that can be used for tracking the user or the device. The system remembers the user’s choice and doesn’t prompt again unless a user uninstalls and then reinstalls the app on the device.

Note, when calling `requestTrackingAuthorization(completionHandler:)`, the `NSUserTrackingUsageDescription` key must be in the Information Property List.

Source: Apple Developer Documentation
Can the opt-in message be customized?

Some parts of the message can be customized. The part in bold is set by the system (i.e. Apple) and can't be changed.

However, the text in the red box can be modified using the NSUserTrackingUsageDescription key.

**Discussion**

App developers need to provide custom text, known as a usage description string, which is displayed as a system-permission alert request. The description informs the user why the app is requesting permission to use data for tracking the user or the device. The app user has the option to grant or deny the authorization request. If you don’t include a usage-description string, your app may crash when a user first launches it.

Your app needs to request permission to track sometime before tracking occurs. This could be at first launch or when certain app features are used. For example, when signing on with a third-party SSO.

Set the NSUserTrackingUsageDescription key in the Information Property List (Info.plist):

1. Select your project’s Info.plist file in the Xcode Project Navigator.

2. Modify the file using the Xcode Property List Editor: Privacy - Tracking Usage Description.

   • Use sentence-style capitalization and appropriate ending punctuation. Keep the text short and specific. There’s no need to include your app name because the system already identifies your app.

   • If the title is a sentence fragment, don’t add ending punctuation.

See Apple's Human Interface Guidelines for example usage descriptions.
How many iOS users will opt in?

Nobody knows for sure but most estimates put the opt-in rate between 1% to 20%.
What are some possible workarounds?

There isn’t a clear replacement for the IDFA, but some workarounds for identification, ad targeting, and attribution include:

- **Device fingerprinting for identification**: Not recommended due to privacy reasons and Apple will likely crack down on this.

- **Contextual ad targeting**: It’s often considered not as effective as IDFA-based ad targeting.

- **Using an email address or phone number as an identifier**: Limited in scale.

Any workaround that aims to identify users likely won’t meet Apple’s privacy guidelines and will probably be squashed.
What does the future hold for mobile measurement platforms (MMPs) and AdTech companies?

With the main advertising processes (identification, targeting, measurement, and attribution) being taken away from independent AdTech companies, it will be harder for MMPs and AdTech companies (e.g. ad networks, DSPs, SSPs, etc.) to operate the way they do currently.

It just means they’ll have to come up with innovative solutions to tackle these challenges.

Expect to see some short-term workarounds while they consider long-term solutions.
Questions?

clearcode.cc/ask-us-anything

Contact us

EMAIL
sales@clearcode.cc

PHONE
US: (800) 615-0584
Europe: +48 71 881 766

WEB

clearcode.cc