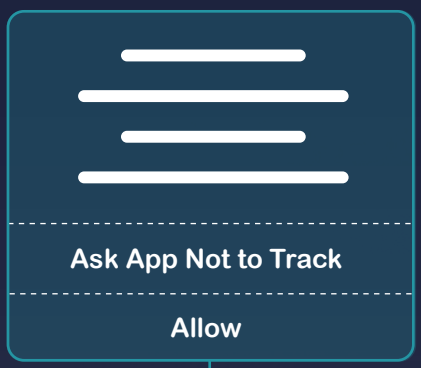
IDFA IS GOING AWAY

A GUIDE TO GETTING READY FOR iOS 14.5



In June 2020, Apple announced the plan to restrict the Identifier for Advertisers (IDFA) for iOS 14. To give developers more time to prepare for these changes, the implementation was not carried out, as first planned, in September 2020 but delayed to early 2021.

With the upcoming release of iOS 14.5 - the version in which the IDFA restrictions will come into effect for the first time, as well as the ATT (App Tracking Transparency) comes into force - we would like to address some important questions, possible procedures, facts, tips and tricks for a good start in ATT.

WHAT IS THE IDFA?

What cookies are for the browser, the IDFA is for the iPhone or iPad: It is a random, resettable unique identifier that makes it possible to identify a user across all apps. This identifier is used to ensure personalization, targeting (both audience targeting and frequency capping) and ad attribution (conversion rates). Since the IDFA is consistent and equally available to all participants in the ecosystem - unlike 3rd party tracking in the browser - it is considered to be of particularly high quality.

WHAT ARE APPLE'S PLANS?

During the Worldwide Developers Conference 2020, Apple announced that the IDFA will be masked by default in iOS 14. Thus, apps will only get access to the IDFA if the user confirms an explicit opt-in.

This is a logical continuation of the already introduced LAT (Limited Ad Tracking), which was to be implemented in September 2020 but got postponed to give publishers and mobile app developers more time to take concrete measures. With the release of iOS 14.5 this deadline has now finally expired.
The following requirements accompany the release of iOS 14.5:

- **ATT (App Tracking Transparency) permission:** This is a pop-up that designed by Apple and looks the same for all apps. It is mandatory in order to receive the IDFA. Once rejected, it is not easily possible to revisit the pop-up from within the app.

- **Privacy Nutrition Label in the App Store:** In the future, apps must already disclose in the App Store whether and for what purpose tracking is used.

Incorrect information in the Privacy Nutritions and attempts to circumvent the ATT via technical measures, such as fingerprinting, will result in the app being excluded from the App Store. Likewise, there is no possibility to update apps after iOS 14.5 should the requirements not be met.

See also: https://www.preferencechoice.com/blog/new-apple-ios-14-privacy-features/

WHY IS THIS TOPIC IMPORTANT FOR ME AS A PUBLISHER?

The availability of IDFA has a strong influence on the eCPM (effective cost per mille) of publishers and thus also on the monetizability of the app. Available traffic with IDFA achieves up to 30% higher eCPMs. This is due to several reasons: Not offering IDFA strongly influences campaign diversity - especially in branding advertising, advertisers demand more specific targeting. As a result, often only low-priced performance campaigns can be resorted to without IDFA, which also affects the quality of campaigns. Furthermore, this can be attributed to a lack of security measures, such as fraud protection or the loss of frequency capping.

With iOS 14.5, this topic receives special attention because Apple provides various mechanisms to protect the user from being permanently asked for tracking. On the one hand, the tracking pop-up can be globally disabled via the device settings. On the other hand, the pop-up cannot be called up again after the tracking permission has been rejected once. Thus, users have to make the change manually in the settings of the device - a step they are unlikely to take voluntarily. Hence, it is not possible to ask for tracking permission until the user gives up and reluctantly agrees.
For EU users, another difficulty arises: The ATT query and an explicit opt-in do not release

the publisher from additionally including a TCF 2.0 compliant CMP (Consent Management Platform) in the app in order to meet GDPR requirements (General Data Protection Regulation).

Asking for ATT, consent according to TCF 2.0 and, if necessary, further permissions (app and advertising-related) can quickly overwhelm and discourage users.

WHAT CAN I DO?

Apple‘s ATT request is standardized (design and process) and can only be done once in the app. However, the publisher is free to display its own, self-designed pop-ups when the app is launched. These make it possible to prepare users for the subsequent permission request for ATT in the best possible way. In this step, the user is informed why the publisher needs the tracking, what the data is used for, and why the user‘s consent is relevant (e.g., to keep the app free of charge).

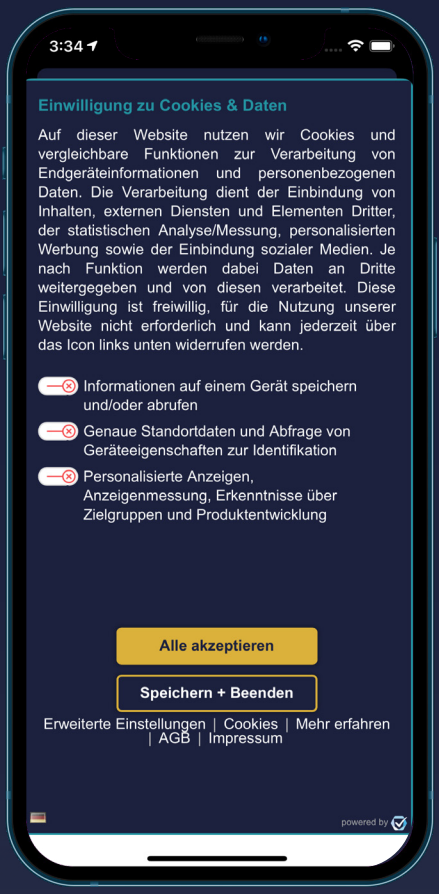
If the user refuses ATT, a later pop-up can again point out why tracking is required. Here, the user is provided with instructions and subsequently the selection can be adjusted in the settings of the corresponding Apple device. The ATT pop-up itself cannot be initiated again by the app after an initial rejection.

SUCCESS FACTORS

- **Design:** Use of own CI for the design of the pop-up. This is not about third-party concerns (advertising partners).
- **Wording:** Transparency creates trust, but too much and too detailed information quickly overwhelms the user. Therefore, the message should be short and concise.
- **Build acceptance:** We recommend making the first app uses free of advertising for the user. Thereby users can convince themselves of the quality of the app and its added value. This helps to build acceptance of advertising.
- **Order of request:** Publishers should first query the CMP; thereby it can already be deduced whether the user is sufficiently sensitized to the topic. If the user does not give consent for data processing in the CMP or selects manual setups, it is more likely that the ATT will also be rejected.
- **Frequency of request:** The user can also be reminded of the importance of tracking, but without deterring her/him from the app. After all, a user without IDFA is still more valuable than a user who uninstalls the app. Thus, a slow request cadence should be started, which is then gradually increased. The acceptance rate should be monitored to identify an ideal frequency.
- **Educate on benefits of IDFA:** Users may be under the misconception that refusing ATT will result in less or no advertising. However IDFA only determines the quality and relevance of advertising. Publishers could design different ad layouts and use fewer ad units for users with IDFA. Especially in the conversion of users this is crucial (**„Give me your IDFA and you get less advertising“**).

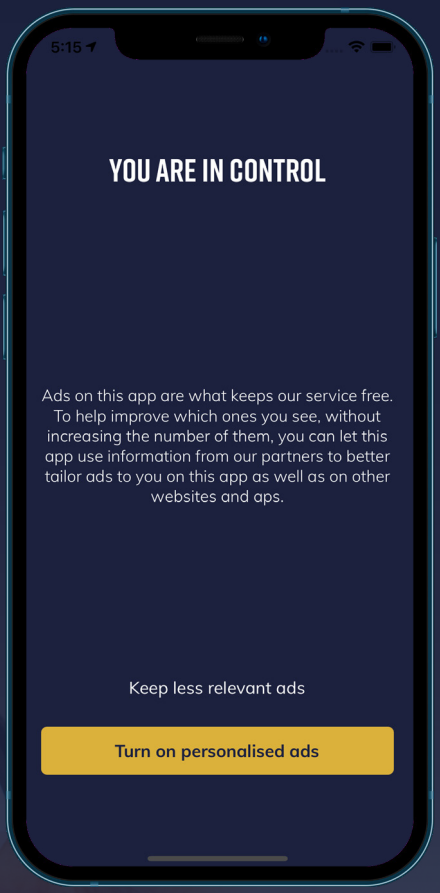
Important: According to current information, we have to assume that Apple will block the release of apps in the App Store if tracking is enforced. This means that content or features cannot be hidden behind a tracking wall.

01 CONSENT REQUEST VIA CMP



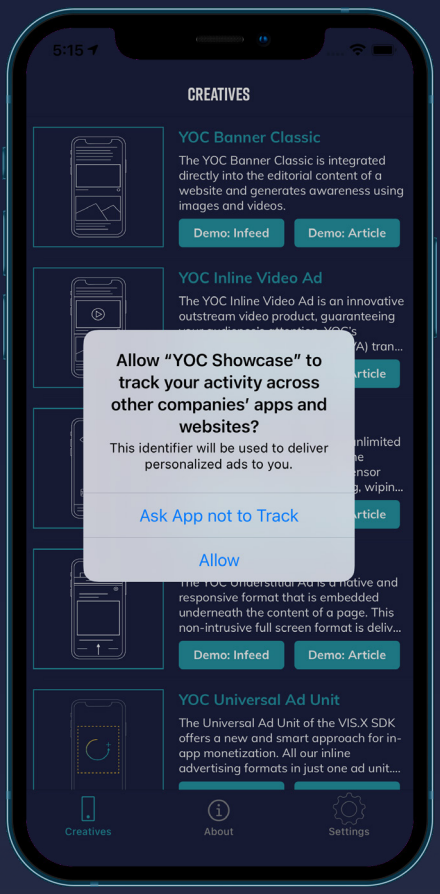
02 ATT PRE-PROMPT (EXAMPLE)

Soft layer clarifies why ATT is required and prepares user for query that will follow



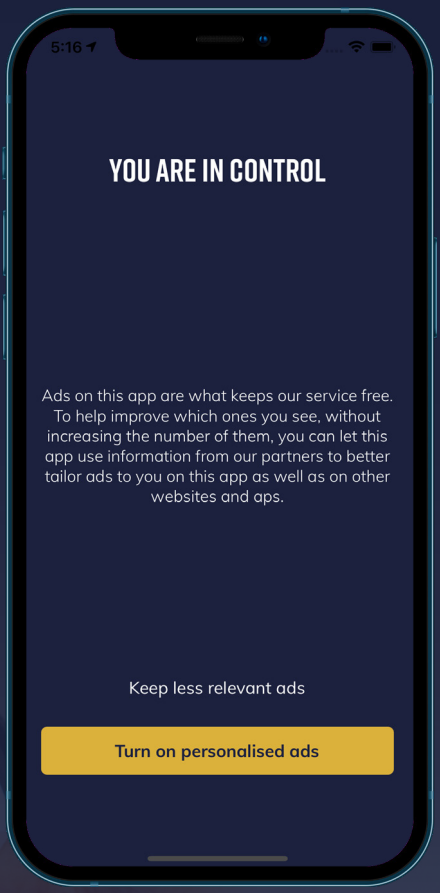
03 INITIATION OF ATT AFTER CLICK ON PRE-PROMPT

AFTER REJECTION



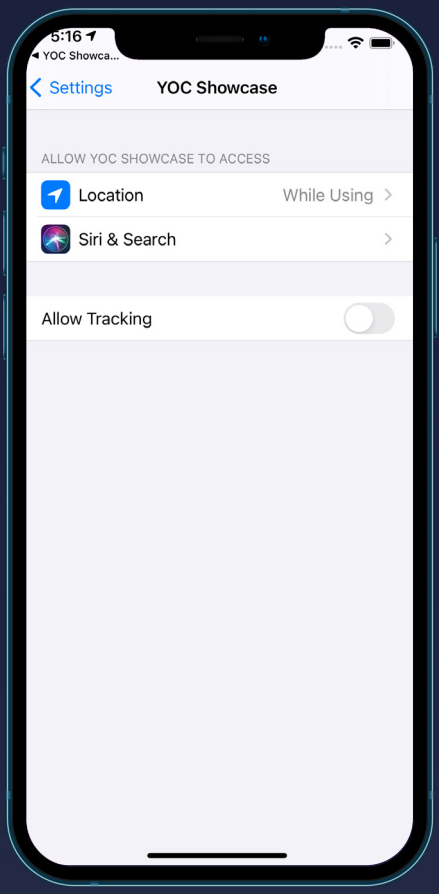
04 ATT POST-PROMPT (EXAMPLE)

If ATT was denied, a soft layer follows after a pre-defined time. This enables users to easily navigate to settings again.

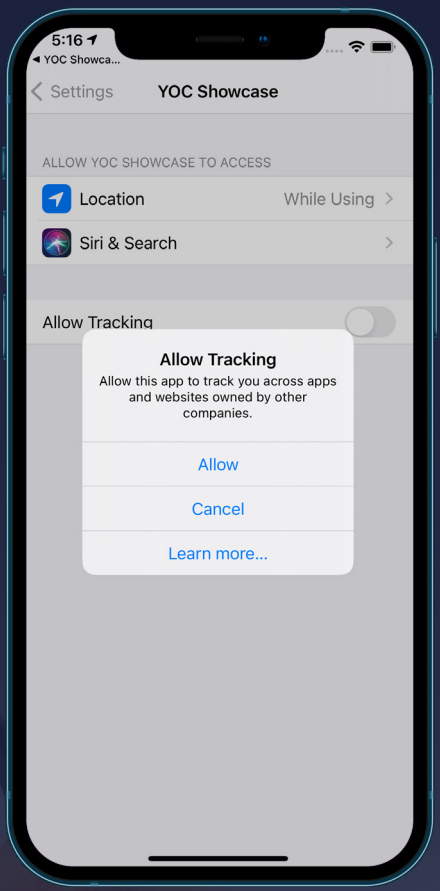


After clicking on „Turn On Personalised Ads“ user is directed to settings.

05 POST-PROMT: NAVIGATION TO SETTINGS

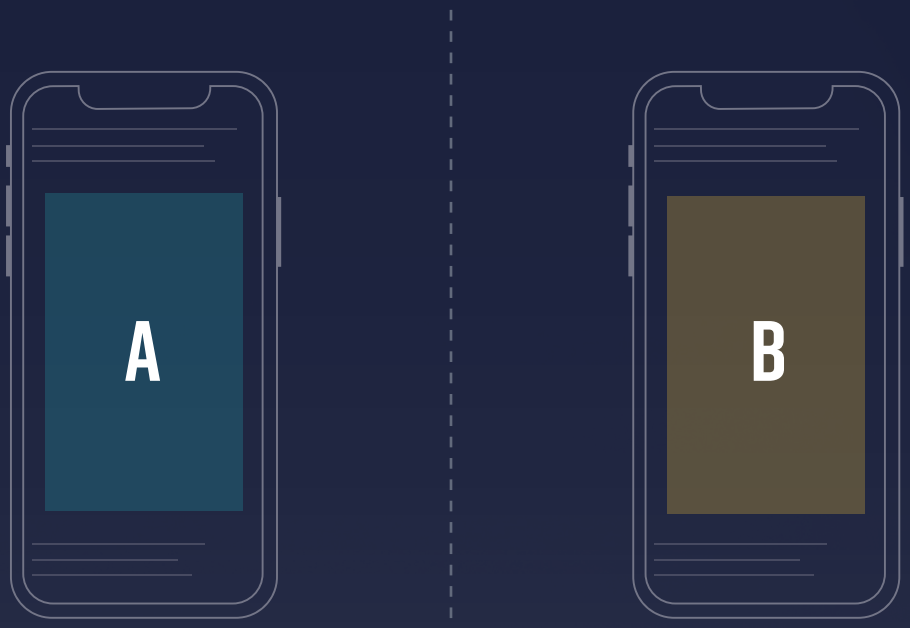


06 TRACKING CAN BE ALLOWED



DATA-DRIVEN APPROACH, WHENEVER POSSIBLE

If possible, A/B testing is recommended. Publishers should prepare several strategies, divide their users into random groups and test the rate of acceptance against each other. An important KPI is not only the rate of immediate permissions, but also the downstream conversion of the originally rejected users (% consent over time).



WHAT DOES THIS MEAN FOR ME AS AN ADVERTISER?

Although Apple‘s changes primarily affect apps and thus publishers, the loss of the IDFA also has an impact on advertisers. Since it will be easier for iPhone users to deactivate tracking, it can be assumed that the majority of users will undertake this step.

By deactivating the tracking function, many users will no longer be directly addressable. Media planners will have to ask themselves following question when planning campaigns in the future: Do I plan my campaign with the aim of addressing a very specific target group, albeit with a much smaller audience, or do I pursue reach goals? Combining both goals in one campaign will be more difficult to achieve. In this case, the campaign budget will have to be split.

Attribution of conversions will also become more difficult to track in the future, influencing especially performance-driven advertising. Apple has developed the so-called SKAdNetwork for anonymous conversion tracking, but this only works for conversion tracking for app installs in Apple‘s own App Store. Conversion tracking outside the Apple ecosystem is thus not possible.

Unfortunately, there are no solutions to this challenge at this point in time. It can be assumed that Apple will not accept any efforts by the industry to establish alternative tracking methods, or even fingerprinting. A small consolation: the rules of the game are the same for all market participants. No vendor gets an advantage by having access to user IDs, but no market participant gets a disadvantage either.

In the long run, this change may lead to a shift from user-based targeting back to the contextual targeting world. It can be assumed that this step will be taken for branding campaigns.

If you have questions, don‘t hesitate to contact your partner at YOC or send an email to marketing@yoc.com