Blogs
June 23, 2021
iOS Tracking Analysis

With the release of iOS 14.5, Apple introduced new App Tracking Transparency (ATT) standards requiring iOS app developers to either cease engaging in user and device data tracking or request permission to continue doing so. According to Apple, "tracking" occurs when user or device data is either (1) linked with information that identifies such user or device collected on apps, websites and other locations owned by third parties for the purposes of targeted advertising or advertising measurement, or (2) shared with data brokers. Although many iOS developers themselves may not engage in tracking activities, it's prudent to conduct preliminary analyses of any third parties with access to the developer's iOS user or device data to better elucidate whether such third parties, and thus the developer according to Apple, are engaged in tracking. To that end, below are some high-level steps an iOS developer can take to identify whether third parties may be engaged in tracking through the developer's app.

1. **Linking as Tracking**

- For each third party, perform a two-step analysis asking the following questions:
    - Q1: Is user or device data being combined or linked with any user or device collected from any third party or their owned/operated properties?
        - If no, the linking is most likely not tracking.
    - Q2: If yes to Q1, is the developer or third party's purpose of the linking/combination targeted advertising or advertising measurement?
        - If no, the linking is most likely not tracking.
        - If yes, the linking is most likely tracking.

2. **Sharing with Data Brokers as Tracking**

- Apple generally defines a "data broker" as any company that regularly collects and sells, licenses, or otherwise discloses to third parties the personal information of particular end-users with whom the developer does not have a direct relationship. Applicable statutory/regulatory definitions of data broker may apply as well.
- Some states have data broker registries (e.g., California and Vermont), so a good first step is to perform an online search in such registries for the third parties with access to user or device data through the developer's iOS app.
    - If the third party has access to developer's iOS user or device data and is included in one or more registries, they are a data broker and likely engaged in tracking.
- Even if the third party isn't listed on any registry but they are receiving user or device data from the developer, the developer should review the applicable agreement(s) between the developer and such third party to determine whether the third party is expressly prohibited from (a) using such data for purposes other than providing the services to the developer or (b) disclosing such data to third parties generally.
    - If the service provider is expressly prohibited (and not listed on any registry): assuming the third party is in compliance with the agreement(s), the third party most likely isn't tracking via the developer's app and Apple's "sharing with data brokers" trigger.
    - If the service provider is not prohibited (and not listed on any registry): the developer must conduct more in-depth analysis to determine what the third party actually does with the developer's iOS user/device data to come to a clearer conclusion on whether such activities constitute tracking. The developer should also seek to amend such agreement(s) to ensure tracking activities are expressly prohibited.

If the developer determines that one or more third parties are tracking via the developer's iOS, the developer

generally has two options: If the developer prefers to abstain from requesting user consent for tracking: the developer will need to cease linking/sharing user and device data with any tracking third parties (and ensure it itself is also not engaged in such tracking activities) to become iOS 14.5 compliant. If the developer prefers to continue tracking and request user permission to do so: the developer will need to (a) request user permission to do so via the standard pop-up protocol, (b) logically separate the user/device data of users that do grant permission from those that don't, and (c) only link/share data from those users who do grant permission with the tracking third parties. Developers should also stay apprised of further privacy-related developments coming in iOS 15, including functionality allowing users to (a) see with which third parties apps are sharing their data and (b) prevent trackers from detecting if/when the user opens and emails. Further details are available here.

Explore more in

Privacy & Security