LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Data & Technology Transactions Practice June 30, 2020 | Number 2767

Apple Announces Enhanced Privacy Features for All iOS Apps

New tracking and privacy-related features will apply to all iOS apps when iOS 14 is released in September 2020.

Key Points:

- During Apple's WWDC 2020 keynote address on June 22, 2020, Apple announced two key privacy features impacting how apps can track users and what needs to be disclosed regarding data processing practices. This will affect all iOS app publishers. These are likely to be implemented in the next App Store Guidelines refresh when iOS 14 is launched on September 18, 2020.

- With the new tracking feature, any app that tracks users across apps and websites owned by other companies must ask for users' express consent to do so. iOS app publishers must also explain how they will use that tracking data.

- Under the new "privacy summary" feature, every app will be required to detail the types of personal information that the app collects and whether that information will be used for tracking. Apple's intention is to provide users a "quick snapshot" of what an app collects and encourage iOS app publishers to minimize data collection.

- All iOS app publishers should take note of these features, which will directly impact all apps available on Apple's App Store as well as the changes taking effect.

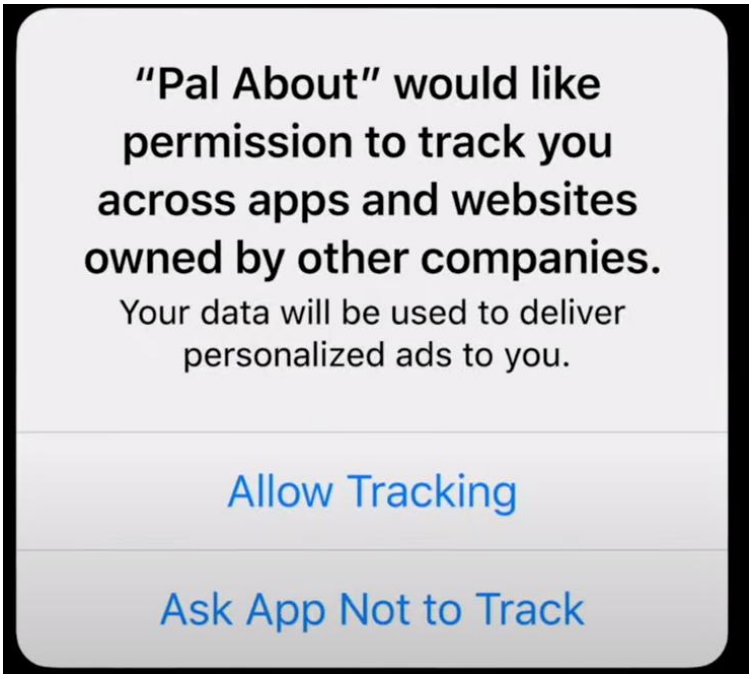
On June 22, 2020, Apple announced at its annual Worldwide Developers Conference (WWDC) that the next major iOS release, iOS 14, scheduled for September 18, 2020, will feature two privacy-related features that will apply to all iOS apps (see Apple's press release here).

Tracking permissions

With this new tracking feature, any app (regardless of method) that intends to "track" a user, whether using Apple's technology or some other method such as IDFA identifiers or IP address, across apps and websites owned by other companies, will be required to **expressly** ask users for their consent to do so (see sample screenshot below). This requirement also applies if an app tries to access a user's device advertising ID, the identifier commonly used for targeted advertising.

Tracking refers to the act of linking user or device data collected from an app with user or device data collected from other companies' apps, websites, or offline properties for targeted advertising or advertising measurement purposes. Tracking also refers to sharing user or device data with data brokers. Examples of tracking include displaying targeted advertisements in an app based on user data collected from apps owned by other companies and using third party SDKs in an app for data analytics purposes.

This upcoming iOS feature means that **iOS app publishers must ask users if they want to be tracked by the app and they must explain how that tracking data will be used** (*e.g.*, to deliver targeted advertising). Users must also be given the right to reject consent to tracking. If an app fails to implement the above, or is discovered tracking users without obtaining their consent through the pop-up agreement, the app may breach the Apple Developer Agreement. Such a breach can result in suspension or removal of the app from the App Store and potentially suspension of the iOS app publisher's account.



Credit: Apple, WWDC Keynote

Apple lists two exceptions through which an app can track a user without asking for their consent: (1) when an app is sharing data locally on a user's device with another app, but the data never leaves the user's device in a way that can identify the user or device; and (2) when data is shared solely for fraud detection or security protection purposes.

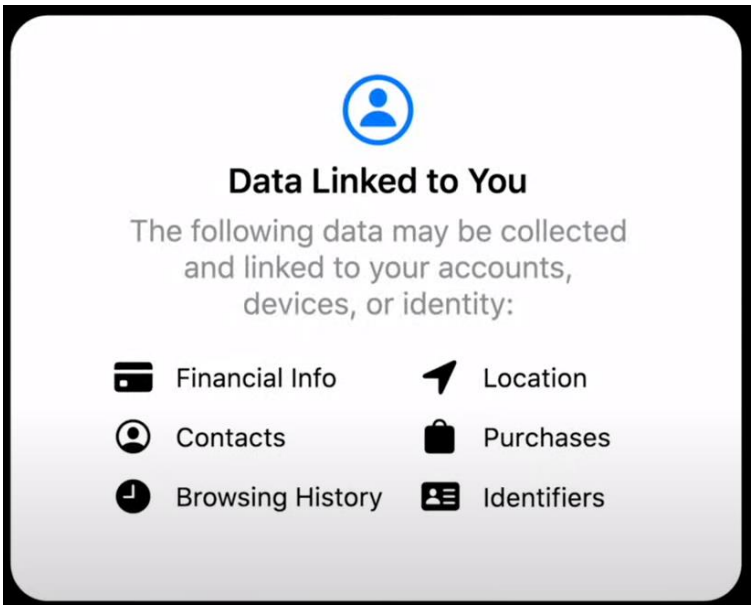
Although this tracking feature depends on app publishers self-reporting the tracking data that they collect on their apps, the feature is likely to reduce the amount of data that apps collect. Given that a large number of apps use tracking methods, whether for targeted advertising or simply to enhance the app's functionality or user experience (*e.g.*, fitness or sleep tracking), app publishers should start to review their app's permissions before the new guidelines take effect.

Privacy summary

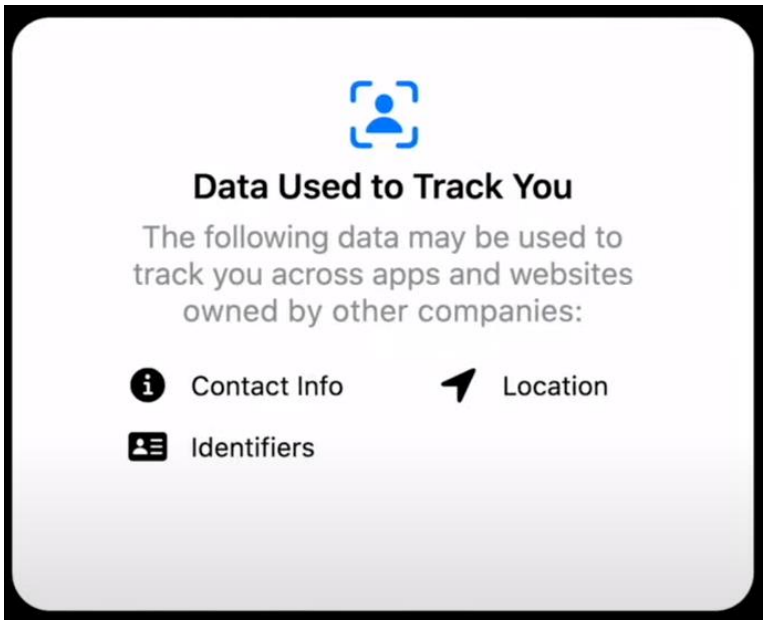
Another key privacy update under iOS 14 will require every app submitted to the App Store to identify the categories of personal information that it collects, *e.g.*, financial information, browsing history, identifiers, contacts etc. This requirement **applies globally to all apps on the App Store** rather than only apps that "track" users. Later this year, App Store product pages will feature summaries of app publishers' self-reported privacy practices before users download the app. This summary is intended to help users better understand how the app uses collected data and to encourage iOS app publishers to minimize data collection. App publishers will also have to spell out the third party SDKs incorporated into their apps (if any), the data the third party SDK collects, how the data may be used, and whether the data is used to track users.

In general, users must be shown the following two summary panels:

- A summary of "data linked to you"
- A summary of "data used to track you"



Credit: Apple, WWDC Keynote



Credit: Apple, WWDC Keynote

Other privacy features

Apple also announced two other features under iOS 14 that aim to enhance users' privacy and to limit the location information collected by apps. The first feature allows users to share their **approximate location** (*e.g.*, the user's city) with apps instead of their precise location (*e.g.*, the user's street address).

The second feature shows a camera and microphone recording indicator (similar to the ones already implemented in Macs and MacBooks) in the status bar which will light up when the device's camera is in use or a microphone is active.

Legal requirements: Who will this impact?

Any organization that has an iOS app. In particular, those:

- That use targeted advertising
- Performing cross-platform analyses
- Involved in health or fitness tracking (*e.g.,* fitness activity, sleep cycles)
- Profiling user interests (such as lifestyle, food, restaurant and travel apps)
- Linking user's activities in the app with other non-app activities (*e.g.,* across different games)
- Involved in open banking (where third party financial data is accessed and may be tracked as a result)

Data privacy laws across the globe, such as the EU's General Data Protection Regulation (GDPR), the California's California Consumer Protection Act (CCPA), Thailand's upcoming Personal Data Protection Act (PDPA), as well as data privacy laws in South Korea, India, Hong Kong, Singapore and many others all include various levels of legal requirements with respect to notice, consent, and disclosures regarding the processing of personal data.

The App Store requirements sit in addition to such legal requirements (even though in some cases they may appear to align with some legal obligations). Determining how these new features impact specific apps and identifying any top-up "App Store" data privacy review that may be required will be key issues for organizations, as well as harmonizing such considerations with existing privacy compliance programs.

Please click here for more information on Apple's new iOS 14 privacy features.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Gail E. Crawford
gail.crawford@lw.com
+44.20.7710.3001
London

Kieran Donovan
kieran.donovan@lw.com
+852.2912.2701
Hong Kong

Malika Sajdik
malika.sajdik@lw.com
+852.2912.2693
Hong Kong

Aster Y. Lin
aster.lin@lw.com
+852.2912.2705
Hong Kong

The authors would like to thank Bianca H. Lee for her contribution to this Client Alert.

You Might Also Be Interested In

ESMA Draft Guidelines on Outsourcing to Cloud Service Providers

Online Marketplace Liability: Court of Justice of the European Union Ruling in *Coty v. Amazon*

EDPB Guidelines – What is the Territorial Reach of the GDPR?