

# 【WWDC22 10166/10167】探索应用追踪透 明化 App Tracking Transparency 与隐私标签

老司机技术

预计阅读时间10分钟

2 天前

摘要：现阶段，所有 App 想要追踪用户的数据，必须通过 AppTrackingTransparency 框架来获得用户授权。因此，本文将聚焦于应用追踪透明化(App Tracking Transparency)，并解释了用户追踪是如何定义的以及在确实需要接入此框架时，具体应该如何接入。

本文基于 [Session 10166](#)、[Session 10167](#) 梳理

作者：小铁匠 Linus，iOS 开发者，微信公众号《WLB 工作生活两不误》博主。

审核：Damien，就职于字节跳动，目前负责 TikTok 隐私和安全相关的工作。

前提提要

App Tracking Transparency (ATT) 是苹果官方从 iOS 14 开始重点强调的 申请用户广告追踪权限 相关的框架。

当用户了解自己的数据将如何被共享时，他们才更有可能信任并使用 App，这就是为什么从 iOS 14 开始，苹果官方要求所有的 App 在追踪用户之前必须获得用户授权的原因。

本文主要从以下四个方面探讨 App Tracking Transparency：

1. 如何定义用户追踪
2. 在明确需要用户追踪的情况下，如何获得用户的许可
3. 隐私标签的使用
4. 注意事项

相关 Session：

[Session 10167 Create your Privacy Nutrition Label](#)

[Session 10038 What's new with SKAdNetwork](#)

[Session 10096 What's new in privacy](#)

## 如何定义用户追踪

苹果官方对用户追踪的定义是：将从 App 中收集的 用户或设备数据 与从其他公司的 App、网站或离线数据中收集的 用户或设备数据 结合起来，用于定向广告或广告效果衡量的行为。

如果你觉得上面的定义晦涩难懂的话，那么通过以下几个具体的例子，相信你一定能大致掌握关于用户追踪定义的门道了。

### 不涉及用户追踪的场景 1

假设你早餐想吃鸡蛋饼，你打开一款美食评价 App 搜索了附近的鸡蛋饼店，此时这款 App 记录了你的搜索记录。然后，这款 App 正好想给那些早餐店做广告，它基于你的搜索记录就给你展示了早餐的广告。

在本例中，该款 App 没有将用户数据与其他公司的 App 或网站中的任何数据相结合，以用于给你推荐早餐广告。因此，此场景不会被视为用户追踪。

### 不涉及用户追踪的场景 2

再次假设：拥有上面那款美食评价 App 的公司还有另一款优惠券 App，两款 App 的数据都是存储在自家的服务器上。然后，这款优惠券 App 基于你对鸡蛋饼的喜爱而给你发放了相关的优惠券（它用到了你在美食评价 App 中搜索鸡蛋饼的记录）。

在本例中，该款优惠券 App 不需要获得用户追踪的授权，即不属于用户追踪，这是因为美食评价 App 并没有将获取到的用户数据与其他公司的 App 或网站的任何数据相结合。

划重点：自家 App 内部的数据共享是不需要授权的。

### 用户追踪的场景 1（跨主体的 App）

假设你使用了一款不是上面那家公司的外卖 App，而且还在深夜点了一份夜宵。在注册外卖 App 时，你使用了与美食评价 App 相同的联系方式（可能是电子邮箱、地理位置、电话等等）。此后，美食评价 App 给你推送了一则全天提供早餐的餐馆广告，因为它利用相同的联系方式从外卖 App 处收集到了你点外卖的订单数据。

此场景需要美食评价 App 请求用户追踪权限，因为它出于广告目的，跨 App 将用户数据通过特定的联系方式链接在一起。因此，只要是出于结合用户数据的广告目的，即使将电子邮箱或其他用户标识符提前进行了哈希处理，App 仍然是需要用户追踪权限的（因为 App 中用户的数据仍会与其他公司的数据相链接）。

值得注意的是，标识符的类型以及它是否被哈希化并没有改变它被用于追踪的事实，即不管什么形式都需要要进行用户追踪的授权。

### 用户追踪的场景 2（第三方 SDK）

要确定 App 是否需要请求追踪权限，还需要考虑第三方 SDK 是否有共享 App 中的数据。

继续举例，假设美食评价 App 中并没有编写任何需要用户追踪权限的代码，但希望在其 App 中包含第三方 SDK、用于广告效果的衡量。此时，美食评价 App 是否需要申请用户追踪的权限，就取决于该第三方 SDK 有没有将美食评价 App 的用户与从其它 App 或网站获取的用户数据进行结合了。

这时候你可能会问，我怎么知道第三方 SDK 到底有没有做需要用户追踪权限的事情呀？！答案就是：询问该 SDK 的开发人员。毕竟作为开发人员，你要对整个 App 的行为负责。

### 与数据代理共享数据

除上面提到的情况之外，用户追踪还包含与数据代理商共享用户或设备数据的行为。

#### 什么是数据代理商

数据代理商有很明确的法律定义，但一般来说，数据代理商是指那些定期收集和出售、许可或以其他方式向第三方披露与业务没有直接关系的特定用户个人信息的公司。

#### App 接入了数据代理商，该怎么办

苹果官方明确了以下几个要求：

1. 无论共享给数据代理商的数据是否与其他公司用于广告或广告效果测量的数据相关，该场景都被视为用户追踪，需要得到用户的授权。
2. 即使 App 没有直接将数据共享给数据代理商，但后续通过自家的服务器将数据共享给数据代理商的场景，也是需要 App 端向用户申请追踪权限的。

### 如何获得用户许可

根据 App 自身场景，如果确定需要追踪用户，则需要请求并获取用户的授权。相应的方法步骤如下。

#### 请求 App 的追踪权限

为了请求 App 跟踪的权限，您需要通过调用 `requestTrackingAuthorization(completionHandler:)` 方法来显示 App 跟踪授权请求提示。

调用这个方法将会有一个系统权限提示框出现在 App 里。



这是一次性提示。系统将记住用户的选择，并且不会再次提示，除非卸载并重新安装 App。

#### 配置 NSUserTrackingUsageDescription 隐私描述

在 `info.plist` 文件中配置 Key 为 `NSUserTrackingUsageDescription` 对应的字符串，用于在请求权限时展示给用户。一个清晰、简洁的字符串，可以帮助用户理解为什么要求他们允许自己被追踪。

此字符串不需要包含 App 的名称，因为系统将自动识别请求的 App，并在系统提示中显示 App 名称。

如果未包含使用说明字符串，则当显示系统提示时，App 将崩溃。

#### 判断当前 App 追踪权限的状态

iOS 14 起，可以使用 `trackingAuthorizationStatus` 确定用户对 App 追踪权限的状态。如果用户已选择允许授权，App 有权将用户的活动数据链接到其他 App 和网站，只要其追踪授权的状态是保持授权不变的。当然，用户可以随时更改、授予或撤销其追踪授权，因此请**确保在每次启动时的授权状态**，再进行后续的操作。

用户可以控制 App 是否具有追踪每个 App 的权限。用户授予某个 App 追踪的权限，并不意味着同一公司另一个 App 的追踪权限也被授权了。不同的 App 在从该 App 获取数据之前，必须分别请求用户对该特定 App 的权限。

```
01: if (@available(iOS 14, *)) {
02:     ATTrackingManager.AuthorizationStatus status = ATTrackingManager.tracki
ngAuthorizationStatus;
03:     ...
04: } else {
05:     ...
06: }
```

#### 隐私标签（Privacy Nutrition Label）

从 WWDC 2020 开始，开发者在提交 App 时，还需要声明 App 将使用什么数据来追踪，而这些描述会显示在 App 的隐私营养标签 (Privacy Nutrition Label) 上。隐私营养标签（下称：隐私标签），类似于食物上的营养标签，展示的是 App 在用户追踪时所需信息的描述。

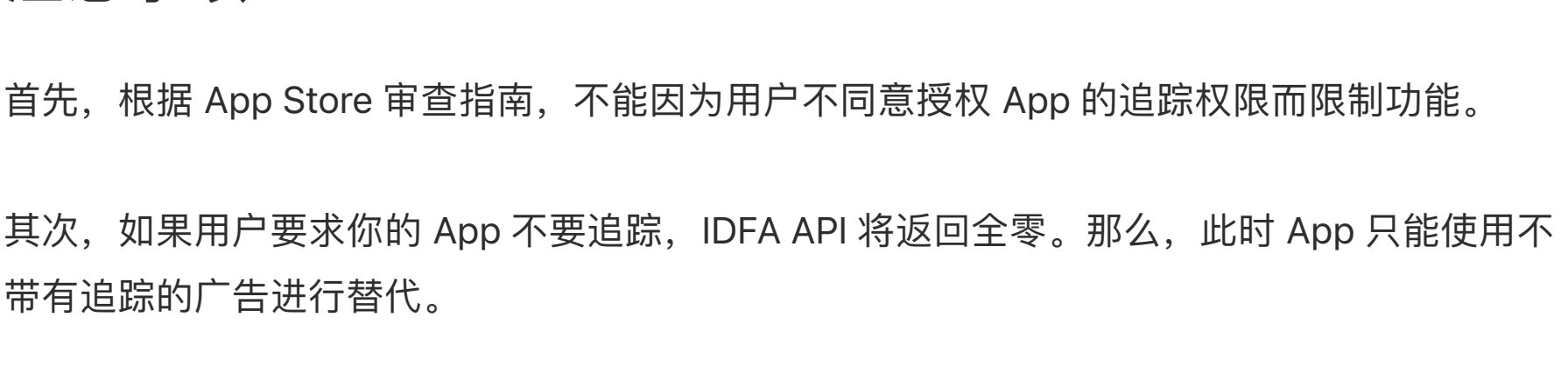


#### 如何创建隐私标签

为了创建隐私标签，开发者可以在 App Store Connect 中创 App 收集的数据、数据类型的场景，以及这些数据如何存储进行说明。作为开发者，你可能没法完整列举 App 中的所有数据类别，除了可以从列出 App 所有功能开始以外，也请确保与 App 的各类干系人取得联系。比如，了解营销团队使用了哪些数据，与法务一起梳理 App 隐私政策中记录的所有数据等等。

#### 隐私标签的更新策略

开发者可以在任何时候更新隐私标签，并且不需要 App 发布新版本。苹果官方的建议是在改变 App 中数据使用的方式时，需要确保隐私标签是最新的。常见的场景有，在 App 中添加了新功能、接入了新的第三方 SDK，或收集了新的数据等等。比如，IP 地址可以用于多种目的，包括作为标识符或用来推断用户的大致位置。如果需要使用 IP 地址来进行位置分析，那么就需要在隐私标签中声明位置这一项。



### 注意事项

首先，根据 App Store 审查指南，不能因为用户不同意授权 App 的追踪权限而限制功能。

其次，如果用户要求你的 App 不要追踪，IDFA API 将返回全零。那么，此时 App 只能使用不带有追踪的广告进行替代。

而对于广告效果测量方面，苹果也在持续建立和改进广告网络的相关技术。有关 SKAdNetwork 和广告点击转化计算等方面的更多信息，请参阅 [Session 10033 Meet privacy preserving ad attribution](#) 和 [Session 10038 What's new with SKAdNetwork](#)。

最后，苹果官方对指纹 (Fingerprinting) 的态度非常坚决：无论用户是否授予 App 追踪的权限，利用指纹或其它来自设备的信息尝试识别设备或用户，都是不允许的。其中，尝试识别的内容包括但不限于用户的 Web 浏览器及其配置、用户的设备及其配置、用户的地理位置或用户的网络连接等。

### 总结

现在你应该已经了解了应用追踪透明化 App Tracking Transparency 的基本情况了。那么作为开发者，首先明确什么是用户追踪，其次确认你负责的 App 是否需要，最后根据 App 的实际情况，如果确实需要用户追踪，就按官方的要求去获得用户的许可。除此之外，本文中也列举了苹果官方明令禁止的一些可能损害用户隐私权益的行为，希望开发者不要触碰红线。

### 关注我们

我们是「老司机技术」，一个持续追求精品 iOS 内容的技术公众号。欢迎关注。



微信扫描二维码，关注我的公众号

关注有礼，关注【老司机技术】公众号，回复「2022」，领取 WWDC21 及以前的内参

© 著作权归作者所有

这个作品真棒，我要支持一下！

点赞

👍 赞

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏

🔖 收藏