Myths Apple Tells About User Privacy and Security With Other Payment Systems

Apple's iOS App Store is a powerful gateway for users to download, access and update apps for their iPhones. Apple claims that only Apple's payment system for apps through the App Store is secure enough, and that users' security and privacy is at risk if other companies offer competing payment systems.

We decided to dig deeper into their claims, to see what's *really* true.

✕ THE MYTH 1:

Apple claims that its App Review process is successful in protecting user security.[1]

✓ THE TRUTH:

Many malicious and fraudulent apps have been approved by Apple's App Review.[2]

For example:

A developer said they were **"seeing more fraudulent activity on the platforms"** and the potential fraud could equate to "2% - 5% of gross revenues on iOS alone."[3]

One fraudulent app claiming to offer virus scanning was accepted and published by an Apple reviewer, which then **became one of the "top grossing" apps in the App Store,** offering weekly renewing subscriptions to non-existent virus scanning services through Apple's payment system.

Researchers discovered that there are **204 "Fleeceware" apps containing hidden subscription fees** (ignoring Apple's policies) that boast more than a billion downloads and $400 million in revenue on the Apple App Store and Google Play Store.[4]

Spotify

✕ THE MYTH 2:

Apple threatens that using a different payment system than its iOS App Store's would

"cripple the privacy and security protections that have made iPhone so secure, and expose users to serious security risks."[5]

✓ THE TRUTH:

Apple knows that cybercrime and bad actors can break through its privacy and security protections. For example, just last year Apple secretively released updates for two disclosed security vulnerabilities that they knew could have been exploited on millions of Apple devices.[6]

✕ THE MYTH 3:

Apple says that

"developers would be harmed... because the increased threat from sideloading would erode users' trust in the ecosystem, resulting in many users downloading fewer apps from fewer developers, and making fewer in-app purchases."[7]

✓ THE TRUTH:

Decentralized software downloads have always been the norm for app developers, and companies like Google already offer sideloading, which more than 2.5 billion monthly users use across 190+ countries worldwide to keep downloading the apps they want to buy.[8]

Spotify

✕ THE MYTH 4:

Apple claims that

"sideloaded apps could access other device or user data... As a result, users' data may be collected and shared without their permission."[9]

✓ THE TRUTH:

Apple already continues to track, collect, and share users' data without their permission.

For example:

Researchers found that even when a user disables "Sharing Data Analytics" on their iPhone, **the device still sends vast amounts of user data to Apple,** including what that user tapped on, which apps they searched for, what ads they saw, how long they looked at a given app and how they found it.

As Apple itself admits, Apple's own Search Ads uses App Transaction Data (historical information about the apps you've downloaded and in-app purchases you've made) to **collect information about what you're doing in competing apps.**

Apple still tracks users to serve personalized ads. Apple uses your location, keyboard language settings, device type, OS version, mobile carrier, and more of your data to serve you "more relevant ads" within its own apps. Apple also uses account information and past purchases to group customers into market segments to better target you with ads.

To learn more, **visit www.TimeToPlayFair.com**

Sources

[1]Apple's Sideloading Paper, page 3.
[2]Epic v Apple trial [2021] - Epic Games, Inc.'s Proposed Findings of Fact of 8 April 2021, paragraph 557a.
[3]Epic v Apple trial [2021] - Epic Games, Inc.'s Proposed Findings of Fact of 8 April 2021, paragraph 324.
[4]How 'fleeceware' apps have earned over $400 million on Android and iOS. The purpose of these applications is to draw users into a free trial to "test" the app, after which they overcharge them through subscriptions which sometimes run as high as $3,432 per year.
[5]See Building a Trusted Ecosystem for Millions of Apps, A threat analysis of sideloading (**"Apple's Sideloading Paper"**), page 6. When discussing direct app downloads and rival (third-party) app stores in public fora, Apple intentionally fails to distinguish the two, using the term "sideloading" (which is typically used to describe direct downloads) to refer to both collectively, alleging that they carry similar implications for user privacy and security.
[6]According to Apple, a kernel vulnerability — CVE-2022-32894 — and a WebKit vulnerability — CVE-2022-32893 — are present on various devices, including iPhones (6s or later), all iPad Pros, iPad Airs (2 or later), iPads (5 or later), iPad minis (4 or later), seventh generation iPod touches, and Mac computers running macOS Big Sur, Catalina or Monterey. See Apple's announcement at: https://support.apple.com/en-us/HT213412. This was covered by various press outlets, including *inter alia:* https://www.securitymagazine.com/articles/98198-apple-warns-of-cybersecurity-vulnerabilities-affecting-millions-of-devices
[7]Apple's Sideloading Paper, page 6.
[8]https://play.google/howplayworks/#:~:text=Google%20Play%20is%20an%20online,quality%20apps%20and%20delightful%20content.
[9]Apple's Sideloading Paper, page 24.

Spotify