

MYTH VS. FACT:

DEBUNKING APPLE'S BIGGEST MYTHS

Apple bills itself as a champion of security, privacy, and the consumer. The company uses this reputation to justify its anti-competitive App Store practices and guidelines, and to maintain its dominance in the marketplace. Apple regularly

promotes the App Store as a safe and trusted place for users to download the apps they love and as a great business opportunity for developers. But Apple's claims don't match up with reality. It's time to separate the myths from the facts.

MYTH: "We treat every developer the same. We have open and transparent rules, it's a rigorous process. Because we care so deeply about privacy and security and quality we do look at every app before it goes on. But those rules apply evenly to everyone."

- [APPLE CEO TIM COOK](#)

FACT: Apple gives special treatment to its own apps and the tech giants who cut deals with them, creating a broken marketplace for developers and consumers alike.

Not only is Apple not forced to pay the same steep fees as their competitors on the App Store, but they are also not subject to the same rules. These fees and rules have routinely been bypassed by large companies who have Apple's blessing. The unlevel playing field hurts consumers through a lack of choice and reduces opportunity for startup and growing companies.

EXAMPLE: Amazon is not subject to the 30% app tax after cutting a deal with Apple.

The same deals and preferential treatment are not given to small and medium-sized companies. In another example, Apple Arcade has flourished on Apple's app store. Meanwhile some rival game makers have been shut out of the platform due to Apple's restrictions, which were not placed on their own app. Those apps that are offered in the app store are also disadvantaged because Apple Arcade is not subject to the same fees, disclaimers, and roadblocks as competing apps.

MYTH: "If you force other software onto iPhone...you undermine the privacy, security, safety, and performance that is built into the iPhone by design."

- [APPLE'S CHIEF PRIVACY ENGINEER ERIC NEUENSCHWANDER](#)

FACT: Apple has always allowed “other software” on its Mac computers and iPhones. The company only has “security concerns” when its competitors want a level playing field.

Apple allows several tech giants to use their own payment systems on the iPhone. However, they force smaller developers and their customers to use Apple’s payment system if they do not sell physical goods, allowing Apple to extort up to a 30% app tax. They prevent developers from creating software that meets their privacy standards, because no such standards exist.

EXAMPLE: Apple allows alternative payments for Instacart, Uber, AirBnB, and Grubhub, but for apps with subscriptions and digital payments – like your Spotify, Epic, and Match apps – Apple charges a 30% tax through their in-app purchasing system.

MYTH: “The App Store is designed to be a safe and trusted place for users to get apps, and a great opportunity for developers to be successful. We do not tolerate fraudulent activity on the App Store, and have stringent rules against apps and developers who attempt to cheat the system.”

- [STATEMENT FROM APPLE](#)

FACT: Apple’s “standards” are inconsistently applied across apps, and only enforced when they benefit Apple’s business - exposing consumers to scams.

How apps and developers are treated by Apple boils down to one thing - whether or not they pose a threat to Apple’s bottom line. The App Store has been accused of approving and distributing “scam apps” that target and deceive consumers so long as they do not compete with Apple’s apps. Inconsistently enforced rules and lax moderation allow scam apps and apps that clone

software from other developers to run rampant, “siphon[ing] money away from consumers under false pretenses using exploitative subscription services.”

EXAMPLE: Scam apps that mimic FlickType, the Apple Watch keyboard app, were sold on the App Store, netting the scammers millions of dollars.

Fake apps like these skyrocket to the top of the App Store using fraudulent reviews, hurting the original app and defrauding consumers. The Washington Post has reported extensively on how scam apps have defrauded app store customers.

MYTH: “We at Apple believe that privacy is a fundamental human right. But we also recognize that not everyone sees things as we do. This is surveillance, and these stockpiles of personal data serve only to enrich the companies that collect them.”

- [APPLE CEO TIM COOK](#)

FACT: Apple’s claim of opposing ad-supported business models is a hypocritical falsehood.

Apple profits from collecting and monetizing people’s personal data, even if not as well-known as other large, ad-driven businesses. Specifically, Apple Search Ads use iOS user data to serve targeted ads that allow app makers to promote their products and move them to the top of searches in Apple’s App Store. They are not getting consent from iPhone users before reading or writing any data on their devices. But Apple holds competitors to higher standards of data collection than it does for itself - making the default for other apps to explicitly ask users to turn tracking on, while Apple’s tracking is automatically turned on. Apple’s supposed opposition to data collection and monetization is nothing more than grandstanding for positive public relations.

EXAMPLE: Apple Search “constitutes an essential marketing channel” for app advertisers, and they continue to reel in more advertisers and expand ad-based revenue.

At the same time, Apple blocks app developers from accessing user data, while exempting themselves from all of their own rules – profiting off the very companies whose business model it publicly critiques.

MYTH: “We are deploying powerful, new requirements to advance user privacy throughout the App Store Ecosystem. The first is a simple revolutionary idea we call the privacy nutrition label. Every app, including our own, must share their data and privacy practices, information that the app store presents in a way every user can understand and act on.”

- [APPLE CEO TIM COOK](#)

FACT: Apple’s privacy labels apply to all... except for Apple’s own products, disadvantaging competitors and leaving consumers in the dark.

EXAMPLE: While WhatsApp’s privacy label is visible on the App Store before downloading, Apple’s pre-downloaded Message app doesn’t have an easily visible privacy label.

To find Message’s privacy label, users have to navigate to Apple’s website. However, the average user isn’t likely to know that this webpage exists. Additionally, as privacy labels are often checked before downloading an app, and the Messages app is pre-installed on a new iPhone, most users will not consider checking the privacy label. This obscures the privacy information for Apple’s apps, while highlighting its competitors’.

bottom line

While Apple claims to be committed to its users, it hides behind false claims to install anti-competitive, monopolistic roadblocks that undermine app developers and hurt consumers. It is time for Apple to be held accountable for these practices. Consumers and app developers deserve an open and fair marketplace. It is time to open the app store.

contact

info@appfairness.org



CAF
appfairness.org