Online Platforms and Market Power Part 6: Examining the Dominance of Amazon, Apple, Facebook, and Google

Questions for the Record from the Honorable Guy Reschenthaler

Questions for Tim Cook, CEO, Apple, Inc.

1. What is Apple's current revenue from advertising growth, and what is their expected growth? What steps has the company taken in their advertising business to protect user privacy?

Apple generates very little of its revenue from advertising. Ads that are delivered by Apple's advertising platform may appear on the App Store, Apple News, and the Stocks app. Apple's advertising platform has been carefully designed to adhere to Apple's privacy standards. Our advertising platform is designed to protect user information and give users control over how we use their information:

- Apple's advertising platform does not share personally identifiable information with third parties.
- Apple's advertising platform does not track users across companies. We define tracking as 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 advertising or advertising measurement purposes or sharing user or device data with data brokers.
- Apple's advertising platform is limited from using information about the user for ad targeting (i.e., to serve more relevant ads to the user), if Personalized Ads is turned off on the user's device. Users can turn off Personalized Ads on their iOS or iPadOS device by going to Settings > Privacy > Apple Advertising and tapping to turn off Personalized Ads. On Mac, they can go to System Preferences > Security & Privacy > Privacy, select Apple Advertising, and deselect "Personalized Ads."
- We create segments, which are groups of people who share similar characteristics, and use these groups for delivering targeted ads. To protect user privacy, targeted ads will be delivered only if more than 5,000 people meet the targeting criteria.
- Users can see information about them that may be used to deliver targeted ads by Apple's advertising platform, including the segments that they are in. To see this information on their iOS or iPadOS device, users can go to Settings > Privacy > Apple Advertising and tap View Ad Targeting Information. On Mac, they can go to System Preferences > Security & Privacy > Privacy, select Apple Advertising, and then click View Ad Information. If users believe their listed account information is inaccurate, they can update their Apple ID account information. Users have the ability to understand why a specific ad was shown to them on the App Store, Apple News, or Stocks, by tapping the "Ad" button on the ad. This will present the segments and other data, such as demographic information, that were used to determine which ad they received.
- Apple does not know or make available to advertisers information about the user's sexual orientation, religious beliefs, or political affiliations.
- No Apple Pay transactions or Health app data is used by Apple's advertising platform.
- A user's precise device location is not stored by Apple's advertising platform, and profiles are not constructed from this information.
- Users can opt out of the use of device current location by Apple's advertising platform. Users can opt out on their iOS or iPadOS device by going to Settings > Privacy > Location Services, selecting App Store or News from the list, and setting it to Never. On Mac, they can go to System Preferences > Security & Privacy > Privacy, select Location Services, and deselect "News." Apple's advertising platform also does not receive location-based information when

Location Services is turned off on the device.

2. Did Apple reduce ad measurability in iOS 14? If so, why?

Apple has viewed privacy as a fundamental human right long before it became trendy. As Steve Jobs explained in 2010: "We've always had a very different view of privacy than some of our colleagues in the Valley. We take privacy very seriously."[1]

Apple has a track record of designing privacy protections into its products. Data privacy and security are fundamental pillars of the App Store and are crucial elements of its success. Consumers trust that Apple will equip them with tools to control the data they share with apps, and that Apple seeks continuously to improve the App Store's user privacy and security features and to confront novel privacy and security risks.

iOS 14 will give users even greater control and transparency over their data. Developers will be required to obtain the user's permission before tracking that user's activity across other apps. This change will enhance transparency for users and further empower them.

We define tracking as 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 advertising or advertising measurement purposes or sharing user or device data with data brokers. An example of tracking is displaying targeted ads in an app based on user data collected from apps and websites owned by other companies. Another example is sharing a list of emails, advertising IDs, or other IDs with a third-party advertising network that uses that information to retarget those users in other developers' apps. When a user is tracked, her data can end up in the hands of other companies without the user knowing. We believe users should be aware of this practice and should be able to choose whether their data is used and shared in this manner. It is not considered tracking when the data is linked solely on the user's device and not sent off the device in a way that can identify the user or device externally, or when the data broker uses the data shared with them solely for fraud detection or prevention or security purposes, and solely on the developer's behalf.

In iOS 14, when a user declines to give permission to be tracked, Apple will not provide the Identifier for Advertising ("IDFA") and will relay the user's choice to the developer. When enabled, a system prompt will give users the ability to allow or reject tracking on an app-by-app basis. To be clear, we are not prohibiting tracking—a developer will still be able to track users with the IDFA and other means so long as they gain user permission. This change reflects Apple's ongoing efforts to add innovative privacy features into each new generation of its software.

Apple recently announced that it would delay the implementation of this feature in iOS 14 to give developers more time to make the necessary changes. The requirement to use this tracking permission will go into effect early next year.

At the same time, Apple is developing an innovative solution to help developers with a more privacy-friendly alternative to tracking that they may use for advertising attribution and, by extension, measurement of in-app advertising. For many developers, tracking is a side effect of trying to answer business questions like which advertising campaign is most effective. Apple is making major improvements to SKAdNetwork, a free framework that gives developers a privacy-friendly way to understand advertising performance. SKAdNetwork is engineered to hold advertising data on-device

[1] *See* Paul Resnikoff, *What Steve Jobs Said About Protecting Privacy In 2010*, Digital Music News (Mar. 25, 2018), https://www.digitalmusicnews.com/2018/03/25/steve-jobs-user-privacy-2010/.

separate from apps, allowing advertising conversion measurement to be reported without users being tracked. By way of example, if a developer decided to advertise its app through ads in other apps, SKAdNetwork can help that developer determine which ads led to how many app installations and new user acquisitions. With SKAdNetwork, third-party advertising networks serving ads across a wide variety of apps can provide advertising attribution to developers without knowing the identity of the user. Apple doesn't monetize this API. SKAdNetwork is free to use.

3. Does Apple have plans to open iOS 14 to alternative app stores?

No. Apple has no plans to open iOS to alternative app stores. Not only would allowing third-party app stores be inconsistent with Apple's longstanding and consistent approach to product development, it would also create significant privacy, performance, and security vulnerabilities.

The App Store is an integral part of the integrated iOS experience and a feature of the iPhone. Customers buy iPhones for the whole experience—from unparalleled design, to cutting-edge technology, to the first truly mobile operating system, to services and software. Having one app store on the iPhone allows us to fulfill our promise to our customers that the apps they download will meet our high standards for privacy, performance, and security.

Nothing is more important to Apple than maintaining the trust of its users. The App Store ensures that Apple delivers on its promise that apps are held to a high standard for privacy and security. Apple has reviewed every app distributed through the App Store since the opening of the App Store in 2008. Apple expended significant effort to put various "controls in place," allowing the company to "turn off the spigots" when harmful third-party apps are detected.[2] This is critical, as the iPhone operates in a different environment than a computer. Products like the iPhone could offer access to a trove of users' personal data—data that unscrupulous actors could seek to collect or exploit. As Steve Jobs explained in 2007, "[y]ou don't want your phone to be like a PC. The last thing you want is to have loaded three apps on your phone and then you go to make a call and it doesn't work anymore."[3]

Apple's rigorous App Review process is designed to protect users and developers alike from fraud, malware, and unwarranted intrusion into their privacy. Apple reviews, on average, 100,000 submissions for apps or app updates per week—most within 24 hours of submission. This process includes roughly 1,000 calls per week to developers to diagnose and cure issues. Apple rejects approximately 40% of the reviewed apps. Many of these apps are rejected because they have software glitches or bugs, and/or would compromise users' data privacy or security. There is a significantly smaller number of malicious iOS apps than those available on Android.[4] In 2018, the iPhone platform accounted for just 0.85% of malware infections. By contrast, Android accounted for 47.15% and Windows/PC accounted for 35.82%.[5] And among app stores, Android app stores have significantly higher numbers of malicious apps than the App Store.[6]

Incorporating third-party app stores into iOS would undermine Apple's carefully created privacy and

[2] *Steve Jobs Introduces the App Store – iPhone Software Roadmap Event*, YouTube (Mar. 6, 2008).

[3] John Markoff, *Steve Jobs Walks the Tightrope Again*, N.Y. Times (Jan. 12, 2007), https://www.nytimes.com/2007/01/12/technology/12apple.html.

[4] *Internet Security Threat Report*, Symantec, at 11 (Apr. 2016) ("Apple is well-known for its stringent screening processes, which is why the number of malicious iOS apps is so much smaller than for Android."), https://docs.broadcom.com/doc/istr-21-2016-en.

[5] *See Nokia Threat Intelligence Report – 2019*, Nokia, https://pages.nokia.com/T003B6-Threat-Intelligence-Report-2019.html.

[6] *See* Jordan Herman, *2019 Mobile App Threat Landscape Report*, RiskIQ (2019), https://www.riskiq.com/research/2019-mobile-threat-landscape-report/.

security safeguards, and would seriously degrade the consumer experience and put Apple’s reputation and business at risk. Apple would have no reliable way of delivering on its commitment to consumers that every app available for download meets Apple’s rigorous standards for security and privacy.