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

Questions for the Record from the Honorable Ken Buck

Questions for Tim Cook, CEO, Apple, Inc.

1. **Apple has reduced the measurability of ads in iOS 14. Is Apple pushing developers to monetize their apps through in-app purchases and subscription services? What impact would such ad monetization have on independent developers and innovators seeking to build sustainable businesses.**

Apple has long made consumers a promise that it will do everything it can to ensure that the user has transparency over the data that could be collected about them and control over that data. The decisions to introduce new privacy enhancements and controls year after year is not driven by commercial interests. Apple is not pushing developers to monetize their apps through in-app purchases or subscription services in iOS 14. Apple's decisions are driven by what it believes are the best interests of the consumer. The changes in iOS 14 empower the consumer, not Apple.

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 continuously seeks to improve the App Store's user privacy and security features to confront novel privacy and security risks.

iOS 14 empowers consumers by giving them a greater ability to control their data. It is not intended to reduce the measurability of ads. Rather, the changes in iOS 14 will require developers to obtain user permission in order to track users across different developer apps and company websites. The consumer will get to decide, and we believe that is unambiguously a good thing. Having listened to developers, we want to give them sufficient time to make the necessary changes, and as a result, the requirement to use this tracking permission will not go into effect until early next year.

Apple is not pushing developers to monetize through in-app purchases and in-app subscription purchases. The intent of these changes is to put users in charge of their data and their devices, and we are doing this because we believe it is right. We believe that Apple's new tracking protections will spark further innovation that respects user privacy and inspire developers to treat privacy as a chance to innovate and to build trust with their users while building great businesses.

The App Store has become a great business opportunity for all developers, including independent developers, and allows for a number of business models that do not monetize through in-app purchases or subscription services. Apps with different business models have flourished on the App Store: (1) apps that are ad-supported, (2) apps with sales of physical goods and services, (3) apps where users consume or access content that they purchased or subscribed to outside the App Store, and (4) apps that have some other business model not generated from app revenue. Since the launch of the App Store, an entire industry has been built around app design and development, generating over 1,500,000 U.S. jobs. When distributing through the App Store, independent and small developers get immediate access to the free

[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/.

tools, technology, and software that Apple has created to help developers distribute their apps to one billion App Store customers around the world.

2. Mr. Cook how frequently does Apple's iPhone report location data of its users back to Apple for advertising purposes?

Apple's advertising platform does not access a user's device location unless they have enabled Location Services on their device and they have granted permission to the App Store or Apple News apps—where Apple offers its ad services—to access their device location. Users can disable Location Services, as well as change Location Services permissions for App Store or News, on their iOS or iPadOS device by going to Settings > Privacy > Location Services. Apple's advertising platform does not receive device location information when a user turns off Location Services on their device or does not grant permission to the App Store or Apple News to access location.

If the user grants the App Store or Apple News access to device location, Apple's advertising platform may use the current location of the user's device to provide the user with geographically relevant ads on the App Store and on Apple News. Apple's advertising platform does not store the user's precise device location and does not construct profiles from this information.

In iOS 14, users can choose to share only their approximate location with an app, even if the app asks for precise location. For Apple News, users can limit access to approximate location. The App Store only requests approximate location.

3. The App Store is the only practical way for app developers to reach iPhone and iPad users. I'm concerned that Apple is using this power to dictate the terms of service for app developers. This prevents app developers from controlling their own services and insulates Apple from competition. How will Apple ensure that free choice by app developers and app users will drive innovation in user experience, privacy, and security?

I respectfully disagree with the premise that "the App Store is the only practical way for developers to reach iPhone and iPad users." We believe that the App Store is a great choice for developers to reach Apple customers, but it is not the only choice. Distribution of digital content over the Internet remains an important option for developers. This includes developer websites and web apps (like those available from Instagram and Starbucks), which can be accessed through any web browser on iPhone and iPad. Indeed, many developers interact with users on their websites, including by allowing users to purchase digital content, and then making that digital content available through their iOS apps. The App Store terms and conditions, including its commission, do not apply to any transactions that take place through a web browser or web app.

The App Store also competes directly with software distribution on other smartphone platforms—including Google Play, Samsung Galaxy, and Amazon app stores—as well as across a range of devices that is growing larger and more diverse. Every desktop computer, notebook, television, phone, camera, car, game console, tablet, speaker, eBook reader, watch, and more are becoming methods of distributing software to consumers. This list will continue to grow with the emergence of 5G. These are all options for developers, and this competitive dynamic drives Apple to innovate and create new features and technologies to convince developers to create great apps for iOS.

We do not prevent developers "from controlling their own services." The guiding principle of the App Store is to provide a safe, secure, and reliable experience for users on their devices and a great opportunity for all developers to be successful. Our users trust Apple—and that trust is also critical to how we operate a fair, competitive store for developer app distribution. We believe competition makes

everything better and results in the best apps for our customers. We support third-party app developers and we want them to succeed, so we created the App Store to give developers a great opportunity to reach our customers.

And we work hard to get third-party apps into the App Store, not keep them out. We started the App Store with just 500 apps, and in just 12 years, we now have about 1.8 million apps. Apple's own apps represent a tiny fraction of the apps available on the App Store. In every category where our software competes, we face strong competition from numerous successful apps. For example, iCloud competes with Box, DropBox, Google Drive, Microsoft OneDrive, and so on. Mail competes with Gmail, Microsoft Outlook, Spark, Yahoo Mail, and others. Apple Music competes with Amazon Music, Pandora, Spotify, YouTube Music, and others. Apple's business incentives are completely aligned with promoting competition and choice by developers and users.

We want a vibrant and rich app ecosystem because that is what our customers want. We remain committed to ensuring our customers have the best possible experience. We have a fundamental interest in making sure that our platform and the apps on our platform will continue to drive innovation in user experience, privacy, and security. User experience, privacy, security, and innovation are the values on which we compete.

Questions for Jeff Bezos, Tim Cook, and Sundar Pichai

1. **Do you employ end to end encryption for communications on your products in China?**

Apple makes products for customers, not countries—we design them with privacy and security woven in, regardless of where they are sold or used. That is why, all around the world, our products are equipped with the same encryption and security features. The encryption that we use for each of our services is described at <https://support.apple.com/guide/security/welcome/web>. Apple's iMessage and FaceTime communication services are end-to-end encrypted everywhere in the world, including in China.

2. **Do you provide user enabled and controlled encryption on the communications devices you sell in China?**

We do not provide any way for users—anywhere in the world—to reduce the strong levels of encryption that our devices use.

3. **Do you provide China and the Chinese Communist Party access to users' information and content as required by Chinese law?**

Apple only provides information or content to law enforcement when we receive a request from law enforcement that is narrowly tailored, provides a valid legal basis, and provides an appropriate jurisdictional scope. We carefully vet every request to ensure it is as narrow as possible and jurisdictionally appropriate. We do not allow backdoors into our devices or servers. We do not provide information or content in response to bulk requests.

More details about the cases in which we provide information and content to law enforcement are available in our transparency report at <https://www.apple.com/legal/transparency/>.

4. **What user information or content do you provide the Chinese government under Chinese law?**

Requests for customer data are received from government agencies related to device, financial identifiers, account, and emergency matters involving imminent danger. Requests can be made in various formats such as subpoenas, court orders, or warrants. If we determine a request does not have a valid legal basis, or if we consider it to be unclear, inappropriate, and/or over-broad, we challenge or reject it.

A detailed listing of the requests we receive from global law enforcement is available in our transparency report at <https://www.apple.com/legal/transparency/>. We publish these reports so customers can understand how their personal data is managed and protected.

5. **If you deploy Artificial Intelligence to identify illegal content consistent with Chinese law:**

    - **What data points does your AI examine?**
    - **How is your AI trained to identify and keep up with the changing language, vocabulary and codes used by pedophiles and other criminals**?

We do not use artificial intelligence to identify illegal content under Chinese law.

6. Does China require you to submit either your encryption of AI algorithms to Chinese authorities for technical evaluation before you are permitted to deploy them in China?

No.

7. Does China require providers to back up the contents of all devices into the either the company's data center or a government data center in China?

China does not require that all devices have their content backed up. China's 2017 Cybersecurity Law requires that some personal information and content from Chinese citizens be hosted in data centers in China. The iCloud service in China is subject to this requirement. Chinese citizens who use Apple's iCloud service and choose to back up their devices will have their data backed up to servers hosted in China. iCloud users who do not have "China" selected as their country do not use Apple's iCloud service in China. "China" can only be selected in device settings by users that have a China Apple ID, which requires a local phone number.

8. Does China require information on any or all of your devices that access the Chinese cellular telephone infrastructure or Internet to backup their content and user information in Chinese datacenters? Does this apply to tourists and business travelers, to include United States citizens?

As noted in response to Question 7, we do not store content or information inside China for our users unless they have selected "China" as their country.