Before the
U.S. Department of Commerce
National Telecommunications and Information Administration
Washington, DC 20230

In the Matter of Developing a Report on Competition in the Mobile App Ecosystem	Docket No. 220418–0099

COMMENTS OF PUBLIC KNOWLEDGE

Public Knowledge welcomes the opportunity to offer these comments for the NTIA's forthcoming report on competition in the mobile app ecosystem. The app ecosystem is a pillar of the digital economy and a source of much innovation. Unfortunately, many of the valuable tools and business models that have made mobile devices, in general, more secure than traditional desktop computers, and that have made apps and app stores commercial successes, can also be used to harm competition. Policymakers can and should pursue policies that open up mobile devices to more competition without opening them up to bad actors and malware. Despite rhetoric from opponents of increased competition, this is more than feasible. It's necessary. The distribution and control of software on dominant platforms cannot be left in the hands of the platform vendors alone.

It is hard to fashion bright-line rules or tests in this area, in large part because technology is so malleable. One platform might offer a feature as part of an app, another might bake it into the operating system, or the hardware of a device itself. Policies designed to enhance competition should be written in a way that implementation details like this do not frustrate their aims. NTIA's report should help policymakers do this, offering not only data on the state of the market, but, as a technical, expert agency, how the state of competition for apps relates to the technical features of mobile devices, and the legitimate threats that users face from bad actors and malware.

2. Are there any important and specific entities (or categories of entities) such that it would be a mistake to omit—or improperly include—them by defining the "mobile app ecosystem" to focus on mobile devices, such as phones and tablets?

The focus on mobile devices is appropriate. Like any market definition question, the proper starting point is consumer behavior. General purpose mobile devices like smartphones and tablets do not compete in the same market as dedicated devices, like gaming consoles or e-readers, that are optimized for fewer uses (even though all these things are in a technical sense just different kinds of computer). And, while high-end tablets might be substitutable with laptops for some users, in general, tablets and smartphones are complementary to desktop and laptop computers that run "desktop" operating systems.

2b. For example, should mobile apps offered specifically for enterprise use (e.g., for use by businesses, not for consumers) be considered in this study?

4. How should web apps (browser-based) or other apps that operate on a mobile middleware layer be categorized?

(Answer to 2b and 4)

Enterprise apps that are offered directly by businesses to their employees, and that are not available for use by ordinary consumers, should not be part of this study. Enterprise apps are apps, but they are not part of the consumer app market (and may offer different functionality than is available in consumer apps).

One aspect of the app market the study should consider is the extent to which different apps in the app store use standard APIs and operate under standard terms with the platform, or whether they have negotiated special deals (e.g., a lower percentage for in-app purchases) or use private APIs or entitlements that are not available to ordinary app developers. For example, iOS developers that want to use CarPlay (integration with car infotainment systems) must request it specially from Apple; CarPlay is otherwise not available to third-party developers. Recently, Google has entered into special deals regarding app store terms with Epic Games, Spotify, and the Match Group.[1]

Web apps should only be considered to the extent that they have identical performance and capabilities as native software—according to both technical benchmarks, and in terms of user-facing features, appearance, and performance. Additionally, the discovery and management of such apps must be as easy as installing software from an app store. Absent these things, while web apps remain a valuable release valve for some kinds of software and content that is not available on app stores, they should not be considered substitutes for native software. This is for two reasons: first, web apps cannot be considered substitutes for native applications until they are truly comparable. But also, on both iOS and Android, the platform vendor controls both the primary (or only) app store, and the web browser and rendering engine that web apps require. In the case of Apple, developers have long complained that Apple limits the functionality of web apps to benefit its app store. A company should not be able to benefit from an expanded market definition that downplays its competitive significance while also taking steps to limit the true competitive potential of the web.

5. There are some indicators that there is a difference in kind between some apps that generate large amounts of money or are downloaded often and most other apps. For example, one industry analyst reported that 97% of publishers that monetize through the Apple App Store earned less than $1 million per annum in 2021, compared to other reports of more than $1 billion earned by the top 13 apps (including games) on both Apple and Google platforms.[23]

[1] https://techcrunch.com/2022/05/23/epic-games-bandcamp-temporarily-wins-right-to-use-its-own-payments-system-on-google-play; https://newsroom.spotify.com/2022-03-23/spotify-and-google-announce-user-choice-billing/

What is the best way to assess the competition environment for less popular apps and start-ups?

a. Can any potential harms, such as deficiencies in data security and privacy protections, be traced back to the current market imbalance?

b. Is there evidence to suggest that consumers are less likely to avoid or stop using a particular app even if they would prefer a more privacy enhancing environment because of a lack of competitors offering similar services?

Smaller developers can be disadvantaged due to market pressure driving the initial cost of most apps to zero, with monetization happening though ads, in-app purchases, subscriptions, and other things. Monetization strategies of these are more complex and riskier than with traditional a la carte software purchases, and users might be more comfortable with paying a subscription to a major, established company like Microsoft or Adobe, than to a new entrant.

In this market, a user might download a free app instead of a paid one, and might prefer to see ads than to pay for some rarely-used app. But that app or its adtech vendor might be harvesting personal data and selling it to data brokers, unbeknownst to the user. This creates a market pressure in favor of apps that engage in these unscrupulous behaviors. Just as the dominance of a particular app cannot always be separated from the dominance of the company that creates it, or the service it is a window to, a full assessment of competition in the app space may also have to include privacy, data security, and other factors that can have effects on app competition. A more competitive marketplace does not and should not mean a race to the bottom in terms of user privacy, and a strong nationwide privacy law would likely benefit competition and new entrants, while reducing the dominance of incumbent developers and the strength of platforms.

9. What role does interoperability play in supporting and advancing a competitive mobile app ecosystem?

a. What are the key characteristics of interoperability as it relates to the mobile app ecosystem?

b. What other barriers (e.g., legal, technical, market, pricing of interface access such as Application Programing Interfaces [APIs]) exist, if any, in fostering effective interoperability in this ecosystem? How are these barriers different or similar than those present in other ecosystems?

c. How does data portability, or lack thereof, factor into consumers keeping the same app if they switch from one operating system (iOS or Android) to another? [29]

Interoperability is a cornerstone of a pro-competition approach to technology policy. But it is a broad term, and more than meaning different things to different people (though it does), there are different, sometimes incompatible, ways to achieve interoperability even within the same market, and some forms of interoperability may come with heavy tradeoffs, others not at all. Identifying the places where and how interoperability, writ large, might benefit the mobile

app ecosystem would be a substantial undertaking. Here however Public Knowledge can offer initial thoughts regarding promising approaches and potential pitfalls.

The strongest case for interoperability in the mobile app ecosystems is 1) enabling users to switch from one app to another, and from one platform to another, and 2) enabling users to communicate between apps, and between platforms.

A lack of data portability (data that can be exported from one app or platform, and imported into another, by a user with limited technical expertise) can a barrier to interoperability. The NOI asks about barriers to users "keeping the same app" moving from one platform to another. One barrier might be that an Android app does not exist on iOS or vice versa. Or, a developer, having expended signifiant resources creating paid iOS and Android apps, might prefer a user to buy the new platform's version of app if she switches.[2]

These issues aside, and considering that many apps are free, it may be beneficial if there was a way for users to port a list of apps from one platform to another and to automatically install corresponding apps on the new platform. Even measures that merely reduce friction and hassle for users can benefit competition and aid switching. But still other barriers might remain: Not just apps are purchased, but in-app purchases and subscriptions. A developer's app on one platform might make use platform features that make moving data even to another app from the same developer difficult.

Competition between software platforms like Android and iOS is good. This means that they should be able to differentiate from each other, each adding new features and capabilities to win over users and developers. Interoperability does not require uniformity, [footnote: This is is not to downplay the important role of standards even in operating system design. See POSIX.] and it may be difficult for a user to switch from one platform to another, or for a developer to write apps for different platforms, if certain operating system features that exist on one platform do not exist on the other. Such a feature may be valuable differentiation, or anti-competitive lock-in. For example, one platform may offer audio APIs that make it easier for developers to create podcast or music apps. The other might not. Porting an app from the first platform to the second might require the developer to re-implement low-level audio processing functions that might be highly technical—and so, it might not happen. But this is not a "barrier" to competition, provided that developers are not *forced* to use features (e.g., proprietary cloud storage or authentication) that are not available on other platforms. Different platforms trying different things to attract users and developers is generally beneficial—provided that platforms remain free, as they are today, to copy good ideas from each other, and to reverse-engineer and re-implement each other's proprietary APIs and features free of baseless legal threats. *See Google v. Oracle*, 141 S.CT. 1183 (2021) (it does not infringe copyright to re-implement an API for the purpose of attracting developers already familiar with it on another platform).

[2] An iOS and Android app might be in some sense "versions" of each other but they are not "the same app," even if they look and behave the same to users. While the only barrier to accessing some kinds of content such as books and movies on different platforms and in different apps is artificial (digital rights management), apps typically need to be written specifically for, and tailored to, a particular platform.

13. Some mobile apps are pre-loaded on mobile devices or set as default apps, while others are only available through an app store, through a browser (web apps), or, for devices using the Android system, by sideloading. Is there data comparing these mechanisms and their effect on app distribution?

a. Is there a competitive advantage to being preloaded or available by default to the users of phones and tablets? What is the evidence to support or contradict there being an advantage? [30]

b. Is there data on the number of developers that have been able to have their apps preloaded or available as default apps or the types of apps?

c. What information is available on the types of agreements these developers reached and with whom to preload or set their app as a default app?

Customers expect a certain number of basic apps to be pre-loaded on their phones—and phones would be considered broken if they did not come with basic apps like a web browser, an email client, or a calendar. Yet the anti-competitive harms of preloaded and bundled apps, including from app functionality that is included directly in an operating system, are well-known. Not only is it "hard to compete with free" (even though many "free" apps carry hidden costs), but the power of defaults alone has major competitive implications.

There are many ways to balance the need for a minimally functional out-of-the-box device with the goal of ensuring competition. As a start, all default apps should be un-installable, and users should have the ability to install third-party apps as defaults. But features like this, while welcome, will never completely overcome the advantage apps have from coming pre-installed on user devices. In some cases, a dominant platform vendor pre-installing its own app, or that of a partner, maybe be so competitively harmful that it should not be allowed. It may be very fact-intensive to determine when this is the case, but one starting point is to examine which pre-installed apps (or operating system features) are truly offered to users as part of the initial sale, or not. Apps that are pre-installed on a phone that require a separate purchase or subscription (regardless of whether there was a "free trial" or some other promotion) or has some other monetization strategy, such as ads or the collection and sale of user data, are more likely to be harmful to competition, and to offer limited consumer benefit. Additionally, treating a bundled app as an additional source of revenue is a good indicator that it is a separate product that is simply tied to a different product, as opposed to a natural evolution of the minimum feature set of a mobile phone.

15. How do, or might, alternative app stores (other than Google Play or the Apple App Store), affect competition in the mobile app ecosystem?

a. What data is there to assess how well existing alternative stores distribute apps, in general or specific types of apps?

b. What unique barriers are there affecting each of the main operating systems (Android, iOS) that might prevent web apps or—to the extent allowed on Android system—alternative app stores and sideloading, from gaining more popularity with users and app developers than they currently have?

c. Is there analysis comparing competition on iOS ecosystem (where app distribution is limited) to that of alternative distribution mechanisms on Android operating systems?

Sideloading (including the sideloading of alternative app stores) is one of the best ways to increase user choice in the mobile app market. It gives users the option of installing apps that are not or cannot be made available on app stores, forces platform app stores themselves to compete and improve, and it provides a release valve for free expression and other values that are harder to quantify in a purely economic analysis.

Sideloading exists on Android, but it's a cumbersome process that, because Google does not require sideloaded apps to be cryptographically signed by developers, does carry more risk than necessary. But this specific implementation should not be taken to mean that sideloading is not important, or is risky—after all, most Windows and Mac software, to this day, is "sideloaded,"[3] not installed via an app store, and on iOS, developer-installed and enterprise apps have to be signed just as app store ones are.

16. What evidence is there to assess whether an app store model is necessary for mobile devices, instead of the general-purpose model used for desktop computing applications?

The goals of privacy, security, and competition are not at odds, and increasing competition in the app ecosystem does not require that platforms discard the valuable technical protections they have built in to devices and operating systems to protect users from bad actors, malware, and even from inadvertently misconfiguring their devices, or installing software that harms their device performance or battery life.

The security and privacy enhancements present in mobile operating systems are there in part because of lessons learned from desktop operating systems. It is good that an app, by default, cannot see the data saved by other apps, due to sandboxing. It is good that apps cannot store data and executables wherever they want on a device's storage, that apps are limited in the background tasks they perform, and that deleting an app on a mobile operating system fully deletes all of its components. It is good that apps cannot access sensitive data like photos, contacts, or location information without express user opt-in.

App stores, too, are beneficial, in that they make finding and installing software much easier for ordinary users. The policy problem is not that these things exist, but that they are abused for business reasons, or in the case of app stores, monopolized.

[3] Like "acoustic guitar," "sideloading" is a term that did not need to exist until a newer alternative was invented. Just as acoustic guitars used to just be "guitars," and "sideloading" software used to just be called "installing" software.

Policymakers and those interested in increasing mobile app competition can do so without compromising privacy and security. This requires not only expertise in how markets function, but about the threats users face from bad actors and malware, how mobile devices and operating systems protect against them, and how platforms have addressed similar challenges before.

18. Are there other areas, specific technologies or procedures, that offer lessons on more and less successful ways to screen out problematic apps? What are the characteristics of such success?

a. Are there good examples by enterprise users? [35]

b. For example, some devices allow sideloading only after warning the user to make sure they trust the app before proceeding with the download, in a way similar to how some browsers issue warnings for unknown websites. What material exists about the efficacy of such methods?

c. What roles, if any, do independent or third party security testing play in the app store ecosystem?

d. Does the current model discourage competition and innovation in the development or advancement of security testing?

Sideloaded apps are not inherently more risky than app store apps from a technical perspective. They can be subject to the same security protections, sandboxing, and permission models that app store apps are subject to. These technical security features are the first line of defense, protecting users, and they are not related to app stores or app store policies.

The primary difference between app store apps, and sideloaded apps is one of policy. App stores can reject apps that engage in certain behaviors that it is hard to put a stop to via technical means, and the abuse of certain kinds of APIs can best be addressed via policy choices. For example, many of the same technical capabilities that are useful for parental control services can also be used for "stalkerware." But there are ways of addressing these issues besides anticompetitively preventing users from accessing apps from sources other than platform app stores, and different app stores might enforce policy restrictions of this kind better than the first-party app store itself does. For example, in a more competitive app market, a third-party store might specialize in apps that highly value user privacy, dedicated more resources to vetting these apps for policy compliance, and even putting into place stronger policies.

Of course, policymakers and regulators around the world have recognized that app store "policies" can be anticompetitive—policy, not technological limitations, is all that stands in front of app developers and a more competitive billing market, for instance.

Public Knowledge believes that users should be able to sideload apps if they so choose, and that sideloaded apps can have the same security protections as app store apps (including sandboxing and code-signing). Informing users that sideloaded apps are not subject to policy

review may be appropriate, but it would be inappropriate for a platform to imply that sideloaded apps are riskier from a technical perspective, or to imply that they have greater access to personal data than app store apps.

24. Some apps make use, or would like to make use, of additional mobile device components beyond those that are more commonly accessible (e.g., camera, microphone, contacts) in order to offer an innovative product or service, but the operating system or device provider does not allow such access.[36]

Similarly, for some apps, it might be essential to be able to interconnect to other hardware and services, such as cloud services. What are the valid security concerns and technical limitations on what device functionality an app can access?

a. What factors should be considered in striking a balance between encouraging companies to ensure proper security measures, while allowing third parties to access the protected features that might allow for further innovation and competition?

b. Are there specific unnecessary (e.g., technical) constraints placed on this ability of app developers to make use of device capabilities, whether by device-makers, service providers or operating system providers, that impact competition?

c. Are there other means or factors to consider for mitigating specific risks that would not inhibit competition?

In general, third-party app developers should have the same access to the same user-facing capabilities as the platform vendor's first-party apps, via supported, secure, and well-documented APIs, whether they are hardware or software features. This is the case whether a platform vendor simply gives its own apps capabilities not available to other apps, or has incorporated features directly into the operating system.

As an example, some time ago, Apple made it more difficult for apps to constantly monitor a user's location in the background. This was a beneficial move that benefits user privacy, and even national security. But Apple exempted itself from this rule. It did not do this by giving Apple Maps or another user-facing app special permissions not available to third parties. In fact, Apple Maps (the app) has no special location privileges at all. It doesn't need them, since Apple baked location-tracking into the operating system itself, and it is this tracking information that Apple uses to improve Apple Maps (the service). Apple claims it does this in a privacy-preserving way. In a context like this, the best policy solution would not be to require Apple to allow apps to indiscriminately track user location, but to develop an API that allows other apps or services to make use of location information in the same privacy-preserving way that Apple does. Ensuring a fair marketplace for apps requires addressing this sort of self-preferencing.[4]

Some developers might want more than being able to match the consumer-facing features of a platform or its apps. For example, a developer might want more granular location tracking

[4] *See* John Bergmayer, Tending the Garden (2020) at 49-50, for more on this example.

than Apple itself performs. But a "level playing field" does not depend on an app having the same access to low-level hardware features (here, mobile networking data and GPS) that Apple necessarily can access in its role as the operating system vendor. It is the role of an OS to mediate between apps and a device, but a policy that required platforms to grant third-party apps the same level of hardware access that the operating itself has would be likely be harmful to user security and ease of use, with minimal benefit to competition beyond alternative approaches.

27. What specific measures might the federal government take to foster healthy competition—especially for nascent app innovation—in the mobile app ecosystem?

In the paper Tending the Garden (2020), Public Knowledge put forth a number of policy proposals that, if adopted, would promote app competition and user rights. These include: Permitting sideloading, limiting in-app-purchase requirements to app functionality, ensuring that developers can truthfully communicate with their customers about app store policies, allowing users to set and change default apps, limiting pre-installed apps to essentials, app store transparency, limiting the use of proprietary developer data by platforms, offering secure APIs proactively to new hardware and software features, due process, increased business model flexibility, and more.

Respectfully submitted,

John Bergmayer
Legal Director
PUBLIC KNOWLEDGE
1818 N St. NW
Suite 410
Washington, DC 20782

May 23, 2022