



Developing a Report on Competition in the Mobile App Ecosystem

National Telecommunications
and Information Administration

Docket No. 220418-0099

Comments of Center for Democracy & Technology

The Center for Democracy and Technology submits these comments in the above-referenced matter. We are pleased the NTIA is developing a report on this important subject, and that it is soliciting public input.

Effective competition is essential for making the marketplace work for consumers, and for all who seek to reach them. Competition provides all participants with the leverage of choice – the ability to go elsewhere for a better deal. This means that businesses – all sellers, suppliers, and intermediaries – have a healthy incentive to offer the best deal they can, in order to attract and keep customers. Competition spurs businesses to provide a variety of high-quality products and services at affordable cost, to continue innovating to make their products and services better and more affordable, and to develop attractive and affordable new products and services. Competition is the engine that drives economic progress.

This is true in the marketplace for mobile apps as it is elsewhere throughout the economy. Competition is all the more critical here, as Americans rely increasingly on using the internet for commerce and communication – buying and selling, connecting with others, and creating and receiving information – and as apps account for virtually all time Americans spend on mobile devices.¹ It is essential that the benefits of competition reach the online marketplace, including the mobile apps marketplace, and are protected there.

The state of competition in the mobile apps marketplace is clearly in need of improvement.

¹ See generally Investigation of Competition in Digital Markets, Final Report and Recommendations, H. Comm. on the Judiciary, April 2021, at 93-100, <https://docs.house.gov/meetings/JU/JU00/20210414/111451/HMKP-117-JU00-20210414-SD001.pdf>.

High market concentration in any of the delivery pipelines that connect app developers to app users – from app stores to payment mechanisms -- can create a choke-point. And high switching costs can make it impractical for users to leave one app ecosystem for another. The result will be gatekeeper power – which can be used to hamper or frustrate competition that would give the marketplace alternatives to the gatekeeper – and for the gatekeeper, an innate profit-seeking incentive to use its power that way.

Currently, these delivery pipelines are controlled by two platform ecosystems, Apple’s and Google’s. Their operating system software, Apple’s iOS and Google’s Android, runs virtually every mobile device in the U.S. For Apple, those devices are manufactured by Apple itself. For Google, device manufacturers are subject to contractual requirements on their use of Android. For Apple, users can access apps only through Apple’s app store; on Android, Google’s store is the easiest and therefore most common way for users to obtain apps. This makes the Apple and Google ecosystems essential conduits for app developers to reach users.

Because app developers have little choice but to make their apps compatible with iOS and Android, Apple and Google are able to set the terms for how app developers get access to the technical information and software they need in order to do so. Some of the requirements Apple and Google impose may be necessary to ensure that the apps function effectively and are safe for the devices. Both users and developers can benefit from having familiar and trusted ecosystems for apps.

But the concentrated structure of the app marketplace creates the potential for platforms to impose other requirements that go beyond those purposes and unduly restrict competition. For example, if Apple or Google uses its gatekeeper power to preference its own apps by imposing undue barriers or discriminatory terms on app developers, that restricts the choices available to consumers. Moreover, the app ecosystem can be a source for Apple or Google to gather private data from the transactions between app developers and their customers, which can be a source of anticompetitive self-preferencing if that data is used to gain intelligence on building and improving the platform’s own apps to take business away from competing app developers. Finally, these platforms have the ability to exact a toll from app developers, potentially on every transaction. The size of the tolls Apple and Google exact – as much as a 30 percent cut of the price charged for purchasing an app, and a 30 percent cut of any “in-app purchase” – would not be sustainable in a marketplace where competition offered developers and users other options.²

Addressing market power problems to improve competition in any sector requires a particularized understanding of how commerce in that sector operates. That understanding must include not only how the relationships among market participants are arranged, but the functional means by which commerce is transacted. The technology involved in transacting online commerce is particularly complex, and presents some unique challenges.

A mobile app runs on computer software – both its own, and the operating system software in the device – that stores, processes, and transmits digital information. That’s different than selling products and services in the sorts of walk-in or mail-order or over-the-phone marketplaces that the antitrust laws have traditionally dealt with.

² See generally Final Report and Recommendations, supra n. 1, at 211-223, 333-375.

One consequence of this difference is that remedies to address market power problems – whether through antitrust enforcement actions, new legislation or regulation to reform or supplement the antitrust laws, or restructuring the marketplace to make it more conducive to competition – needs to be designed with special attention to ensuring that they do not have collateral consequences that harm consumers and the marketplace. In particular, such remedies should avoid undermining mobile device and platform security or user privacy.

Apps need to have appropriate access to a device’s operating system, hardware, and software in order to function. Ensuring such access, through required functional interoperability, is viewed by many as showing promise for fostering a more open mobile apps marketplace where competition can better take root and flourish. At the same time, such access presents potential risks to security and privacy if, for example, a developer misuses such access to introduce malware onto a device or to disclose user data for unauthorized purposes.

Fostering competition and protecting privacy and security need not be in tension. To the contrary, in a competitive marketplace, providers might even be spurred to compete to offer more secure and privacy-protective products and services. Ideally, both platforms and app developers would be required to protect user privacy and security by a comprehensive federal privacy law as CDT has long called for. Nevertheless, particularly in the absence of such a law, platforms need to be able to take effective steps to protect privacy and security. For antitrust enforcers, courts, and regulators, the key question is how to distinguish actions that genuinely and appropriately advance privacy and security goals from actions that use privacy and security as a pretext for anticompetitive goals.

Privacy and security are not the only areas of potential collateral consequences that need to be considered in designing remedies to address competition problems in the apps marketplace. Platforms may also legitimately seek to curtail the posting of hate speech, disinformation, or other abusive content through setting and enforcing terms of service. Implementing this content moderation at scale is exceedingly challenging; honest errors, and difficult judgment calls on which reasonable people might disagree, are inevitable. An app provider against which a platform takes content moderation action might wrongly claim it is the victim of anticompetitive discrimination. Here again, care should be taken that competition remedies do not create undue disincentives to content moderation that a platform deems warranted – or even potentially force platforms to host business users that traffic in hate speech, disinformation, or other harmful content.

As a result, to effectively implement remedies to address market power problems in the mobile apps marketplace, enforcers and regulators will need more than their general expertise in antitrust and competition policy. They will need broader expertise across issues such as security, privacy, and even content moderation. And they will require the benefit of technical expertise to fully understand the various points in an app delivery pipeline that could be used as an interface to separate the open, standardized, interoperable parts of the pipeline from the proprietary parts that are appropriately kept secure.

Platforms such as Apple or Google may assert – and may have good reason to – that what appears to the enforcers or regulators be a suitable pro-competitive requirement or remedy is not technologically feasible, or would unduly risk data security or core platform security and

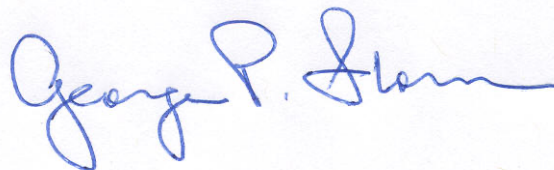
functionality, or other important functions and protections the marketplace is depending on the platform to provide. The platforms will have technical experts to support those assertions. Likewise, app providers will make their own technical assertions backed by their experts.

Enforcers and regulators therefore need the assistance of their own in-house technological expertise, bound to a duty to focus on the public interest, on what is good for the marketplace. The expert perspectives and insights of the platforms and the app developers will be extremely useful, but unavoidably colored by self-interest. Independent non-profit organizations can also contribute informed perspectives, including CDT – even more so when independent researchers are given sufficient access to platforms’ technology. But there is no substitute for enforcers and regulators having their own in-house expertise, sufficient to independently weigh all those perspectives and insights and ultimately arrive at what is workable and effective in the public interest.

One approach NTIA might explore in its report is whether some neutral and independent body might develop standards or best practices that apps could satisfy in order to qualify for access to a mobile device’s hardware or software. That might take the form of a multi-stakeholder process under the auspices of either a government agency or a standards development organization. The process could, for example, examine the types of security- or privacy-related conditions that Apple, Google, and other platforms currently impose, assess whether they are legitimate conditions to protect users and their devices, and consider how they might be revised or improved to lessen adverse impacts on competition. The standards or best practices resulting from such a process could increase trust across the ecosystem, giving app developers and consumers more confidence that platforms imposing conditions consistent with those standards or best practices are not engaging in anticompetitive action, and reducing the potential for platforms to incur liability for taking legitimate actions to protect their users. Competing app stores seeking access to a platform’s mobile devices could use those same standards or best practices for apps they offer.

We hope these comments will be useful to the NTIA as it develops its report. Please contact me if you have any questions or if we can be of further assistance.

Respectfully submitted,



George P. Slover

Senior Counsel for Competition Policy
Center for Democracy & Technology