Brian C. Rocca, S.B. #221576
brian.rocca@morganlewis.com
Sujal J. Shah, S.B. #215230
sujal.shah@morganlewis.com
Michelle Park Chiu, S.B. #248421
michelle.chiu@morganlewis.com
Minna Lo Naranjo, S.B. #259005
minna.naranjo@morganlewis.com
Rishi P. Satia, S.B. #301958
rishi.satia@morganlewis.com
MORGAN, LEWIS & BOCKIUS LLP
One Market, Spear Street Tower
San Francisco, CA 94105-1596
Telephone: (415) 442-1000

Neal Kumar Katyal, *pro hac vice*
neal.katyal@hoganlovells.com
Jessica L. Ellsworth, *pro hac vice*
jessica.ellsworth@hoganlovells.com
HOGAN LOVELLS US LLP
555 13th St. NW
Washington, D.C. 20001
Telephone: (202) 637-5600

Counsel for Defendants

Glenn D. Pomerantz, S.B. #112503
glenn.pomerantz@mto.com
Kuruvilla Olasa, S.B. #281509
kuruvilla.olasa@mto.com
MUNGER, TOLLES & OLSON LLP
350 South Grand Avenue, Fiftieth Floor
Los Angeles, CA 90071
Telephone: (213) 683-9100

Justin P. Raphael, S.B. #292380
justin.raphael@mto.com
Dane P. Shikman, S.B. #313656
dane.shikman@mto.com
Rebecca L. Sciarrino, S.B. #336729
rebecca.sciarrino@mto.com
MUNGER, TOLLES & OLSON LLP
560 Mission Street, Twenty Seventh Floor
San Francisco, CA 94105
Telephone: (415) 512-4000

Jonathan I. Kravis, *pro hac vice*
jonathan.kravis@mto.com
MUNGER, TOLLES & OLSON LLP
601 Massachusetts Ave. NW, Suite 500E
Washington, D.C. 20001
Telephone: (202) 220-1100

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

IN RE GOOGLE PLAY STORE ANTITRUST LITIGATION

THIS DOCUMENT RELATES TO:

Epic Games Inc. v. Google LLC et al., Case No. 3:20-cv-05671-JD

Case No. 3:21-md-02981-JD

GOOGLE'S PROFFER REGARDING EPIC'S PROPOSED REMEDIES

Judge: Hon. James Donato

PUBLIC REDACTED VERSION

TABLE OF CONTENTS

I. INTRODUCTION

At the Court's direction, ECF No. 978, Google respectfully submits this proffer describing the technical work and estimated costs to: (i) provide third-party app stores with access to Google Play's app catalog; (ii) provide "library porting" of users' Play-installed apps to third-party app stores; and (iii) distribute third-party app stores through the Google Play store. Accompanying this proffer are the declarations of four senior Google employees: (1) Vitor Baccetti (Group Product Manager), (2) Edward Cunningham (Director of Product Management), (3) David Kleidermacher (Vice President of Engineering for Security and Privacy for Android and Made-by-Google Products and Services), and (4) Christian Cramer (Finance Director for Android Ecosystem).

In submitting this proffer, Google does not waive and maintains its objections to Epic's proposed injunction, *see* ECF No. 958. Google's description of how it would attempt to implement catalog access, library porting, and/or Play distribution of third-party stores, if ordered by the Court, does not reflect any agreement by Google that these remedies, as described in Epic's proposed injunction, are reasonable, appropriate under the law, or feasible absent significant expense and fundamental changes to the way Play and Android operate.

As discussed below, these proposed remedies would require a dramatic redesign of the Play store and Android that would harm Android users and developers, the trust and safety of the Play store, and the Android ecosystem and require Google to become a forced dealer for its competitors. Catalog access would fundamentally change Play's relationship with developers, and would require the design and implementation of a new system to provide developers with information about the options available to them under this new program on a regular basis. It would also require the design and implementation of a new method to provide metadata on Google's catalog to third-party app stores, and additional installation and update services for apps discovered in third-party app stores. Library porting, as described in Epic's proposed injunction, would require changing the Android operating system in ways that would compromise the security of Android users. Distribution of third-party app stores would effectively require Google to build a team to screen third-party app stores for malware, pirated apps, and other content that violates

Play store policies on an ongoing basis. This remedy would also require fundamental alterations to the Play store to transform it from an app store that distributes only apps to an app store that also distributes other app stores—a change that would inevitably harm users, developers, and the Play store brand. It would also require changes to fundamental user security protections in the Android operating system.

These remedies would be very costly and would take a substantial amount of technical work and time to implement. Google's best assessment at this point in time is:

- Catalog access would require 12-16 months to implement, and would cost Google between $27.5 million and $66.9 million to build, implement, and maintain for the duration of the injunction.
- Library porting, as described in Epic's proposed injunction, would require a year to implement, and would cost Google between $1.7 million and $2.4 million to build, implement, and maintain.
- Distribution of third-party app stores would take 12-16 months to implement. This remedy would cost Google between $32.1 million and $67.7 million to build, implement, and maintain for the duration of the injunction, with an additional annual ongoing cost for review of apps and updates in third-party app stores. The cost of this ongoing review depends on the number of third-party app stores that request distribution through Play and the size of their catalogs. Assuming the catalogs of those app stores led to a 20 percent increase in the current review work performed by Play, that cost would be approximately [redacted] per year. For an injunction of two to six years in duration, that additional cost would be between [redacted] and [redacted]

These estimates reflect the technical and review costs to Google. They do not include the incalculable costs that Google would suffer from the harms to the Google and Play brands or to the security and viability of the Android ecosystem caused by these proposed remedies.

This proffer reflects Google's current analysis within the timeframe provided and based on the limited description of the proposed remedies set forth in Epic's proposed injunction. Google

reserves the right to modify this description in response to any further submission by Epic describing these proposed remedies in more detail. Should the Court order Google to implement one or more of these remedies, it is possible that, in the course of complying with that order, Google could encounter unanticipated consequences of the Court's order. That may require Google to pursue different methods of implementation (which may involve different timelines), and Google reserves its right to do so.

Finally, in submitting this proffer, Google renews its request for the opportunity to submit further briefing. In addition to implementation and cost issues, the technical details of Epic's novel proposals raise significant legal issues, particularly in light of the fact that Epic asks this Court to impose a worldwide injunction. Google respectfully requests the opportunity to brief those issues before the Court issues any injunction in this matter.

II. CATALOG ACCESS

Epic's proposed injunction would require Google, for a specified period of time, to provide third-party app stores—Google's competitors—with "access [to] the Google Play Store's catalog of apps not then available on those" stores. ECF No. 952, Proposed Injunction § II.D.1. If a user "wishes to download and install an app not then available on that" third-party store, Google would be required to "have the Google Play Store download and install that app on the Third-Party App Store User's device." *Id.* Epic's injunction effectively asks the Court to override the developers' decision on where to distribute their own apps (which are the developers' intellectual property) and force Google to distribute each developer's apps on stores with which the developer has no relationship and without the developer's express consent. The proposal further allows third-party app stores to free ride on Google's substantial investment in building its catalog, by focusing on building relationships with developers of profitable apps while getting free apps from Google.

If Google were ordered to implement this remedy over its objection, Google currently expects that it would do so in four steps: (1) build, launch, and maintain a method for delivery of the metadata associated with the apps in the Play store catalog, as well as a method for installation of apps through the Play store; (2) create a developer consent mechanism to allow developers to decide whether to participate in catalog access and further share its intellectual property, and if so

in which third-party app stores; (3) develop and implement a model for charging third-party app stores for the service of catalog access and value of Play's catalog; and (4) develop and implement eligibility criteria for third-party app stores that wish to participate in catalog access to mitigate harm to users and developers.

A. App Catalog Metadata Export

Epic's proposed injunction does not describe how Google should provide third-party app stores with "access" to the Play store's catalog or what "access" would constitute in this context. Google assumes that such "access" involves some technological ability for a third-party app store to obtain a listing of the apps available in the Play store.

Google proposes to provide such access through the metadata export process discussed in the Declaration of Vitor Baccetti. *See* Baccetti Decl. ¶¶ 7-10. Specifically, Google would export "metadata" (information about an app, such as the app's name, the developer name, image of the app icon, and app category) associated with the generally available apps in its catalog through a server capable of providing that metadata to any authorized third-party app store's serving system.[1] As discussed below, access to this metadata would be subject to terms of service set by Google. Google would regularly export and refresh this metadata. The third-party store would be able to maintain its own local database containing the exported data, as well as a local database of apps published directly in its store. When displaying apps to a user, the third-party store could query both databases and merge the results to create a single user-facing catalog in the third party's storefront. This process would satisfy Epic's proposal that Google provide third-party app stores with "access" to the "Google Play Store's catalog of apps not then available on those" stores, as Google understands this requirement. ECF No. 952, Proposed Injunction § II.D.1.i.

As Mr. Baccetti explains in his declaration, if the user selects an app published directly in the third-party app store, the store would use its own code to download and install the requested app and Google would not be involved. Baccetti Decl. ¶ 11. If the user selects an app that is

[1] The export would not include metadata for apps that are not publicly available, such as apps that are published only for users in a specific domain (e.g., enterprise-specific apps) or apps in closed beta.

published by Play, but not by the third-party app store, then the third-party store could request that the Play store install the app and deliver the download. This request would be made through an Application Programming Interface ("API") that Google would provide. The API would then render a Google-generated user interface that allows the user to download the app without leaving the third-party app store.[2] (If the user is not eligible to install the app—for example because the user is a minor or because the app is not available in the user's country or is not compatible with the user's device—then the Google-generated user interface would inform the user of this fact.) This interface would contain Play branding, so that the user is on notice that they are downloading an app from the Play store (rather than the third-party store) and that they are signed into a Play account and are agreeing to Play's terms and conditions, just as if they were installing an app directly from the Play store itself. In addition, certain jurisdictions have regulatory requirements regarding the information displayed to users at the point of install, and because Play is fulfilling the installation, Google must be able to generate the interface so it can ensure compliance with those regulations. This process addresses Epic's proposal that such installation be accomplished through "a background process similar to the Alley Oop integration offered by Google to certain third-party Developers," as Google understands that term. ECF No. 952, Proposed Injunction § II.D.1.i .

Because the Play store is handling the installation (and subsequent updates) of the app, the user is treated in the same way as a user who installs an app directly from the Play store. Baccetti Decl. ¶ 18. This means, for example, that the user will be required to agree to relevant Play terms of service (if they have not already done so) and will receive Play points for the installation (if enrolled), and the Play store will, as with any Play user, communicate with the user about updates as well as notifications about Play store products and promotions. The user will also be required to sign into the Play store to complete the installation, and if the user has not previously signed

[2] Google will also need to build and implement an additional security layer that ensures that the app store seeking to call the Play API is, in fact, an app store that the developer has authorized to make the app available through catalog access. This mechanism would involve building and maintaining, in real time, a list of approved callers of the Play API described above. Baccetti Decl. ¶ 16.

into the Play store, then the user will be redirected to the Play store to register. These steps are necessary because the Play store has no mechanism to install apps for a user that is not signed into the store.

The metadata provided to the third-party app store will include fundamental identifiers for the apps in Google's catalog, such as the name of the app, the associated package name, and the name of the developer. Baccetti Decl. ¶ 8. The provided metadata will also include some basic information *provided by the developer* to Google about the app, such as the countries in which the app may be distributed and whether the app offers in-app purchases. The purpose of providing this additional data is to allow the third-party app store to reduce the number of instances in which a user clicks on an app in the third-party app store that the user is not eligible to download, for example because the app is not available in the user's country. The metadata provided by Google to the third-party app store would *not contain any user data***.** Requiring Google to share user data with third-party app stores would raise very significant security, privacy, and regulatory concerns. Google does not understand the proposed injunction to suggest that Google would be required to share user data as part of the catalog access remedy. Nor would the metadata provided by Google include any data generated by Google itself, like auto-translations, age ratings, or install counts. *Id.*

Google would provide the catalog data to the third-party app stores using the method described above rather than through a method that directly connects Play's catalog into the third-party app store, because that approach would require far deeper technical integration with Google's competitors than the method described above. *See* Baccetti Decl. ¶¶ 28-30. A direct connection to Play's catalog would require establishing and maintaining server-to-server or client-to-client connections between Google and the third-party app stores, effectively partnering the technical operations of Google with those of its competitors. This level of integration goes far beyond what is necessary to provide access to the Play store catalog. And this approach would increase the complexity, implementation time, and cost for Google and likely also for third-party app stores because it would require integration of the third-party app store's discovery function with Google's systems. This approach would also require Google to build, support, and maintain

servers to handle the traffic of users browsing another app store. Finally, this method of implementation would deprive third-party app stores of the ability to differentiate themselves from competitors by organizing and building their own discovery functions, recommendations, and merchandising capabilities within their storefront. *Id.*

Building and implementing Google's proposal for catalog access as described above would be extremely challenging and costly. *See* Baccetti Decl. ¶¶ 32-35; Cramer Decl. ¶ 12. Google could have to build and implement a system to aggregate and export metadata for approximately 3 million apps, as well as a system to refresh that metadata. Google would also be responsible for communicating with the approximately one million developers who list their apps in the Play store about the details of the catalog access program and the options available to them. Google would also have to tailor the metadata provided to the third-party app stores enrolled in catalog access based on the responses of each developer. Depending on the number of third-party app stores that enroll in catalog access, this could be incredibly burdensome—there are hundreds of third-party app stores on Android today. Cunningham Decl. ¶ 71. Google would have to repeat this process as developers list new apps in the Play store and as new third-party app stores elect to participate in the catalog access program.

Google would also have to devote resources to developing a billing system, onboarding third-party app stores, and creating a policy enforcement team to ensure compliance by third-party app stores with terms of service and developer preferences. Based on the information currently available to Google, and in the limited time available, Google estimates the total cost of building and implementing this remedy to be approximately $13.6 million to $23.7 million. Cramer Decl. ¶ 12. In addition, Google estimates an ongoing maintenance and policy enforcement cost of $7.5 million to $27 million, depending on the duration of the injunction. *Id.* It is Google's practice in its quarterly planning exercises to build in a 20-30 percent buffer to account for unforeseen costs. Applying the same approach here brings the total cost of this remedy to $27.5 million to $65.9 million. *Id*. It would take Google 12-16 months to implement this remedy. Baccetti Decl. ¶ 36.

B. Developer Consent Mechanism

The second aspect of Google's technical implementation of this remedy would be to build a mechanism to obtain developer consent to participate in catalog access generally, and specifically for particular third-party stores. This could be accomplished through a checkbox that developers can select to include an app in the catalog access program generally, as well as individual checkboxes allowing developers to identify the authorized third-party app stores that would have access to the app metadata through the program. Google would send a message to all developers upon implementation, as well as periodic updates as additional third-party app stores enroll in the catalog access program. *Id.* ¶¶ 19-20.

At the May 23 hot tub proceeding, Epic's expert proposed an "opt out" rather than opt in approach for this developer consent. In this context, "opt out" is both practically unwarranted and legally insufficient.

From a practical perspective, catalog access would fundamentally change Google's relationships with app developers. Since the launch of Android Market, the Play store's relationships with developers have been premised on Google's distribution of the developers' apps only in the Play store. This limitation is set forth in the Developer Distribution Agreement ("DDA"), Baccetti Decl., Ex. A, and in the commercial agreements that Google enters with app developers regarding the distribution and the use of their intellectual property. In addition, some developers enter into sublicenses of the intellectual property of third parties (e.g., the property of a movie studio or music producer) for purposes of distributing their apps, and those sublicenses may themselves limit the developer's distribution authority when it comes to app stores. *See* Baccetti Decl. ¶¶ 20-21.

The catalog access remedy would upend this premise for all developers, with enormous implications. Developers would now have to assess the scope of their own intellectual property sublicenses, the reputational and regulatory concerns associated with distribution of their apps in other app stores, and (potentially) the capabilities and nature of every third-party app store that participates in catalog access. If the Court adopts Epic's request for a worldwide injunction, developers would suddenly face a host of regulatory and compliance risks associated with

advertisement and distribution of their apps around the world. And Google would have to explain all this to the developers—what the program is, how it works, the options available to developers, and so on, in many different languages. Under these circumstances, it is not reasonable to assume that developers consent to have their apps distributed in every third-party app store that participates in catalog access unless the developer affirmatively opts out.

Moreover, Google would have no way to enforce a developer's decision to de-list their app from a particular third-party app store. Baccetti Decl. ¶¶ 21-22. Once the initial tranche of metadata associated with the Play catalog has been sent to a third-party app store, Google would have no way to claw that metadata back, and so even if a developer's app is removed from the next tranche, the third-party app store will still have all the metadata from the previous updates. While Google would make it a condition of terms of service for catalog access that third-party app stores abide by developer decisions, Google would have no technical way to prevent the third-party app store from continuing to use the metadata already in its possession. As a result, in certain circumstances, the third-party app store may be able to use that metadata to continue listing the developer's app in the store, notwithstanding the developer's decision to opt out.

As a legal matter, implementing catalog sharing on an opt-out basis would violate developers' intellectual property rights. Developers own substantial IP rights in their apps, including copyrights on the software and trademarks for brand features like logos and other images. The DDA grants Google a nonexclusive license to use developers' IP "in connection with" "the operation and marketing of Google Play." DDA § 5.1 (copyrighted software products); *see also id.* § 6.2 (comparable license for brand features, including trademarks). Google has no ability under the DDA to sublicense developers' content to third-party app stores. On the contrary, Google's only sublicensing authority is a highly limited sublicense permitting Google to allow third-parties to perform certain security functions, *see* DDA § 5.1(e), and developers expressly state that Google possesses no other "right, title, or interest" from developers. DDA §§ 4.4, 6.1.

Implementing catalog sharing would thus exceed the scope of Google's rights to developers' IP under the DDA, as Google would now be using the intellectual property of

developers in connection with the operation of third-party app stores, by providing the third-party app stores with the metadata necessary to list those apps in their stores. This Court lacks authority to compel non-party developers to grant third-party app stores the necessary licenses, or to compel them to grant Google the ability to sublicense their content to third-party stores. The Court's injunctive power extends only to Google and any non-parties working "in active concert or participation" with Google. *See* Fed. R. Civ. P. 65(d). This is a demanding standard, and Epic has not attempted to show that the test is satisfied with respect to non-party developers. *See Comedy Club, Inc. v. Improv West Assocs.*, 553 F.3d 1277, 1287 (9th Cir. 2009) (narrowing injunction improperly imposed on non-parties). Thus, to the extent the Court is inclined to order catalog sharing, it must do so on an opt-in basis, which would ensure that developers have consented and granted third-party stores the necessary licenses to distribute apps.

C. Fee for Catalog Access

The third aspect of Google's technical implementation of the catalog access remedy would be to develop and implement a model for charging third-party app stores for the services provided by Google through catalog access. Epic's proposed injunction does not state (as it does in the provision regarding distribution of third-party app stores) that Google may not charge such a fee.

As discussed above, Google estimates that it would cost approximately $27.5 million to $65.9 million to build and implement catalog access and to provide ongoing maintenance support and policy enforcement for the duration of the injunction. Those costs do not include the billions of dollars in costs that Google has incurred to build the enormous catalog that its competitors would now be permitted to access, nor does it account for the likely strategy of third-party app stores only developing direct relationships with apps that execute in-app transactions for digital services, meaning Google Play will supply all free apps without the potential of earning any revenue in return. These costs weigh strongly against an order compelling Google to implement this remedy at all. But if Google is forced to implement catalog access, then it must be permitted to charge third-party app stores for the significant services and value that Google is providing. An injunction to the contrary would amount to an order that Google perform valuable work for its competitors for free.

D. Eligibility Criteria

Finally, as part of its implementation of catalog access, Google would need to develop eligibility criteria for third-party app stores to mitigate the risk that catalog access would legitimize app stores that distribute malware, violate the intellectual property of developers through pirated or "unlocked" versions of apps (for example, an unauthorized version of a subscription app with the subscription requirement removed so that the user can access the content in the app for free), or otherwise promote illegal activity or objectionable content (e.g., pornography, hate speech). Google would also need to develop and implement an ongoing audit and enforcement system to ensure that third-party app stores enrolled in catalog access continue to meet those criteria. *See* Baccetti Decl. ¶¶ 23-24.

There are hundreds of third-party app stores that vary in terms of quality, sophistication and policies with respect to objectionable or illegal content. *See* Cunningham Decl. ¶¶ 71-75. App stores that traffic in malware or pirated content often have fewer apps in their catalogs because app developers do not want to legitimize these stores or associate their apps and brands with them. Without eligibility criteria, this proposed remedy would require Google to provide such app stores with the ability to appear like legitimate app stores, and would effectively place Google's imprimatur on them by showing the user a full catalog of apps from Play in those stores and funneling users to Play-branded pages.

As the technical implementation discussion above makes clear, such ill-intentioned app stores could then intermingle the apps from Google's catalog with malware or pirated apps from their own catalog, so that users are unable to distinguish legitimate Google-provided content from these app stores' objectionable or illegal content. This would harm Android users, who would be more likely to download malware that is intermingled with Google's catalog. It would also harm app developers both financially and reputationally, as pirated versions of their apps would be downloaded at higher rates when those pirated versions sit next to legitimate Play catalog apps. It would harm Google and the Play store, whose brands would be tarnished by having the Play store catalog mixed with unlawful or objectionable content. And it would harm Android, by increasing the prevalence of malware and pirated content in the ecosystem.

This is not a theoretical problem. Android app stores that traffic in malware or pirated content exist today. For example, HappyMod is an app store dedicated to hosting "modified" apks—that is, pirated, unlocked, or cracked—Android apps. Cunningham Decl. ¶ 72. Allowing these apps to flow through Android app stores using Play's trusted brand and catalog would further harm competition between Android and Apple's iOS.

To partially mitigate these harms, Google would create and implement a set of eligibility criteria for third-party app stores requesting catalog access, and a system to implement and enforce the criteria. *See* Baccetti Decl. ¶¶ 23. At a minimum, those criteria would include that an app store has: (1) a minimum number of apps in its own catalog and the basic infrastructure in place to conduct app store business; (2) bans on malware, pirated apps, and other illegal content; (3) procedures in place to enforce those bans; and (4) reasonably sufficient safeguards to protect the exported metadata.

The eligibility criteria would also include an agreement to terms of service with Google. Terms of service would be necessary to ensure compliance with local laws and regulations, and to address the novel questions arising from the unprecedented forced partnership between Google and its competitors created by catalog access. As noted above, terms of service are critical to mitigate the risk that third-party app stores will not abide by developer requests to remove their apps from catalog access. Such terms of service would also address other possible topics of dispute between Google and third-party app stores around catalog access, such as: unauthorized redistribution of the catalog metadata; responsibility for addressing developer complaints; responsibility for customer service; use of Google's brands and trademarks; and destruction of the catalog metadata when the injunction expires. Google must be able to require qualifying third-party app stores to abide by terms of service that address these and scores of other questions that are likely to arise during and after the period of any imposed injunction. And Google must be able to enforce those terms of service, including by disqualifying violating third-party app stores.

III. LIBRARY PORTING

Epic's proposed injunction requires "Google to provide users with the ability, subject to a one-time user permission, to change the ownership" for any or all apps installed by the Google Play store "such that the Third-Party App Store becomes the update owner for those apps." Proposed Injunction § II.D.1.

The existing capabilities of Android largely address the goal of the library porting remedy. Android 14 already enables third-party app stores to request user permission to update apps installed by other app stores. The additional permissions required by Epic's proposed injunction—to allow for bulk transfer of updating permissions and to allow app stores to change the ownership of all apps, including apps that are not distributed by the third-party app store—are unnecessary and would have serious negative consequences for the security of Android users and would impose significant costs and technical work on Google.

A. Existing Capabilities of Android 14

Epic's proposed remedy is unnecessary because Android's controls over cross-store updates already allow most of what Epic refers to in its proposed injunction as "library porting." Prior to Android 14 (released in October 2023), any preloaded app store on the user's device could update any app on the device without user permission or notification. For example, if the user had three preloaded app stores on the device, all three app stores could attempt to automatically update any app that was installed by the user from any app store. When app stores push updates to apps that the user expects to be updated via a different app store, problems for the user can arise. Such unauthorized cross-store updates, sometimes called "app clobbering," can result in loss of the user's prior in-app purchases or purchased subscriptions, and could cause apps to crash more frequently. Unauthorized cross-store updates can also create problems for developers, for example by frustrating their efforts to roll out new versions of their apps to a fraction of their user base in the first instance in order to ensure that any bugs in the new version are fixed before the new version is released more broadly (a process known as staged release). Cunningham Decl. ¶¶ 5-10.

To address these problems, Android 14 introduced the concept of "update ownership." This concept allows an app store to protect the user by requiring user confirmation before a

different app store can update apps installed from that app store. In other words, any app store can ensure that, by default, an app installed from that app store will receive automatic updates only from that app store unless and until the user decides otherwise. But any app store on the device can request user permission on an app-by-app basis to update an app that was installed by another app store when the new store has a compatible update available. When "update ownership" is cleared from the app, any app store on the device (including but not limited to the app store that requested the permission) can then update the app. *Id.* ¶¶ 11-14.

These existing features of Android largely achieve the goal of library porting as described by Epic's expert. In his statement, Dr. Bernheim explains that the purpose of library porting is to "allow[] users to transfer the responsibility of updating apps that were originally downloaded from the Google Play Store to the third-party app store such that the third-party app store would be responsible for automatic updates of apps (and would from that point forward be entitled to any ongoing revenues from the developer)," resulting in "competition between Google Play and its rivals" that "will directly benefit users." ECF No. 952-1, Bernheim ¶ 64. Android allows third-party app stores to update apps in this way by requesting permission from the user to "clear ownership" on an app-by-app basis. Cunningham Decl. ¶¶ 11-14. This app-by-app permission requirement is not particularly burdensome on the app store because there is no limit to the number of update requests that an app store can send the user. And if the developer has provided the third-party app store with a version of the app that incorporates the third-party store's billing system (or has otherwise complied with that app store's policies on billing), then the third-party app store could start collecting service fees on in-app purchases (assuming it collects a fee for equivalent digital goods and services) once it has updated the app on the user's phone with that version.[3]

[3] As discussed in Mr. Cunningham's declaration, developers must take certain actions with respect to their apps to allow for the possibility of third party app stores updating their apps, thereby receiving "ongoing revenues" as Dr. Bernheim describes. In particular, the developer would have to provide the third party app store with updated versions of the developer's apps incorporating the third party app store's billing system. The developer would also have to ensure that the Android operating system recognizes the third party app store's version of the app as the same app that the user acquired from a different app store. As Mr. Cunningham's declaration explains, the

B. Changes Required to Implement Remedy

Epic's library porting proposal would require the addition of two capabilities that do not currently exist in Android 14. The first is a bulk update request (described by Epic as a "one-time User permission" to change ownership for all apps on the phone).[4] The second is a "change ownership" permission rather than a "clear ownership" permission. These changes would significantly harm Android users and impose substantial technical work and costs on Google.

1. Bulk Update Request

The Android operating system requires app stores to request permission to clear ownership on an app-by-app basis when the third-party app store has a compatible update available, rather than (as Epic has proposed) through a bulk request. To implement the "one time User permission" requirement of Epic's proposal, which would require *bulk* ownership change of apps on the user's device, Google would have to modify the Android operating system. Specifically, Google could introduce a new Android API to request a bulk ownership change, with a corresponding "behind-the-scenes" permission that app stores would declare in their app manifest and that governs the use of this API. When this API is invoked along with a list of app package names, the API would display a user interface that the app store could use to seek user consent to perform updates to one or more apps without the per-app update ownership dialog prompt. The actual change in update ownership for each app would be deferred until the app store successfully installs an update for each app. Cunningham Decl. ¶ 19.

This change to Android 14 would harm users. The app-by-app approach to cross-store updates was designed to give users a straightforward decision they can make quickly and easily one app at a time. This approach makes sense because users may have good reasons to prefer to have different apps updated by different app stores. For example, App Store A may offer

---

developer could accomplish this in several ways, including through the use of a single signing key for the app across app stores. Cunningham Decl. ¶¶ 33-39.

[4] Google understands the term "one-time User permission" to mean that an app store can issue a single update ownership request for a group of apps already installed on the phone, and not that an app store can issue a single request for permission to automatically update all apps acquired from any source in the future. The latter interpretation would lead to a host of additional problems discussed in Mr. Cunningham's declaration. Cunningham Decl. ¶ 22.

exclusive content for one app on a user's device, while App Store B may offer promotional discounts for a different app on a user's device. This is consistent with the way users already make decisions about installation of apps on their device–one app at a time. By contrast, requiring the user to make a single decision about all the apps on their device at one time is likely to confuse the user. Indeed, a user presented with a "one-time User permission" to update all apps on the device from a single app store may not realize that the consequences of agreeing to that request will be to lose protection against having *any* app store update *any* app on the device. *Id.* ¶ 18.

To mitigate these harms, if Google were ordered to implement this change to the Android operating system, Google would also modify the operating system to permit the developer to choose whether to allow its apps to be subject to the new bulk ownership change protocol. Google would do this by giving developers the ability to indicate in the code of their APKs whether the app can be transferred in bulk along with other apps, or if instead the per-app permission would continue to apply to that app. Google would also give the developer the opportunity to indicate in the code of the APK which third-party app stores are permitted to obtain ownership over the app by means of the bulk transfer. *Id.* ¶ 20.

2. Change Ownership

The second change to the Android operating system that would be required by Epic's proposed injunction is to add a "change ownership" capability. As described above, the Android operating system does not allow a user to "change the ownership" of an app from one store to another. Instead, Android enables a user only to "clear ownership" of an app so that the app can be updated by *any* app store, not just the app store that requested the update permission, without any further authorization by the user.

If Google were ordered to implement Epic's "change ownership" proposal, Google would create a capability in the Android operating system to perform the update owner switch. Google would also create a new "update ownership" dialog, design, and language to accommodate this change in behavior. *Id.* ¶ 30.

Here again, Epic's proposed change would harm Android users. *See id.* ¶¶ 24-27. The proposed "change ownership" permission (unlike "clear ownership") would allow only the app

store that requested the permission to update the app. The problem is that an app store could ask a user to "change ownership" of an app that the app store does not actually distribute. (The Android operating system has no way to tell whether an app store actually distributes any particular app, and so the operating system has no way to limit the "change ownership" permission to an app store that actually distributes the app.) In that circumstance, the user would stop receiving updates for the app. This would lead to several harms. First, the app developer (who has no association with the third-party store) would be unable to push updates out to its users, significantly harming the developer's business. Second, users would stop receiving security updates. Many apps, including banking apps, push updates to users on a regular basis to patch security holes. Mr. Cunningham describes a recent example in his declaration. *Id.* ¶ 26.

If users were unable to obtain these kinds of security updates—because an app store that does not actually distribute the app has convinced the user to "change ownership" of the app—the results could be disastrous for the user. These risks would not be apparent to a user who is simply shown a dialog box asking for permission to "change ownership." Android 14 addresses these risks by allowing an app store to request user permission to "clear ownership" on an app-by-app basis, but not "change ownership" for a user's entire set of apps. As discussed above, the "clear ownership" permission does not prevent another app store from updating the app, thereby preventing the scenario described above. *Id.* ¶ 27.

The risks to users associated with Epic's proposed "change ownership" permission are even greater when considered alongside Epic's proposed "bulk update" permission. If Google were required to implement both of these changes to Android 14, then an app store could send a one-time user permission to "change ownership" of every app on a user's device, including apps that the third-party app store cannot update. At that point, every app on a user's phone will be incapable of updating, potentially including apps that are integral to the functioning of the phone. *Id.* ¶ 28.

Here again, if Google were ordered to modify the Android operating system to implement Epic's "change ownership" proposal, then Google would also have to build some protections into the operating system to mitigate these harms. Google would do so through a developer choice

protocol similar to the "one time User permission" mitigation discussed above. A developer could embed a statement inside the APK file indicating whether ownership of the APK can be transferred, and if so which particular app stores are authorized to change ownership of the app. OEMs and carriers could configure the same permission for apps they preload. *Id.* ¶ 30. This approach is consistent with the provision in Epic's proposed injunction that the new store would become the "update owner" of bulk-transferred apps only "if and when those apps become available on the Third Party Store." These protections would potentially mitigate, but not eliminate, the harms to the user that may arise from an app store taking advantage of the single permission to take control of apps.

C. Costs of Library Porting

These changes to the Android operating system would be very costly. Changes to the Android operating system are enormously consequential. The operating system is the underlying software that powers billions of Android phones. An error or bug in the operating system can have disastrous consequences for users, developers, OEMs and Google. Accordingly, changes to the Android operating system that involve behavior changes to APIs and that impact external developers, like those that would be required to implement Epic's proposed remedy, require extensive developer previews, beta testing, feedback from users and OEMs, and final bug fixes prior to a public release.[5] Because these tasks must be scheduled well in advance and take several months to complete, Google sets a regular cycle for Android updates. *Id.* ¶ 47.

Making the changes to the Android operating system proposed by Epic earlier than that would not be feasible. New features implemented into the operating system take time to build in a way that avoids unintentional regressions in device functionality, including unforeseen interference with the operation of users' apps. It takes time to test out the changes and establish the possible app compatibility impact, and it takes time for impacted app developers to make necessary adjustments to their apps as well. Google's testing of changes to the Android operating

[5] More minor changes to the Android operating system–like enhancing screen sharing functionality or adding an option from the "quick settings" panel to share Wi-Fi credentials–occur on a more frequent cadence.

system includes public developer preview and beta programs to ensure that the changes operate as intended. Google solicits feedback from developers and users participating in these programs to identify bugs and other issues. These programs take several months, and there is no way to fast track them because this kind of testing requires users to operate their devices in the ordinary course over a period of time. *Id.* ¶ 49-51.

Another important aspect of the operating system testing process involves OEMs, since it is the OEMs that ultimately decide whether to adopt Android changes in their updates or new releases. OEMs engage in significant engineering work to assess and integrate changes, typically also implementing their own testing programs. In many countries, there is yet another level of testing conducted by mobile carriers. The timing of OEM and carrier testing of new versions of the operating system is not within Google's control. *Id.* ¶ 49-52.

The technical costs to implement and maintain these changes to Android would be approximately $1.7 million to $2.4 million. Cramer Decl. ¶ 13. If Google were ordered to implement these changes off-cycle, the cost to Google would be far higher, as Google would have to initiate a separate round of user, developer, and OEM testing and feedback described above. Cunningham Decl. ¶ 53.

IV. DISTRIBUTION OF THIRD-PARTY APP STORES

Epic's proposed injunction would require Google, for a specified period of time, to "allow distribution of competing Third-Party App Stores on the Google Play Store." ECF No. 952, Proposed Injunction § II.D.2. Under the proposed injunction, Google would not be permitted to charge third-party app stores for this service. *Id.* § II.D.2.ii. The details of technical implementation of distribution of third-party app stores discussed below show several of the problems associated with this proposed remedy.

Google's implementation of this proposed remedy would involve four steps: (1) redesign the Play store to accommodate the distribution of app stores; (2) implement a thorough ongoing vetting process for the policies, conduct and catalogs of app stores that request to be distributed through the Play store; (3) change the Android operating system; and (4) build and implement a charging model for third-party app store distribution.

A. Redesign of the Play Store

The Play store as it exists today is designed to distribute apps, not app stores. This change would require a fundamental redesign of the Play store. As explained in the declaration of Mr. Baccetti, that redesign would include the following steps. Google would have to reconfigure the Google Play Console to allow developers to declare an app as an app store, agree to abide by Play store policies, and accept additional terms of service. Google would also have to create ways for the Play store to handle the display of app stores within the store and design a method to track and identify for users which apps in the store are "app stores." And Google would have to build and implement a warning that advises users when they are about to download an app store. *See* Baccetti Decl. ¶¶ 38-41.

B. Vetting Process

Google would implement a thorough vetting process for app stores requesting distribution through the Play store. This vetting process would likely include three components: (a) initial and ongoing review of all apps and updates in the app store's catalog for compliance with Play's security and content policies; (b) initial and ongoing review that the app store meets criteria set by Google to qualify as an "app store"; and (c) initial and ongoing review that the app store complies with behavior policies set by Google.

1. Review of App Store Catalogs

As Dave Kleidermacher testified at trial, and as summarized in his declaration, the Play store performs a human review of all new apps to determine compliance with Play's security and content moderation policies. Kleidermarcher Decl. ¶ 8. The Play store also employs a sophisticated infrastructure that conducts a machine-based review, scrutinizing the application and the developer for signals of risk that would trigger further human review. Google also reviews all app updates using a machine-based review. An app or update is not published until the Play store completes these reviews. Millions of apps and updates are submitted to the Play store annually, and Google conducts the review described above for all those submissions. This app review process is an integral component of the Play store business model and the Google brand. *Id.*

If Google were ordered to distribute third-party app stores through the Play store, then Google would subject the catalogs of those third-party app stores to the same rigorous review, because the content of those stores would now be accessible through the Play store. This would include a thorough review of the third-party app store's catalog at the time the store first requests distribution through Play. Once the third-party app store is listed on Play, Google would conduct the same review for every update to every version of every app in the third-party app store, as well as every app that the third-party app store proposes to add to its catalog, before the app can appear in the third-party store. No app or update could be published in a third-party store distributed through the Play store until Google has cleared that app or update for compliance with Google's safety and content policies. *Id.* ¶ 9. Google would be required to devote substantial resources to enforcing the outcomes of this rigorous review, both by instructing third-party app stores to remove non-compliant apps and updates and by potentially removing app stores that did not comply with Google's review process from Play.

The risk to the Play store and Google brands posed by the distribution of third-party app stores is not a purely theoretical concern. As noted above, there are hundreds of Android app stores today, some of which list and even promote content that violates the Play store's policies. Mr. Cunningham notes in his declaration, for example, the Nutaku Android store advertises itself as "the world's largest 18+ gaming platform," and features apps with adult content. Cunningham Decl. ¶ 74. Similarly, Aptoide (another Android app store) hosts adult apps including Pornhub and an unrestricted version of Telegram that allows adult content, as well as pirated apps. *Id*. HappyMod is an example of an Android app store dedicated to distributing pirated or "unlocked" versions of Android apps and games. *Id.* ¶ 72. And CepKutusu.com was an example of an app store that intentionally distributed malware, incorporating banking malware into every app downloaded from the store. *Id.* ¶ 73. If users were able to access this type of content through the Play store by downloading these app stores from Play, the reputation for safety, security, and content moderation that the Play store has spent over a decade and billions of dollars building would be irreparably damaged.

At the May 23 hot tub proceeding, the Court suggested that Google could show a screen to a user who is about to download a third-party app store from the Play store disclaiming any responsibility for the consequences. While Google certainly would want the ability to implement such a warning, that alone is far from sufficient to protect users, for the same reason that it is not enough simply to show such a screen when a Play user downloads an app. Kleidermacher Decl. ¶ 23. The brand and reputation of the Play store are built on providing users with a safe, secure, reliable experience, not on disclaimers. That experience includes browsing the Play store, downloading the app, and safely using the app after it is downloaded. A "buyer beware" disclaimer does not repair the harm to the Play store's brand when a child is able to view adult content through an app store acquired from Play, or when a user's device is infected with malware from an app store acquired from Play as a result of this proposed remedy. In those scenarios, the Play store is the platform that connects the user with the app stores that inflict those harms. It is unrealistic to expect that the user will not blame the Play store at least partially for those harms, just as it is unrealistic to expect that a user will not blame the Play store at least partially for harms inflicted by an app downloaded directly from the Play store. If users are exposed to unsafe content through Play on Android, users will naturally consider other options they perceive to be more secure, such as Apple's iOS.

2. App Store Criteria

Google's vetting process would also include a definition of what constitutes an "app store" for these purposes. In connection with this protection, Google would set criteria as to which apps are eligible to be distributed as app stores through the Play store. Such criteria are necessary to mitigate the risk that any number of apps on Play would immediately build in the capability to start installing other apps on the devices of users with a single one-tap screen. The evidence at trial showed that Epic distributes its game Fortnite on Android using the Epic Games Launcher, a separate app that has the capability to install Fortnite on a device. This proposed remedy would allow a developer like Epic to avoid Google's service fee simply by distributing the launcher on the Play store as a "third-party app store." To avoid this scenario, if this remedy is implemented over Google's objection, then Google must be allowed to set eligibility criteria for

app stores distributed through the Play store, including prohibiting "launchers" like the Epic Games Launcher, so that developers cannot evade any obligation to pay for the value of the Play store simply by calling their app an app store. *See* Baccetti Decl. ¶¶ 40-41.

3. Behavior of App Stores

Google's vetting of third-party app stores would also include compliance with terms of service setting guidelines for the behavior of app stores distributed through the Play store. For example, one of Google's criteria for app store distribution would be that the third-party store does not automatically install apps on a device that the user has not expressed an intention to install. One recent example of this was the Redstone installer, a pre-installed system app on Android mobile devices sold in Germany that automatically installed malware on the device. Kleidermacher Decl. ¶ 13.

C. Change to Android Operating System

This remedy as described in Epic's proposed injunction would also require a change to the configuration of installer permissions in the Android operating system. Currently, Android has two installer permissions: INSTALL_PACKAGES and REQUEST_INSTALL_PACKAGES. INSTALL_PACKAGES is granted by the OEM when it configures the device. For example, on a Samsung Galaxy Phone, the Samsung Galaxy Store and the Play store are preinstalled with INSTALL_PACKAGES when the device is shipped. INSTALL_PACKAGES allows the app store to install other apps on the device without requesting user permission for each install. Cunningham Decl. ¶ 57.

REQUEST_INSTALL_PACKAGES does not require OEM permission–any app can configure itself to request this permission from the user. For security reasons, each time a user attempts to install an app through another app that has the REQUEST_INSTALL_PACKAGES permission, the user is shown a consent screen. The purpose of this distinction between the two installer permissions is to protect the user from a malicious app installing other apps (including malware) in the background without the user's knowledge or consent. App stores downloaded from the Play store would have the REQUEST_INSTALL_PACKAGES permission (because they were not configured on the device by the OEM), and therefore each time a user installs an app

through an app store acquired from the Play store, the user would see a consent screen. *Id.* ¶ 58. This would appear to violate Section II.D.2.i of the proposed injunction, although the language of this provision is not entirely clear.

To implement this change, Google would remove the need for user confirmation for installation of apps, and add a new behind-the-scenes permission that app stores would add to their manifest. To partially mitigate security vulnerabilities arising from this change, Google would likely add a technical restriction that the new permission must be granted by the installer of the app store itself. For app stores distributed through the Play store, this would mean that Play would grant the third-party app store the permission exempting that app store from the per-app confirmation dialog.[6] *Id.* ¶¶ 61-63.

D. Charging Model

Finally, if Google were forced to implement this remedy, Google would build a model for charging third-party app stores for distribution on Play.

The provision in Epic's proposed injunction stating that Google cannot charge for app store distribution is entirely unwarranted. This proposed remedy would require Google to provide valuable services to competitors on an ongoing basis for free. The evidence at trial showed that the Play store's business model is to provide benefits to app developers and to receive compensation for those benefits through a service fee on in-app purchases within apps downloaded from the Play store. The evidence showed that this is a very common business model among app stores on various platforms, including the Epic Games Store on PCs. An injunction stating that Google cannot charge third-party app stores for distribution through Play would mean that Google would be required to provide these valuable services to its competitors—using Google's proprietary systems and intellectual property—for no compensation whatsoever. This outcome is particularly drastic when considered in tandem with the other proposed remedies discussed in this proffer, which would force Google to provide valuable services to competitor app

[6] In addition, to lessen the risk of silent background installation of harmful and unwanted apps, Google may also require that installing a new app (without a confirmation dialog) be permitted only in response to a proactive install decision by the user, for example by tapping an "install" button that the store renders for the user. Cunningham Decl. ¶ 64.

stores while giving those app stores a mechanism to deprive Google of the service fees that reflect its compensation for those services. Considered together, these remedies amount to an unprecedented forced subsidy to Google's competitors.

E. Total Cost

As explained in Mr. Cramer's declaration, Google estimates that the cost to reconfigure the Play store to distribute other app stores would be $15.1 million to $18.5 million. In addition, the cost of ongoing maintenance, policy, and policy enforcement support would be $9.1 million to $32.2 million, depending on the duration of the injunction. Building in a buffer of 30 percent of the cost, which is Google's standard practice in quarterly planning exercises, yields an aggregate total cost of $31.4 million to $66.7 million. *See* Cramer Decl. ¶ 14. The additional changes to Android to accommodate this remedy would also be between $628 thousand and $751 thousand to build and implement, and then between $79 thousand and $282 thousand to supervise and maintain depending on the injunction's duration.

On top of that, the cost to vet other app stores for distribution on Play would depend on the number of apps in the app stores that were not already in the Play store. Without knowing details about the catalogs of the app stores that would apply for distribution through the Play store, it is impossible to estimate the cost of this vetting. The most Google can say is that the cost of that vetting would depend on the degree to which the vetting of the catalogs of third-party app stores increases Google's current app review process. Mr. Kleidermacher estimates that Play's app and update review process, at its current level, costs approximately [redacted] annually. Kleidermacher Decl. ¶ 14. If the vetting associated with distribution of third-party app stores resulted in a 20 percent increase in Play's app and update review workload (and Mr. Kleidermacher believes that is a reasonably likely possibility), then the cost to Google would be [redacted] annually. For an injunction lasting two to six years, that would cost Google between [redacted] and [redacted].

DATED: June 24, 2024

Respectfully submitted,

By: */s/ Glenn D. Pomerantz*
Glenn D. Pomerantz

MUNGER TOLLES & OLSON LLP
Glenn D. Pomerantz
Kuruvilla Olasa
Jonathan I. Kravis
Justin P. Raphael
Nick R. Sidney
Dane Shikman
Rebecca L. Sciarrino
Jamie B. Luguri
Lauren N. Beck

MORGAN, LEWIS & BOCKIUS LLP
Brian C. Rocca
Sujal J. Shah
Michelle Park Chiu
Minna Lo Naranjo
Rishi P. Satia

HOGAN LOVELLS US LLP
Neal Kumar Katyal
Jessica L. Ellsworth

Counsel for Defendants

E-FILING ATTESTATION

I, Glenn D. Pomerantz, am the ECF User whose ID and password are being used to file this document. In compliance with Civil Local Rule 5-1(i)(3), I hereby attest that counsel for Defendants have concurred in this filing.

s/ Glenn D. Pomerantz
Glenn D. Pomerantz