Aaron R. Marienthal
McGuireWoods LLP
Two Embarcadero Center
San Francisco, CA 94111-3821
(415) 490-0919
amarienthal@mcguirewoods.com

Counsel for Amicus Curiae
(Additional counsel on signature page)

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN RE GOOGLE PLAY STORE ANTI-TRUST 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

BRIEF OF *AMICUS CURIAE* ASSOCIATION FOR COMPETITIVE TECHNOLOGY REGARDING JOINT MOTION TO MODIFY PERMANENT INJUNCTION

Judge: Hon. James Donato

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

INTEREST OF *AMICUS CURIAE*[1]

Founded in 1998, the Association for Competitive Technology ("ACT") is a not-for-profit advocacy and education organization representing the small business developer, innovator, and entrepreneur community that creates countless software applications used on mobile devices and in enterprise systems as well as connected internet of things devices for innumerable consumer and enterprise use cases. In the United States, the ecosystem represented by ACT is valued at approximately $1.8 trillion and is responsible for more than 6.1 million jobs.[2]

As ACT has consistently explained—in comments to the Federal Trade Commission,[3] testimony before Congress,[4] and *amicus* briefs—curated online marketplaces like the Google Play store (Play store) have created immense value for app developers and end users. Developers create mobile software tools, platforms, and services that draw consumers to the online marketplaces. Meanwhile, the marketplaces provide developers with low overhead costs, simplified market entry, consumer trust, dispute resolution, data analytics, flexible marketing and pricing models, and strengthened intellectual property protections. These services, in turn, free up capital that developers use to improve their apps and expand their offerings.

---

[1] No party's counsel has authored this brief in whole or in part, nor has any party or party's counsel contributed money intended to fund the preparation or submission of this brief. Both Google and Epic take no position on this filing.

[2] State of the App Economy, ACT | The App Association 2-3 (2023), https://tinyurl.com/5cz9zbyt.

[3] Comments of ACT | The App Association to the Federal Trade Commission on Competition and Consumer Protection in the 21st Century 3-4 (Aug. 20, 2018), https://tinyurl.com/34fs33p4.

[4] *Online Platforms and Market Power Part 2: Hearing Before the H. Judiciary Comm. on Antitrust, Com. & Admin. L.*, 116th Cong. 3-6 (2019) (statement of Morgan Reed, President, ACT | The App Association) ("ACT Congressional Testimony"), https://tinyurl.com/2srjua3p.

Because of its members' reliance on curated online marketplaces, ACT has a deep interest in ensuring antitrust laws are properly and uniformly applied to those marketplaces to promote competition and increase output. This interest is longstanding. One of the first *amicus* briefs that ACT ever filed was in *United States v. Microsoft Corp.*, where the Department of Justice sought to break up Microsoft and the court discussed Microsoft's "platform[] for software applications." 253 F.3d 34, 53 (D.C. Cir. 2001) (en banc). More recently, ACT closely followed Epic's litigation against Apple that parallels this case and filed an *amicus* brief before the U.S. Court of Appeals for the Ninth Circuit that explained the ways in which Apple's App Store is important to developers and end users. And ACT filed numerous *amicus* briefs during the appeal in this case.

ACT largely supports the parties' joint motion to modify the permanent injunction, which provides needed certainty for ACT's members. *See* MDL Dkt. 1179 ("Joint Mot."). But it writes here to express its concern with including Catalog Access as part of any final remedy accepted or imposed by this Court. Because that remedy threatens developers' intellectual property, associational, and contract rights, this Court should reject it.

SUMMARY OF ARGUMENT

The Revised Proposed Modified Injunction ("RPMI") is a strong step in the right direction. After years of uncertainty, it represents a lasting solution for Google and Epic. Additionally, because aspects of this settlement would affect developers who are not parties to this case, including our members, ACT is pleased that on the whole it represents a positive outcome. For that reason, ACT largely supports the parties' joint motion to modify the permanent injunction. *See* Joint Mot.

But ACT finds it deeply concerning that Catalog Access remains under consideration as a part of any final remedy. Catalog Access requires Google to share

developers' apps with third parties, only stopping it from doing so if the developers take yet-to-be-determined affirmative steps to "opt out" of that default rule. This remedy is an invasive and egregious violation of ACT's members' rights. To protect developers, ACT respectfully requests that this Court should ensure that any final remedy does not include Catalog Access—as the parties suggested in their first proposal to modify the injunction. *See* MDL Dkt. 1119.

ARGUMENT

I. The RPMI Would Bring Much Needed Certainty to App Developers.

Overall, ACT urges the Court to accept the proposed modified injunction and bring finality to this case. ACT supports the modifications that the parties have proposed, with one critical change discussed below. The years of litigation leading up to this point have often left developers unsure of their relationship with the Google Play store and of what the U.S. landscape will look like in the next year, much less in the next five. The RPMI would alleviate some of these concerns. Its six-year timeframe and creation of a single worldwide solution provide much-needed certainty that will make it easier for small and mid-sized app developers to plan next steps and will free up time for them to focus on their true passion: creating innovative apps. For these reasons, ACT largely supports the RPMI and strongly supports the finality it would bring.

II. Catalog Access Invades Developers' Rights and Autonomy.

As the parties note, "the RPMI maintains, unchanged, the Catalog Access remedy from the Existing Injunction." Joint Mot. 5. This is a departure from the parties' first proposed modification, which "remov[ed] … the Catalog Access remedy." *Id.* at 3. As we understand the first proposal, the parties proposed the change in part due to this Court's observation that "there are potential security and technical risks involved in making third-party apps available." MDL Dkt. 1119, at 11 (quoting *In re*

Google Play Store Antitrust Litig., No. 21-md-2981, 2024 WL 4438249, at *7 (N.D. Cal. Oct. 7, 2024)). As we understand the current proposal, the parties have now proposed to keep the Catalog Access remedy due to the Court's concern that it is needed "to overcome the network effects and the entrenched problems of Google's dominance." Joint Mot. 5 (quoting Jan. 22, 2026, Hearing Tr. 13:6-9). While security concerns are significant, that this proposal would violate the intellectual property, associational, and contract rights of roughly half a million active developers on the Google Play store is of even greater concern. We urge the Court to remove it from the permanent injunction.

App developers contract with Google to distribute their apps through the Play store. When they do so, they grant *Google* a nonexclusive license to use their intellectual property. *See, e.g.*, MDL Dkt. 981-2, at 8 (granting Google license to "display Developer Brand Features … for use solely within Google Play"). But this license *does not* either provide parallel grants to other online marketplaces or grant Google the right to sublicense the developers' intellectual property out to others. *See id.* at 6-8. Google thus does not have the right to do what Catalog Access demands—share developers' intellectual property without their express consent. By instructing Google to make developers' apps available on other stores, the RPMI disregards the developers' intellectual property rights.

Even though the Registered App Store will require third-party stores to "meet[] certain safety and security criteria," it also "*requires* Google to approve *any* store" that meets those criteria. Joint Mot. 7 (first emphasis added). But so long as a third-party store meets these limited criteria, Google will have no responsibility to ensure that bad actors on the platform do not steal sensitive information or engage in other mischief. This is no hollow concern. In the past, entire third-party stores have been created by hackers to steal sensitive information. *See, e.g.*, MDL Dkt. 981-3, ¶ 73

(discussing multiple examples of third-party stores that served as "vector[s] for malware," including a "state-sponsored hacking group" that built a seemingly legitimate app store "with the sole purpose of delivering spyware to targeted individuals").

This creates real burdens and harms for app developers and their customers. To continuously monitor for threats requires significant expense and effort, which smaller upstart app stores may not be able to adequately resource.[5] If smaller app stores cannot police these threats, the burden will shift onto the app developers and users. A user whose security is compromised will face the expensive and unsettling experience of trying to re-secure their digital identity. And the user may blame the developer, rather than the store, when their data is accessed.

These risks are only exacerbated by "requir[ing] Google to approve *any* store" meeting certain criteria and thus removing authority Google would otherwise have had over the third-party stores with access to the developers' apps. Joint Mot. 7. Unlike either the current injunction or the prior proposed modification, the RPMI does not even "allow[] Google to review in advance the apps a third-party store intends to carry," *id.* at 8—removing important protections that were already in place.

Catalog Access also invades app developers' rights to freedom of association and freedom of contract. "[F]reedom of association plainly presupposes a freedom not to associate." *Boy Scouts of Am. v. Dale*, 530 U.S. 640, 648 (2000) (citation modified). Likewise, ordinarily "parties are free to contract as they wish" with whomever they

[5] *See, e.g.*, ACT Congressional Testimony, at 9 ("[T]he game of cat-and-mouse between cybersecurity professionals and hackers will never end, and security must continue to evolve to meet and beat the threats. … [D]evelopers want the platform's security features to work seamlessly with any relevant hardware and [to] account for all attack vectors. Platforms should continue to improve their threat sharing and gathering capabilities to ensure they protect developers across the platform, regardless of where threats originate. Moreover, they should approve and deploy software updates with important security updates rapidly to protect consumers as well as developers and their clients and users.").

wish (or not). *United States v. Eurodif S. A.*, 555 U.S. 305, 317 (2009). But Catalog Access would—as a default—enter developers into relationships with third-party stores without their express consent. It would also create the risk that developers' apps could be made available on third-party stores with values diametrically opposed or odious to those of the developers, exposing them to reputational risk. An app appearing on a third-party store themed around, aligned with, or even contributing a percentage of sales to a controversial political movement, for example, would likely lead users to assume the app developer approved of the association. To avoid these harms, developers must retain the right to choose where, through whom, and on what terms they offer their apps in the first instance.

As the RPMI observes, "Google will provide developers with a mechanism for opting out of inclusion in catalog access for any particular third-party Android app store." Joint Mot., Ex. D, ¶ 11. But this gets things backwards. The RPMI effectively requires developers to license their apps to *all* third-party stores approved by Google unless the developers take affirmative steps to prevent it. *See id.* Any reputational damage could not be undone by exercising an opportunity to opt out after the fact. And practically, many small developers that ACT represents may not have the resources to monitor every new store and then take the needed steps to opt out. In short, no opt out can meet the legal or practical requirements of small developers.

No third-party store should have access to developers' apps *without* the developers' say-so. App developers—not Google—should be the ones to choose which stores they do (and do not) offer their apps through. Catalog Access does not adequately respect those app developers' rights and autonomy. Moreover, as the parties in this case are an app store and a third-party store, with no representation for small app developers, instituting a remedy with such significant effect on the rights of those small app developers is inconsistent with due process principles. Because Catalog

Access infringes app developers' intellectual property, associational, and contract rights, it should be rejected.

CONCLUSION

For the reasons above, this Court should modify the RPMI to remove Catalog Access as a remedy but otherwise grant the parties' joint motion to modify the permanent injunction.

Dated: April 6, 2026

Respectfully submitted,

/s/ Aaron R. Marienthal

Aaron R. Marienthal
McGuireWoods LLP
Two Embarcadero Center
San Francisco, CA 94111-3821
(415) 490-0919
amarienthal@mcguirewoods.com

Jonathan Y. Ellis (*pro hac vice* forthcoming)
McGuireWoods LLP
501 Fayetteville St.
Suite 500
Raleigh, NC 27601
(919) 755-6688
jellis@mcguirewoods.com

Nathan Pinnell (*pro hac vice* forthcoming)
McGuireWoods LLP
888 16th Street NW
Suite 500
Washington, DC 20006
(202) 857-2441
npinnell@mcguirewoods.com

Counsel for Amicus Curiae