

March 7, 2022

The Honorable Nydia Velazquez
Chairwoman
House Small Business Committee
Washington, District of Columbia 20515

The Honorable Blaine Luetkemeyer
Ranking Member
House Small Business Committee
Washington, District of Columbia 20515

Re: Competition and the Small Business Landscape: Fair Competition and a Level Playing Field

Dear Chairwoman Velazquez and Ranking Member Luetkemeyer,

As committees across Capitol Hill debate options to address competition in markets with large platform companies, we especially appreciate that the House Small Committee on Small Business (the Committee) continues to shine a light on the perspectives of small, innovative companies. ACT | The App Association (the App Association) is the leading trade group representing small mobile software and connected device companies in the app economy, a \$1.7 trillion ecosystem led by U.S. companies and employing more than 300,000 in New York and 88,000 in Missouri alone.¹ Our member companies create the software that brings your smart devices to life. They also make the connected devices that are revolutionizing healthcare, agriculture, public safety, and virtually all industry verticals. They propel the data-driven evolution of these industries and compete with each other and larger firms in a variety of ways, including on privacy and security protections.

Two antitrust-related proposals in particular have gained traction in both the House and Senate: the American Choice and Innovation Online Act (H.R. 3816)—and its substantive companion measure the American Innovation and Choice Online Act (S. 2992)—and the Open App Markets Act (H.R. 5017 / S. 2710). These proposals are not identical but would have similar effects in the software platform (app store / mobile operating system) context. For example, both bills would diminish and close off distribution options for App Association members. Driven by complaints from the largest competitors on software platforms, H.R. 3816 and H.R. 5017 would reform software distribution to better suit the needs of big business while raising barriers to entry and overhead costs for small app makers.² To smaller companies that opt to reach customers and consumers through software platforms, H.R. 3816 and H.R. 5017 are rooted in a conception of platform markets as being divided between the interests of small companies and consumers on one hand, and the interests of large platforms on the other. But that premise, among others that undergird the bills, as well as their proposed remedies, do not reflect reality for App Association members. In fact, App Association members demand and pay for services H.R. 3816 and H.R. 5017 would prohibit.

Small app companies are constantly pushing platforms to do better, but they do not take the services they buy for granted. As Mark Liber of Brooklyn-based Kaia Health said in one of our Developed | The App Economy tour events in New York, “with platforms, we can bring chronic

¹ ACT | THE APP ASSOCIATION, STATE OF THE U.S. APP ECONOMY: 2020 (7th Ed.), *available at* <https://actonline.org/wp-content/uploads/2020-App-economy-Report.pdf>.

² See Graham Dufault, “Antitrust and You Part 3: Nondiscrimination Provides a Platform for Me but Not for Thee,” ACT | THE APP ASSOCIATION BLOG (Nov. 12, 2021), *available at* <https://actonline.org/2021/11/12/antitrust-and-you-part-3-nondiscrimination-provides-a-platform-for-me-but-not-for-thee/>.

pain management to our customers and meet them where they are.”³ And as Lois Lewis of Missouri-based CoCreate Collective said in another Developed event, “if you can, beta test. Put the product in the hands of users before you officially release. The ability to do that is built into the platform. It’s easy to forget how helpful these built-in tools are.”⁴

We hope that the Committee rejects the overly simple idea that in markets with natural consolidation, large company interests are categorically incompatible with small company interests. In our case, maintaining an even playing field requires Congress to avoid advantaging big businesses by diminishing services and security measures that benefit smaller companies more than larger rivals. Note that the proponents of software platform nondiscrimination are the largest sellers on the app stores,⁵ while the smallest oppose legislation that would prohibit software platforms’ gating functions.⁶ There are a few potential consequences of these bills that are worth considering, from the perspective of App Association members:

1. **H.R. 3816 and H.R. 5017 would make it easier for targeted behavioral advertising-supported businesses to further the aspects of their business models that disrespect privacy expectations and choices.**⁷ For example, Facebook has indicated that it does not want to be subject to platform-level privacy controls software platforms provide for users. Both bills would certainly presume the illegality of privacy restrictions at the platform level that apply to across apps. The relevant provision of H.R. 3816 would ban practices that “restrict or impede a business user from accessing data generated on the covered platform by the activities of the business user, or through an interaction with the business user’s products or services.” The rule of construction in the Manager’s Amendment to the Senate version of the bill, S. 2992, does not appear to address this issue because it only shields a platform operator from liability for “promptly requesting and obtaining the consent of a covered platform user prior to providing access to non-public personally identifiable information of the user” The language seems to only cover real-time prompts for consent as opposed to the expression of a privacy preference that would apply across all apps on a device.

H.R. 5017 includes analogous provisions that together require platforms to allow cross-app tracking by third parties without interference. For example, Section 3(d) requires platforms to provide the “readily accessible means” for users of operating systems to sideload unvetted software and app stores. That provision bolsters a requirement in 3(f) for platforms to provide “access to operating system interfaces, development information, and hardware and software features” on equivalent terms to the platform’s own similar apps. Even though

³ ACT | THE APP ASSOCIATION, DEVELOPED | THE APP ECONOMY TOUR: NEW YORK, NEW YORK (Sept. 19, 2019), available at <https://actonline.org/wp-content/uploads/NYC-Report-V2.pdf>.

⁴ ACT | THE APP ASSOCIATION, DEVELOPED | THE APP ECONOMY TOUR: ST. LOUIS, MISSOURI (Feb. 20, 2020), available at <https://actonline.org/wp-content/uploads/STL-Report-V2.pdf>.

⁵ See Hearing before the Senate Judiciary Committee, Subcommittee on Competition Policy, Antitrust, and Consumer Rights, “Antitrust Applied: Examining Competition in App Stores,” 117th Cong., 1st Sess., (Apr. 21, 2021) (statements of Spotify, Match Group, Inc., and Tile, Inc).

⁶ See Letter from Morgan Reed, president, ACT | The App Association, to Senate Judiciary Committee re: markup of American Innovation and Choice Online Act (S. 2992) (Jan. 20, 2022), Appendix, available at

⁷ See Graham Dufault, “The Great Manipulation: Are Dark Patterns Leading Congress to Help its Biggest Targets?” ACT | THE APP ASSOCIATION BLOG (Oct. 13, 2021), available at <https://actonline.org/2021/10/13/the-great-manipulation-are-dark-patterns-leading-congress-to-help-its-biggest-targets/>.

the Manager’s Amendment to the Senate’s version of this bill would allow platforms to cite a broader range of security and privacy protection reasons for removing an app, the underlying mandate to maintain sideloading still presumptively bans removal of sideloaded software for privacy reasons. Moreover, the evidentiary path for a platform to effectively use the affirmative defense in both the House and Senate versions is so narrow as to be unlikely to inspire any confidence or reliance. Specifically, it requires a defendant to show that the removal was “applied on a demonstrably consistent basis to apps of the [platform] . . . , *not used as a pretext* to exclude, or impose unnecessary or discriminatory terms on, third-party Apps . . . , *and narrowly tailored and could not be achieved through a less discriminatory and technically possible means*” (emphasis added). In other words, Facebook’s attorneys could easily challenge any sort of decision to remove the Facebook app from mobile operating systems for refusing to adhere to a consumer’s decision to have the platform limit tracking by Facebook across apps. Creating a pathway for Meta to evade privacy preferences of smartphone users without a credible threat of removal from the platform, as these bills would do, is plainly counter to Congress’ own efforts to address the harms of social media.⁸ But it is also counter to the interests of App Association members that rely on a marketplace that cultivates trust by respecting and empowering consumers to enforce privacy expectations.

2. **H.R. 3816 and H.R. 5017 would invite the proliferation of security threats like stalkerware and other cyberattacks, which would undermine the trust consumers have in the app ecosystem.**⁹ For example, by requiring software platforms to allow sideloaded software on consumer devices, the bills would erase the security advantage mobile devices have. For the most part, mobile devices are only targets of consumer-level threats if the device runs on an Android operating system (or another operating system that allows sideloading) and someone overrides the default setting that prevents sideloading. The security advantage of iOS’ approach is so lopsided that 98 percent of malware on mobile devices is aimed at Android devices.¹⁰ In other words, cyber attackers see iOS devices as “hard targets” because there is no way to manipulate a consumer into sideloading an app that abuses or exceeds the permission a user gives it to access information and features on the phone like pictures, the camera, the microphone, messaging, and other sensitive things. For iOS users, if they receive phishing messages that link to a direct download of malware, it is likely only because the attacker is hoping they are using Android. And even then, Android is difficult to abuse because consumers must override the default prohibition on sideloading and click through multiple warnings about the security risks of sideloading. Unfortunately, H.R. 5017 and H.R. 3816 would make *all smartphones* soft cybersecurity targets at a time when Congress is calling on small app makers to strengthen their security posture and

⁸ See, e.g., Hearing on “Holding Big Tech Accountable: Targeted Reforms to Tech’s Legal Immunity,” before the House Committee on Energy and Commerce, Subcomm. on Comm. And Tech. (117th Cong., 1st Sess.).

⁹ See Letter from Morgan W. Reed, president, ACT | The App Association, to United States Senate Judiciary Committee (Sept. 15, 2021), available at <https://actonline.org/wp-content/uploads/2021-09-15-ACT-Antitrust-and-Spyware-FINAL.pdf> (discussing the consequences of requiring software platforms to allow sideloading in the stalkerware context).

¹⁰ Joshua Sophy, “98 Percent of Mobile Malware is Aimed at Android Users,” SMALL BUSINESS TRENDS (last updated Sept. 1, 2021), available at <https://smallbiztrends.com/2014/02/98-percent-mobile-malware-aimed-android-users.html>.

protect against attacks on their customers and clients from cyber attacks.¹¹ Russia's invasion of Ukraine has brought these threats ever closer, pushing American private and public sector entities to work together to fend off attacks from State-backed foreign adversaries. Small app makers cannot fight this alone and rely on platforms to secure the marketplace for software.

Specific examples of bad actors taking advantage of the sideloading vulnerability are unfortunately common. The Federal Trade Commission (FTC) recently entered a consent order with SpyFone, a stalkerware app that required its customers to sideload the apps it offered in order to avoid platform controls. Similarly, the recent Anatsa Trojan horse apps¹² and the 1Byte suite of apps have justifiably raised alarms and concern over how consumers can avoid these stalkerware scams.¹³ But, as described above, H.R. 3816 and H.R. 5017 both include provisions that appear to bar a software platform from removing any app, unless it can offer the rather narrow affirmative defense with evidentiary burdens described above. As a result, the bill creates a presumption that removing bad actors found to be surreptitiously stealing consumer data or money is prohibited.

The overall effect of H.R. 3816 and H.R. 5017 in this context would be to create a default presumption barring the removal of stalkerware like SpyFone and the 1Byte or Trojan horse apps like Anatsa's from a platform, unless the platform is able to overcome that presumption, likely in narrower forms, in an expensive process of case-by-case litigation. Although some software firms may have grown large enough that their reputations stand on their own, App Association members generally depend on software platforms to bar bad actors from the marketplace so that consumers feel comfortable downloading software made by otherwise unknown app makers. As Betsy Furler of Texas-based For All Abilities argued during our recent virtual fly-in event, or Mini AppCon (MAC), the platform requirements on companies for baseline security and privacy protections benefit companies like hers that provide smart device-centered accessibility tools and advice. She observed that sideloading, especially if a platform is required to allow it without any security checks, is a major threat vector, as it often leads to malware and viruses being uploaded onto devices unknowingly. She noted that therefore, prohibitions on security and privacy protections would not only seriously hurt her business but would also have a significant impact on the accessibility community that often relies on apps to access and participate in the world.

Lastly, both bills provide a private right of action enabling aggrieved app companies to sue. This authority broadens the penumbra around the bills' prohibitions by inviting interpretations that go beyond what government enforcers would seek to enjoin. The result would be to directly empower those with agendas that subordinate privacy to data

¹¹ Hearing on "Strengthening the Cybersecurity Posture of America's Small Business Community," before the House Committee on Small Business, (Jul. 20, 2021) (117th Cong., 1st Sess.), *available at* <https://smallbusiness.house.gov/calendar/eventsingle.aspx?EventID=3835>.

¹² Dan Goodin, "Google Play apps downloaded 300,000 times stole bank credentials," ARSTECHNICA (Nov. 29, 2021), *available at* <https://arstechnica.com/information-technology/2021/11/google-play-apps-downloaded-300000-times-stole-bank-credentials/>.

¹³ Zach Whittaker, "Behind the stalkerware network spilling the private phone data of hundreds of thousands: A flee of apps share the same security flaw," TechCrunch (Feb. 22, 2022), *available at* <https://techcrunch.com/2022/02/22/stalkerware-network-spilling-data/>.

collection and surveillance to reshape the platforms to suit their aims. But even if the private right of action were removed, leaving only state attorneys general and federal enforcers to bring suit, the breadth of the bills' prohibitions would create unintended issues for the app economy. First, if an enforcement agency brings a lawsuit against a platform for restricting, for example, Meta's access to personal information, the effect on the platform's conduct would not be limited to just Meta. An ongoing lawsuit involving restrictions on access to data for any business user on the platform could easily cause the platform to err on the side of easier access for any business user (including borderline or actual bad actors) as their privacy controls draw public scrutiny from an antitrust lens that deprioritizes privacy. Second, if a law prohibits certain conduct, businesses would be taking extraordinary risks if they were to engage in it anyway, on the hope that enforcement agencies will not notice it or try to enjoin it. This Committee cannot predict the personalities or political agendas that will animate future antitrust enforcement agencies at the federal or state levels. Assuming none of them will bring an action that in some way helps shield a parental control app that people also use to stalk victims—when the text of the bill plainly bars their removal from a platform—is a poor basis for legislative drafting.

3. **H.R. 3816 would prohibit a range of software platform activities and offerings that App Association members pay for at lower cost than they could produce themselves or buy separately on the open market.** App Association members are not necessarily well-known to consumers across the globe. They both demand and pay for access to a marketplace in which consumers trust that software small companies offer is safe to download and that they meet baseline privacy requirements, despite the lack of a prominent profile. H.R. 3816's prohibition on conduct that "advantages the covered platform operator's own products, services, or lines of business over those of another business user" would limit bundled platform offerings for both consumers and developers. On the consumer side, the prohibition would likely limit the availability of pre-installed apps and default features like the software that operates the camera and the default mail app—this in turn limits the usefulness of smart devices, devaluing the products our member companies provide on the platform. On the developer side, the prohibition would likely limit the provision of developer tools, security features, and payment processing, which many developers prefer to sourcing those items on an unbundled and usually more expensive basis.

As Parag Shah of Minnesota-based Vēmos pointed out during a recent virtual MAC meeting with congressional staff, prohibiting the provision of a bundle of services for developers hurts not just the small competitors that use them, but their clients as well. Vēmos serves bars and restaurants, providing analytics and other digital tools that have proven essential for these brick-and-mortar businesses during the pandemic. As Parag explained, if Vēmos' offerings go away, its customers would have to rely on more expensive hardware and software that can't be updated quickly, is not easy to use, and cannot keep up with security and privacy threats. Forcing bars and restaurants to turn to lower-tech, less secure, and more expensive options is surely not what the Committee intends to do. But this is a likely consequence of mandating the dis-integration of services for developers like Vēmos. Stephen Forte, of California-based Fresco Capital, reinforced this point, noting that investors benefit from being able to back companies that can pay a small fee for a set of vertically-integrated platform services. Investment either goes toward these basic overhead elements or it goes into business development and job-creating growth. A requirement to break up the offerings the companies Fresco invests in must start "at zero" with the same size check from investors. This creates a set of conditions that

make it nearly impossible to gain a foothold and then start growing, ultimately causing investors to look to companies that are already more well-resourced and entrenching entrepreneurs with legacy advantages. Put differently, H.R. 3816 would result in higher barriers to entry for small app makers, more difficulty attracting investment, higher costs for App Association member customers like bars and restaurants, and increased costs for developers in the form of cultivating trust on their own without the help and much lower cost distribution avenue provided by software platforms.

4. **H.R. 3816 and H.R. 5017 would prohibit the removal of stolen content and the harmful activity of bad actors using stolen content as bait.**¹⁴ For example, if a fraudster specializing in stolen video content, posing as a fake Disney+, sought to have consumers sideload their video apps in order to upload malware on to as many personal devices as possible, H.R. 3816 would bar a software platform from removing that app and from blocking its access to device features or personal information. The presumption of illegality applies even if Disney filed a takedown notice under Section 512 of the Digital Millennium Copyright Act. Although the software platform could theoretically overcome the presumption by showing the narrow affirmative defense applies, the legal hassle and expense is more likely to deter a platform from squeezing itself between the two sets of obligations just to help the smallest app makers. We appreciate that the Manager’s Amendment to the Senate versions of both bills include provisions exempting “an action taken by a covered platform operator that is reasonably tailored to protect the rights of third parties under [copyright laws].” This could shield meaningful efforts by platforms to remove copycat apps *from the platforms’ own app stores* on behalf of App Association members, but the underlying requirement to allow sideloading in both bills appears to require platforms to do little or nothing about sideloaded software from copyright thieves. Efforts to stop them would also encounter needless challenges, since the platforms would not have been able to vet those apps for proper permissions to access parts of the device and personal information. As a result, App Association members would have to accept a far higher risk that their app will be stolen and that they would have no meaningful recourse, if either of the bills were enacted. This scenario benefits large companies that can do their own policing for content theft while harming small companies that lack the resources to do so in-house.

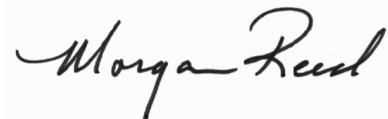
5. **H.R. 3816 could deter software platforms from providing the accessibility features App Association members use to serve clients and consumers with accessibility needs.** As Betsy Furler of App Association member For All Abilities describes, “Apple’s App Store has built-in accessibility features, developer tools, and [application programming interfaces] for everything from speech and Guided Access to VoiceOver and display customization. Features like these ensure that the app works with other accessibility features built into the operating system and are crucial to creating apps for people of all abilities.” The provision of these wraparound services may run afoul of a couple of H.R. 3816’s provisions, including the prohibition on conduct that “the covered platform operator’s own products,

¹⁴ See Debbie Rose, “Sideloading Apps: Mandating That Software Platforms Allow It Will Cost Copyright Owners and Their Customers,” ACT | THE APP ASSOCIATION BLOG (Sept. 17, 2021) *available at* <https://actonline.org/2021/09/17/sideloading-apps-mandating-that-software-platforms-allow-it-will-cost-copyright-owners-and-their-customers/> (discussing the consequences of requiring software platforms to allow sideloading in the copyright context).

services, or lines of business over those of another business user.”¹⁵ Certainly, a software platform offering its own Guided Access feature as part of its bundle of developer services provides a clear advantage for the platform’s own offering over a potential competitor offering such a feature on a standalone basis for developers. Ultimately, the platform’s accessibility features benefit the platform’s consumers on both sides of the market (both end users and app makers) as well as competition, especially in markets defined more broadly than only the offerings on a single software platform—a market definition courts continue to reject.¹⁶

In general, our member companies are worried that large, well-resourced companies may successfully bend the market in their favor by reorienting antitrust law so that it protects larger competitors to the detriment of smaller companies and consumers. We urge Congress not to accede to these demands because doing so would create unacceptable risks to the app ecosystem, and the smallest app makers would suffer the most as a result. We appreciate this opportunity to weigh in with our perspectives on the antitrust legislation Congress is actively considering and look forward to further engagement with you throughout the 117th Congress and going forward.

Sincerely,



Morgan W. Reed
President
ACT | The App Association

¹⁵ ACT | The App Association, “Developed: The App Economy Tour – Houston, TX,” ACT | THE APP ASSOCIATION BLOG (Sept. 14, 2019), available at <https://actonline.org/2019/09/14/developed-the-app-economy-tour-boulder-co-2-2/>.

¹⁶ See *Epic Games, Inc., v. Apple Inc.*, Case No. 4:20-cv-05640-YGR (N.D. Cal. 2021), at 131.