

January 31, 2022

The Honorable Dick Durbin
Chairman
Senate Committee on the Judiciary
Washington, District of Columbia 20510

The Honorable Chuck Grassley
Ranking Member
Senate Committee on the Judiciary
Washington, District of Columbia 20510

Dear Chairman Durbin and Ranking Member Grassley,

As the Committee turns its focus to the Open App Markets Act (S. 2710), we appreciate this opportunity to weigh in on how the bill would impact small app makers. ACT | The App Association (the App Association) is the leading trade group representing small—almost all of our members are 50 or fewer employees—mobile software and connected device companies in the app economy, a \$1.7 trillion ecosystem led by U.S. companies and employing over 200,000 in Illinois and over 40,000 in Iowa 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, education, 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.

Although some of the largest companies selling products and services through the major app stores support S. 2710,² we oppose the bill because it would 1) diminish privacy and security protections on software platforms (app store / operating system combinations); 2) outlaw software platform services like assistance with intellectual property (IP) protection; and therefore, 3) increase overhead costs and barriers to entry for small app makers.

1. S. 2710 would diminish privacy and security protections on software platforms.

S. 2710's requirement for software platforms to provide the "readily accessible means for users" to download apps from sources other than the platform's app store onto their mobile devices³ (referred to as sideloading) would introduce new cybersecurity threats into the app ecosystem. The bill's further requirement that software platforms provide third parties the same level of access to features that the software platform has⁴ also deepens the severity of those cybersecurity threats by forcing the software platforms to allow bad actors access to sensitive parts of smart devices. The bill's carveout for security and privacy protections could be even harder to meet than the affirmative defense in the American Innovation and Choice Online Act (S. 2992), since it requires a platform to show that the protection measure or decision to remove or bar a bad actor was "necessary to achieve user . . . security" (emphasis added) and was "applied on a demonstrably

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 Press Release, Sen. Richard Blumenthal, Blumenthal, Blackburn & Klobuchar Introduce Bipartisan Antitrust Legislation to Promote App Store Competition, (Aug. 11, 2021), <https://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-blackburn-and-klobuchar-introduce-bipartisan-antitrust-legislation-to-promote-app-store-competition> (including a statement of support from Coalition for App Fairness, representing some of the largest companies on the app stores including Match Group, Spotify, and Epic Games).

³ Open App Markets Act, S. 2710, Sec. 3(d) (117th Cong., 2d Sess.).

⁴ *Id.*, Sec. 3(f).

consistent basis to Apps of the Covered Company or its business partners and to other Apps; . . . not used as a pretext to exclude, or impose unnecessary or discriminatory terms on, third-party Apps, In-App Payment Systems, or App Stores; and . . . narrowly tailored and could not be achieved through a less discriminatory and technically possible means.”⁵ Not only must the platform make this rather narrow showing, they would have to do so with a heightened evidentiary burden of “clear and convincing evidence.” Although it could be shown at an earlier stage than if it were an affirmative defense, the carveout appears to be otherwise narrower and harder to reach than S. 2992’s, which itself is mainly unavailable.

Some software platforms allow sideloading, but the main platforms that do so impose guardrails on how consumers download software from third-party sources. Although this may sound at first like micromanagement, it is an exceedingly important aspect of preventing situations where a consumer accidentally—or through manipulation—downloads malware or other harmful content onto their device. For example, Android disallows sideloading by default and consumers can only enable sideloading by going into the device’s settings and enabling the operating system to accept “unknown apps” from specific sources other than the Google Play store.⁶ At this point, Android provides a warning to consumers that “if you download apps from unknown sources, your device and personal information can be at risk. Your device could get damaged or lose data. Your personal information could be harmed or hacked.”⁷ Unfortunately, a mandate for the platform to provide the “readily accessible means for users” to sideload apps or app stores would not just outlaw the iOS model of disallowing any sideloading. It would also create a presumption that any guardrails a software platform imposes on sideloading—such as a warning that enabling sideloading poses a substantial risk to personal information and of being hacked—are illegal.

Evidence of increasing mobile security threats strongly supports disallowing sideloading, or at least requiring consumers to make a conscious decision to overcome a default setting that prevents sideloading—and warning them of the substantial risks associated with enabling it—on mobile devices. Malware attempts on mobile devices have proliferated in the past two years, with the European Union Agency for Cybersecurity (ENISA) reporting 230,000 new malware infections each day in 2019 and early 2020⁸ and mobile phishing schemes increasing 37 percent since the beginning of the pandemic.⁹ Almost none of these attempts—just 2 percent or less¹⁰—affect iOS devices because those devices do not allow sideloading at all and attacking them in this way would yield no results. For example, in one common phishing attempt, attackers send texts to targets that purport to be from their wireless carrier and claiming to offer a gift card for paying the monthly bill, offered via a link. In these attacks, the link might trigger the download of software

⁵ *Id.*, Sec. 4(a) and (b).

⁶ Dallas Thomas, “How to Sideload Apps by Enabling ‘Unknown Sources’ or ‘Install Unknown Apps,’” GADGET HACKS (Jan. 23, 2020), available at <https://android.gadgethacks.com/how-to/android-101-sideload-apps-by-enabling-unknown-sources-install-unknown-apps-0161947/>.

⁷ Fed. Trade Comm’n, Complaint, *In the Matter of Support King, LLC, and Scott Zuckerman*, 192 30003 (Sept. 1, 2021), at para. 6, available at https://www.ftc.gov/system/files/documents/cases/192_3003_spyfone_complaint.pdf (SpyFone Complaint).

⁸ Ann Neville, “Recent cyber-attacks and the EU’s cybersecurity strategy for the digital decade,” EUROPEAN PARLIAMENTARY RESEARCH SERV., (Jun. 2021), available at [https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/690639/EPRS_ATA\(2021\)690639_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/690639/EPRS_ATA(2021)690639_EN.pdf).

⁹ TERRY HE, ET AL., 2021 CYBER THREAT REPORT, SONICWALL, 2021, available at <https://www.sonicwall.com/2021-cyber-threat-report/>.

¹⁰ PURPLESEC, 2021 CYBER SECURITY STATISTICS: THE ULTIMATE LIST OF STATS, DATA & TRENDS, (2021), available at <https://purplesec.us/resources/cyber-security-statistics/>.

intended to infect the device with malware. But this attack cannot be successful unless the target is using a device that allows sideloading *and* the target has enabled sideloading from the text messaging app via the device's settings. The same is true for software intended to help users stalk victims (referred to as stalkerware), an example of which we referred to in a letter to this Committee last year, pointing to the dangers of rolling out the red carpet for apps like SpyFone.¹¹ The unavailability of iOS users as targets for these kinds of attacks has minimized investment in them and caused attackers to focus only on Android devices, where they are still mainly unsuccessful. But a mandate to allow sideloading without guardrails would flip this dynamic on its head, making all mobile device users potential targets and improving investment incentives for attackers. Ultimately, prohibiting the core privacy and security apparatus of software platforms would result in a simultaneous disincentive for platforms to invest in privacy and security features and a strong incentive for bad actors to invest in and innovate on mobile malware attacks.

The costs to American enterprises of malware infections on mobile devices are substantial. Making malware attacks easier would therefore affect how companies and consumers interact with mobile marketplaces. For example, one report found that 97 percent of organizations in 2020 faced mobile threats that used multiple attack vectors and that it costs organizations almost \$10,000 *per* infected mobile device to remediate.¹² As an employer, the federal government recognizes the risks and the costs associated with the fallout of a successful mobile attack on an employee. For example, the United States Department of Homeland Security (DHS) issued a report in 2019 on mobile security, urging federal agencies to treat sideloaded apps and app stores as higher risk, since platform app stores “perform some level of vetting (of both the developer’s identity and of the apps themselves), and requiring the apps to be published openly increases the potential for detecting an adversary’s actions.”¹³ For consumers, the requirement for platforms to allow sideloading would mean that they need to perform the vetting functions on their own, or rely on some other means of vetting. For organizations whose employees rely on mobile devices, they would need to invest more in the vetting functions described in the DHS report and be forced to accept a higher risk of malware infections. For App Association members, the mandate means consumers are less likely to download their offerings because the increased risk of malware and other security threats would cause them to be less likely to download software from a company they have never heard of.

2. S. 2710 would prohibit platforms from helping prevent the theft of App Association members’ content and IP.

S. 2710’s requirement on platforms to support sideloading along with equal access to device and software features to third-party apps and app stores presents a risk of significant increases in content piracy for all copyright owners, including App Association members. The reality is that

¹¹ 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).

¹² CHECK POINT, MOBILE SECURITY REPORT 2021 (2021), *available at* <https://pages.checkpoint.com/mobile-security-report-2021.html>.

¹³ UNITED STATES DEPT. OF HOMELAND SECURITY, EVALUATING MOBILE APP VETTING INTEGRATION WITH ENTERPRISE MOBILITY MANAGEMENT IN THE ENTERPRISE, (Jun. 26, 2019), *available at* https://www.dhs.gov/sites/default/files/publications/4681_evaluatingmobileappvettingintegrationwithemm-clean-r4-508c.pdf.

apps providing access to pirated movies, music, and television are available on all platforms, although less so on mobile platforms thanks in large part to app store prohibitions on content piracy and measures to prevent sideloading of harmful software. A recent report on ad-supported piracy highlighted several examples of apps being used to provide free access to content.¹⁴ Apps like Syncler and Stremio are just two of hundreds of results from a simple search for “free streaming apps.” Notably, the versions of these apps that support free streaming are only available via sideloading, an avenue S. 2710 would widen by requiring software platforms to provide a “readily accessible means” of accessing those apps. Piracy already costs content owners billions each year. S. 2710 would, in effect, clear a path for more piracy, increasing enforcement costs and reducing revenue for creators and app makers. As things are, allowing platforms to use a screening and approval process for apps makes it more difficult for illegitimate apps to get into the store for consumer download.

S. 2710 could also weaken the effectiveness of the notice-and-takedown procedure in Section 512 of the Digital Millennium Copyright Act (DMCA) to get software platforms to remove illegal apps. Section 512 established a system for copyright owners and online entities to address digital piracy. It offered limited liability for online service providers that implement certain measures to prevent piracy, including quickly responding to requests from copyright owners to takedown infringing material. Since becoming law in 1998, copyright owners have grown increasingly dissatisfied with the effectiveness of the provision to fight infringement. In the Section 512 Report issued by the Copyright Office in 2020, copyright owners argued that “...the volume of notices demonstrates that the notice-and-takedown system does not effectively remove infringing content from the internet; it is, at best, a game of whack-a-mole.”¹⁵

Requiring software platforms to allow any app or app store onto smart devices would worsen this dynamic for copyright owners. For example, Busy Bee, one of our member companies, encountered an unfortunate incident where another company stole their children’s app, Zoo Train. Getting the software platform’s attention was no easy task for this small creative house and the App Association helped Busy Bee draft a letter detailing the issue. After some back and forth and due consideration, the platform ultimately removed the copycat, preserving Busy Bee’s prospects.¹⁶ Requiring a platform to allow sideloading, thus prohibiting it from removing the free copycat of an app created by one of our members from the platform, would make Busy Bee’s ultimate success in episodes like this an impossibility. The presumption that removing the copycat is illegal applies even if Busy Bee filed a takedown notice under Section 512. S. 2710’s provision allowing an exemption is only available to the software platform if it can show that removal of the pirate app was “applied in a demonstrably consistent basis to Apps of the Covered Company... 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.” The software platform would have to make this showing by clear and convincing evidence, or else be liable for violating S. 2710 and be subject to civil penalties. This

¹⁴ DIGITAL CITIZENS ALLIANCE, BREAKING [B]ADS: HOW ADVERTISER-SUPPORTED PIRACY HELPS FUEL A BOOMING MULTI-BILLION (B) DOLLAR ILLEGAL MARKET, (Aug. 12, 2021), *available at* <https://www.digitalcitizensalliance.org/issues/breaking-bads>.

¹⁵ UNITED STATES COPYRIGHT OFFICE, SEC. 512 OF TITLE 17: A REPORT OF THE REGISTER OF COPYRIGHTS (May 2020), *available at* <https://www.copyright.gov/policy/section512/section-512-full-report.pdf>.

¹⁶ Alex Cooke, “Member Monday: How One Small Developer Fought a Rogue App,” ACT | THE APP ASSOCIATION BLOG (Nov. 26, 2018), *available at* <https://actonline.org/2018/11/26/member-monday-how-one-small-developer-fought-a-rogue-app/>.

situation would tie the software platform's hands and it could face liability for actions taken in connection with a takedown notice. If copyright owners thought it was a game of whack-a-mole before, imagine if the app stores can no longer serve as a gatekeeper to content piracy.

3. S. 2710 would increase overhead costs and barriers to entry for small app makers.

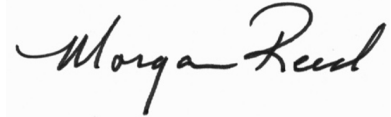
By opening new cybersecurity threat vectors and opportunities for copycat apps, S. 2710 imposes especially heavy costs on the smallest companies on the app stores. Newcomers to this debate might be surprised that this is the case and may have assumed that all app makers want to be able to avoid meeting software platform vetting requirements including those involving privacy and security—or avoiding the registration fees to be a developer (which are \$25 per year for Android and \$99 per year for iOS). But that is not true, especially for small app companies like App Association members. They want to distribute software through a marketplace that consumers trust. If federal law prohibits platforms from removing bad actors, app stores would take on a fundamentally different character, where the consumer is left to their own privacy and security protection skills. As App Association members in the software business before the entry of software platforms know, developing trust without such a marketplace takes substantial investment in marketing and ample amounts of time, which young companies often have only in short supply. Kaity Miller of App Association member SC Codes, which has locations all over South Carolina, noted in our recent Mini AppCon (MAC) covering antitrust issues that she works with several entrepreneurs who are bootstrapping their own companies. In particular, she noted that removing or limiting things like platform-level privacy controls and fraudulent app removal could keep small companies from choosing to develop digital products. She argued that as written, S. 2710 would likely increase the barriers for small companies to enter the digital market when Congress should be seeking to lower those barriers and promoting innovation and diversity. The new dynamic under S. 2710 would require app makers to invest more in developing a public profile through long-term marketing plans to overcome the resulting, more pervasive, presumption that software is unsafe. Small companies receive the short end of this particular stick, as S. 2710 would force them to cede hard-won success to larger rivals that are better positioned with the capital to convince consumers that they have overcome the costs and challenges of a threat-ridden marketplace.

The markup of S. 2992 a couple weeks ago offers plenty of evidence that members of the Senate Judiciary Committee must—and appear to be—carefully thinking about the consequences of limiting the software platform functions for which App Association members pay. Although we understand the competition concerns animating legislation like S. 2710, we believe that as drafted, the bill would both thwart the sponsors' purposes in limiting manipulation-driven business models¹⁷ and result in unintended consequences for privacy, cybersecurity, and the success of small app companies. Moreover, providing carveouts to save some privacy and security measures from overarching prohibitions on protections in place to prevent access to sensitive features and information is simply no substitute for an overarching federal privacy law that mandates privacy protections. We urge you to resist the calls of some of the largest competitors on the app stores to tilt the marketplace in their favor with prohibitions on limiting sideloading and restricting access to

¹⁷ See Hearing on “Protecting Kids Online: Testimony from a Facebook Whistleblower,” before the Senate Committee on Commerce, Science, and Transportation, Subcommittee on Consumer Protection, Product Safety, and Data Security (Oct. 5, 2021), *available at* <https://www.commerce.senate.gov/2021/10/protecting%20kids%20online:%20testimony%20from%20a%20facebook%20whistleblower>.

personal data 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 on S. 2710 and look forward to further engagement with you as you continue to address questions around competition on and around software platforms.

Sincerely,



Morgan W. Reed
President
ACT | The App Association