March 8, 2022

The Honorable Chuck Schumer
Majority Leader
United States Senate
Washington, District of Columbia 20510

The Honorable Mitch McConnell
Minority Leader
United States Senate
Washington, District of Columbia 20510

Re: Open App Markets Act (S. 2710) and American Innovation and Choice Act (S. 2992) Would Create Unacceptable New Threat Vectors in Mobile Ecosystems

Dear Majority Leader Schumer and Minority Leader McConnell,

As Russia and its allies pose advancing cybersecurity threats to American institutions, companies, and individuals, we applaud the Senate's responsiveness, including quick action on legislation to require immediate notifications about indicators of compromise to critical infrastructure. Unfortunately, you are now being asked to hold a vote on the Senate floor on the Open App Markets App (S. 2710) and the American Innovation and Choice Online Act (S. 2992), legislation that would force open new doors for cyber attackers and prevent mobile software platforms (app store / operating system providers) from taking measures to stop and remove malicious apps. 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 37,000 in Kentucky 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.

Recent attacks on consumers' mobile devices indicate an alarming increase in threats to smart devices, providing ample evidence that bills like S. 2710 and S. 2992, which would require software platforms to host unvetted (or sideloaded) software, are not worth the risk. For example, the recent Anatsa Trojan horse apps,[2] the 1Byte suite of stalkerware apps, [3] and SharkBot[4] have justifiably raised questions about the risks of allowing sideloaded software. We also called attention to the Federal Trade Commission's (FTC's) recent consent order with stalkerware maker SpyFone as evidence that bills to prohibit security measures on mobile software platforms should be avoided.[5] **Unfortunately, S. 2710 and S. 2992 include provisions that would bar a software**

[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] 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/.
[3] 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/.
[4] "SharkBot: a new generation of Android Trojans is targeting banks in Europe," Cleafy (Nov. 11, 2021), *available at* https://www.cleafy.com/cleafy-labs/sharkbot-a-new-generation-of-android-trojan-is-targeting-banks-in-europe.
[5] *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-

platform from preventing, removing, or restricting access by any app, unless 1) it can overcome the technical limitations inherent in being unable to vet software, and 2) it can offer a rather narrow affirmative defense with improbable evidentiary burdens. By presuming the illegality of removing or blocking access by any app, S. 2710 and S. 2992 would require software platforms to maintain a default position of allowing any app and any app store on consumers' devices, regardless of the risks they post to privacy and security. We are unaware of any legal or technical analysis that suggests the bills do not create these unacceptable risks, and therefore, we urge you not to support them or give them a floor vote.

The bills' default presumption that software platforms must provide open access to operating system and device features and personal information would create serious technical—not to mention legal—challenges for software platforms to remove apps like SpyFone's, 1Byte's, Anatsa's, or SharkBot. For example, by mandating that software platforms allow sideloaded software on consumer devices, the bills would require the platforms to do nothing proactive about new stalkerware apps like those made by SpyFone and 1Byte. Both SpyFone and 1Byte make apps that a user must sideload onto a target's device in order to spy on them. In both cases, the apps enable the interception of virtually all the device's information, from message and email content to location and photos.

Two requirements in S. 2710 make it technically and legally challenging for software platforms to take any action to stop malicious apps: 1) the requirement to maintain "readily accessible means,"[6] virtually unrestricted, for a consumer to sideload app stores and apps; and 2) the requirement to provide "access to operating system interfaces, . . . and hardware and software features to developers . . . equivalent to the terms for access by similar apps or functions provided by the"[7] software platform. Similarly, several requirements in S. 2992 also create technical and legal barriers to stopping or removing malicious apps, including: 1) the prohibition on conduct that would "materially restrict, impede, or unreasonably delay the capacity of a business user to access or interoperate with the platform, operating system, or hardware or software features that are available to the [apps] of the covered platform operator . . ."[8] and 2) the prohibition on conduct that would "materially restrict or impede a business user from accessing data generated on the covered platform . . . through an interaction of a covered platform user with the products or services of the business user . . .."[9]

The main app stores currently vet apps for "permissions;" that is, which kinds of information to which an app can ask a consumer for access. For example, the main app stores learned long ago that if a simple flashlight app wants to ask consumers for their location data, the app maker better have a good explanation or else there may be an ulterior motive to manipulate a consumer into granting the permission, leading to consumer harms and distressing headlines.[10] Presumably, stalkerware encounters difficulty in the main app stores because it must surreptitiously collect sensitive data from consumers without prompting them for permission at all. So, if a software

---

Antitrust-and-Spyware-FINAL.pdf (discussing the consequences of requiring software platforms to allow sideloading in the stalkerware context).

[6] The Open App Markets Act, S. 2710, Sec. 3(d) (117th Cong., 1st Sess.).

[7] *Id.*, at Sec. 3(f).

[8] The American Innovation and Choice Online Act (S. 2992), Sec. 3(a)(4), (117th Cong., 1st Sess.).

[9] *Id.*, at Sec. 3(a)(7).

[10] *See* Robert McMillan, "The Hidden Privacy Threat of … Flashlight Apps?", WIRED (Oct. 20, 2014), *available at* https://www.wired.com/2014/10/iphone-apps/.

platform discovered that bad actors were using a parental control app on its official app store to stalk people, the app store could shut off the permissions it had approved for use as a parental control app. The platform knows which permissions had been granted, how bad actors were misusing them, and could then shut off that access. However, because stalkerware is generally unavailable in the main app stores and has to be sideloaded, software platforms have to go through additional steps to cut off their access and remove them from devices because the platforms never approved the apps' permissions in the first place. Instead, the platforms must identify the problematic app (or more likely, family of apps), assign a hash to those apps, and push out the hashes to all consumer devices running the platform's operating system, which indicates that the device should no longer allow access by that app. These reactive measures (instead of proactive measures) must necessarily take place slowly and cautiously because S. 2710 and S. 2992 presume that it is illegal to restrict stalkwerware apps' access to the platform and any blacklist a platform develops must also line up (with lots of evidence to back it up) with the affirmative defense. **The requirements ensure that the platforms maintain a content agnostic infrastructure that both 1) allows the initial download of stalkerware onto the platform without restriction, making it technically more difficult to reverse course and block or remove stalkerware; and 2) presumes that stalkerware is not harmful until overwhelming evidence of harm to consumers mounts such that the platform could plausibly raise an affirmative defense, if doing so is less costly than simply allowing the stalkerware to persist.**

The banking "Trojan horse" apps like the Anatsa family of apps and SharkBot are also unable to launch their attacks without manipulating victims into sideloading malicious software. For example, one of the Anatsa apps poses as fitness software, available through the Google Play store with a plausible website to go along with it (although closer inspection reveals the website is filled with boilerplate text).[11] At a certain point, the app prompts the user if they want to unlock further fitness content, which includes a prompt to allow that update to be downloaded outside the Google Play store, via sideloading. The sideloaded "update" is actually malware referred to as a "dropper" that enables the bad actors behind the apps to download further software that can keylog, capture a user's screen, and steal credentials. It is important to note that the makers of Anatsa and similar "dropper" apps took extreme measures to avoid detection by Android's automated threat detection software. For Android, automated threat detection is perhaps even more important than it is for iOS, because Android allows limited forms of sideloading, which raise additional threat vectors not present on iOS.

SharkBot is a similar attack, but instead of prompting users to download the software using a legitimate and approved app in the Google Play store, SharkBot apps simply pose as apps that are in the Google Play store (three examples include Live NetTV, UltData, and Media Player HD).[12] The fake apps even use pirated versions of the real apps' logos—but the SharkBot apps are unavailable in Google Play, and instead, the consumer must sideload them. Once installed on a victim's device, SharkBot immediately accepts the Android-generated prompt to turn on the platform's Accessibility Service (which helps consumers with disabilities access critical device and software features, and mobile services like banking) and then promptly hides the malicious app

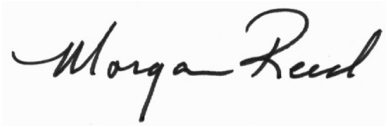
[11] Cedric Pernet, "Android malware infected more than 300,000 devices with banking trojans," TechRepublic (Dec. 8, 2021), *available at* https://www.techrepublic.com/article/android-malware-infected-more-than-300000-devices-with-banking-trojans/.

[12] Peter Arntz, "SharkBot Android banking Trojan cleans users out," MALWAREBYTESLABS (Nov. 16, 2021), *available at* https://blog.malwarebytes.com/trojans/2021/11/sharkbot-android-banking-trojan-cleans-users-out/.

from the home screen. Gaining access to Accessibility gives SharkBot the ability to use the Accessibility Service's autocomplete and related features in the victim's banking app or apps, thwarting behavioral detection countermeasures (e.g., biometrics) put in place by banks. SharkBot and Anatsa have successfully infected about 310,000 devices that researchers know of, and this success rate is only possible because Android allows sideloading. This is a real-life illustration of how prohibiting software platforms from vetting all apps exposes us to greater security risks. But S. 2710 and S. 2992 go much further and would diminish the tools Android currently uses to stop these apps by presuming the illegality of removal or other restrictions, while requiring all devices to be vulnerable to malware attacks. Mandating that software platforms allow banking trojans to be downloaded onto consumers' devices—and crippling their efforts to address the threats they pose with technical and legal obstacles—would bring malware like SharkBot and Anatsa into the mainstream. The attacks we read about would soon become the proximate threats we must constantly avoid on our own devices.

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. The proposals they now support, S. 2992 and S. 2710, create a presumption that fundamental mobile security and privacy measures are illegal. We urge Congress not to accede to their 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

1401 K Street NW Suite 501
Washington, DC 20005

202.331.2130 @ACTonline
ACTonline.org /actonline.org