September 15, 2021

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

The Honorable Amy Klobuchar
Chairwoman
Senate Committee on the Judiciary
Subcommittee on Competition Policy,
Antitrust, and Consumer Rights
Washington, District of Columbia 20510

The Honorable Mike Lee
Ranking Member
Senate Committee on the Judiciary
Subcommittee on Competition Policy,
Antitrust, and Consumer Rights
Washington, District of Columbia 20510

Dear Chairman Durbin, Ranking Member Grassley, Chairwoman Klobuchar, and Ranking Member Lee,

We applaud this Committee for its ongoing examination of the competitive dynamics of tech-driven markets, including the Subcommittee on Competition Policy, Antitrust, and Consumer Rights hearing in April, "Antitrust Applied: Examining Competition in App Stores." 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 205,360 in Illinois, 41,930 in Iowa, 108,260 in Minnesota, and 65,520 in Utah 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.

During your examination of app stores, stakeholders have urged you to prohibit software platforms (app store / operating system combinations) from performing a gatekeeping function.[2] However, recent consumer protection enforcement by the Federal Trade Commission (FTC) illustrates why a statutory mandate for app stores to allow unvetted software onto smart device operating systems could harm consumers.

On September 1, 2021, the FTC published an initial complaint, along with a unanimously approved settlement, with SpyFone.[3] According to the complaint, SpyFone marketed itself as a surveillance

[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, e.g.,* Hearing on "Antitrust Applied: Examining Competition in App Stores," before the Senate Judiciary Committee Subcommittee on Competition Policy, Antitrust, and Consumer Rights, statement of Dr. Mark Cooper, Dir. of Research, Consumer Federation of America (117th Cong., 1st Sess.) (Apr. 21, 2021), *available at* https://www.judiciary.senate.gov/imo/media/doc/Cooper%20Testimony.pdf.
[3] Press release, Fed. Trade Comm'n, "FTC Bans SpyFone and CEO from Surveillance Business and Orders Company to Delete All Secretly Stolen Data" (Sept. 1, 2021), *available at* https://www.ftc.gov/news-events/press-releases/2021/09/ftc-bans-spyfone-and-ceo-from-surveillance-business.

1401 K Street NW Suite 501
Washington, DC 20005
202.331.2130 @ACTonline
ACTonline.org /actonline.org

app, enabling purchasers to track targets in a variety of ways, including by spying on live location, web history, contacts, pictures, calendar, files downloaded onto a device, notifications, emails, video chats, and even social media posts.[4] The company explained to its users how to download the app on a target's device, hide the app so the target would not notice its presence, and bypass Android operating system controls in order to track the target without their knowledge.

Under current law, SpyFone's illegitimate business is rather difficult to carry out, and law enforcement agencies like the FTC can readily investigate their activities. Because iOS prohibits sideloading (downloading software onto a smart device from outside the main app store), and Apple's App Store generally bars apps that are marketed as stalkerware, SpyFone is virtually impossible to install on an iOS device. But even Android presents problems for SpyFone: the Google Play store also generally declines these apps; and by default, the current (and recent) versions of Android disallow sideloading. However, going into the settings, users can allow sideloading from "unknown sources," one at a time. For example, users can enable software to be downloaded from the device's web browser. According to the FTC complaint, SpyFone instructed its users to take these steps in order to download SpyFone from a browser. However, further steps were necessary to enable additional SpyFone features such as viewing outgoing email, including "rooting" the mobile device, giving the purchaser "privileges to install other software on the mobile device that the manufacturer would not otherwise allow."[5] The FTC complaint explains that this access "enables features of the SpyFone products to function, exposes a mobile device to various security vulnerabilities, and can invalidate warranties that a mobile device manufacturer or carrier provides."[6] But the fact remains that SpyFone has to walk a purchaser, who has access to their target's device, through a series of steps to defeat the controls Android has in place**. If, on the other hand, Congress prohibits software platforms from preventing sideloading—whether by prohibiting software platforms from disadvantaging offerings on the platform, prohibiting broad notions of "retaliation" by platforms against app makers, or by some other means—that prohibition likely also bars those Android controls that stand in SpyFone's way.**

For example, **prohibiting a software platform from conduct that "excludes or disadvantages the products, services, or lines of business of another business user . . . relative to the [platform's] own"[7] offerings (as the American Choice and Innovation Online Act (H.R. 3816) would do) prohibits the platform from removing (excluding) any app that arguably has a similar offering to the platform's.** Stalkerware apps could easily claim that iOS and Android have similar offerings because their legitimate uses, as marketed, involve parents managing their children's devices. In this scenario, Android clearly disadvantages SpyFone versus its own offerings by forcing it to go through onerous steps in order for a purchaser to make use of the app. For example, Android forces SpyFone to have its purchasers enable the sideloading capability, which triggers a warning from Android that "[i]f 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."[8] Certainly, these additional steps and a warning like this hurt SpyFone's business. Likewise, iOS disadvantages SpyFone versus its own offerings because it

---

[4] Fed. Trade Comm'n, Complaint, *In the Matter of Support King, LLC, and Scott Zuckerman*, 192 30003 (Sept. 1, 2021), *available at* https://www.ftc.gov/system/files/documents/cases/192_3003_spyfone_complaint.pdf (SpyFone Complaint).
[5] *Id.* at para. 7.
[6] *Id.*
[7] American Choice and Innovation Online Act (H.R. 3816, 117th).
[8] SpyFone Complaint at para. 6.

does not allow SpyFone on iOS devices at all. And the affirmative defense H.R. 3816 provides in cases where a software platform needs to remove an app for violating a law or threatening consumer privacy does nothing to help because as drafted it is so inaccessible as to discourage any sort of reliance on it. **The overall effect of H.R. 3816 in the stalkerware context is to create a default rule barring the removal of stalkerware like SpyFone from a platform, as well as any privacy-related barriers that prevent stalkerware from taking advantage of consumers, unless a platform is able to overcome that presumption, likely in narrower forms, on a case-by-case basis.**

The bottom line is that **taking a nondiscrimination sledgehammer to software platforms' role in removing bad actors rolls out the red carpet for apps like SpyFone. More insidiously, by widening the avenues for fraudsters on app stores, an overbroad federal nondiscrimination regime would narrow the path for smaller app makers like App Association members.** It would also make the FTC's job in enforcing the statutory prohibition on unfair or deceptive acts or practices that much more difficult, as more bad actors enter the fray and less of their activity is discoverable because platforms' hands would be tied. Meanwhile, as consumers adjust to a more fraud and malware-ridden marketplace, they would rationally shift away from experimentally downloading apps with the shortest histories and smallest preexisting distribution in favor of bigger brands. What is now a high trust environment, thanks in no small part to rigorous gating, would then evolve into a no-trust environment, which disproportionately harms smaller companies while benefiting the platform's largest "business users."

As the Senate Judiciary Committee continues its work on antitrust in tech-driven markets, we hope the perspective of small mobile software and connected device companies that leverage software platforms helps guide your work. 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 increased risk of stalkerware is just one potential outcome if Congress accedes to these demands. We appreciate this opportunity to weigh in on your important inquiry and look forward to further engagement with you throughout the 117th Congress and beyond.

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