February 2, 2022

The Honorable Richard J. Durbin
Chair, Senate Judiciary Committee
United States Senate
711 Hart Senate Building
Washington, DC 20510

The Honorable Chuck Grassley
Ranking Member, Chair, Senate Judiciary Committee
United States Senate
135 Hart Senate Building
Washington, DC 20510

Re: Markup of S.2710, the Open App Markets Act (February 3, 2022)

Dear Members of the Senate Judiciary Committee:

We write to express our concerns about S.2710. Even with the manager's amendment, this bill would make it extraordinarily difficult for app stores to protect user privacy, security, and digital safety, and to prevent violations of law, from copyright infringement to the dissemination of child sexual abuse material. To avoid such unintended consequences, we propose four edits. Three would make affirmative defense found in Section 4(b) consistent with the overall purpose of the bill: limiting self-preferencing by app stores. The fourth would ensure that the affirmative defense applies to new ways to protect app users.

Section 3 prohibits an app store from various forms of self-preferencing — defined so broadly as to include many things app stores do today to protect users from harmful apps and various scams, from screening or blocking harmful apps to recommending trusted apps and offering users payment systems that protect against fraud, offer refunds, etc. Section 4(a) creates an affirmative defense for actions that would violate Section 3, but that are "(1) necessary to achieve user privacy, security, or digital safety; (2) taken to prevent spam or fraud; or (3) taken to prevent a violation of, or comply with, Federal or State law."

In three respects, Section 4(b) sets the bar so high that Section 4(a)'s affirmative defense will not prevent the bill from causing significant harm to users. In effect, the bill creates a permitting regime for app store privacy, security and child safety policies — first by banning a wide variety of best practices intended to protect privacy, security, and intellectual property rights, or to guard against other violations of law, and second, by offering an affirmative defense that is largely useless, effectively requiring regular judicial approval for each such practice. Since protecting Internet users is a never-ending process, so, too, will be a company's legal exposure: Any time a platform makes a change to its app store, an opportunistic plaintiff will challenge the move as discriminatory or self-preferencing, forcing the platform to defend the move in court.

Recommendation #1: Delete § 4(b)(3) ("Strict Scrutiny")

This provision requires an app store to show that its actions were "narrowly tailored and could not be achieved through a less discriminatory and technically possible means." This replicates key parts of the strict scrutiny test developed by the Supreme Court for assessing whether certain kinds of legislation violate fundamental constitutional rights. But Section 4(b)(3) would require private companies, rather than state actors, to justify their actions. And instead of protecting a well-established constitutional right, such as free speech, the bill aims to promote some novel, amorphous form of what a "competitive app market" should look like. There is simply no precedent for imposing so heavy a burden in an affirmative defense. For the first time in American history, private companies would be required to justify their actions under a standard so high that it has long been called "'strict' in theory and fatal in fact."[1]

This impossibly high standard will necessarily hinder app stores from responding swiftly to always-evolving threats. App stores encounter a wide variety of harmful content on their platforms, including scams, counterfeit apps, fraudulent payment systems, and stalkerware. For example, Google recently removed a malware app masquerading as a two-factor code manager,[2] and experts warn against the rise of fake tax apps which steal financial data.[3] In response to these threats, app stores must enforce privacy, security and safety policies which address a myriad of concerns. Forcing app stores to "narrowly" tailor their policies undermines their ability to craft robust protections against a wide variety of rapidly changing threats.

That requirement, in conjunction with Section 4(a)(1)(A)'s requirement that an app store prove the "necessity" of measures taken to promote "user privacy, security, or digital safety," will force app stores to follow a piecemeal approach. Under the Act, any time an app store encounters a threat on its platform, it must craft a narrow policy tailored to address that threat alone, or at most a body of threats closely resembling that specific issue. But threats encountered on app stores overlap and evolve rapidly. Piecemeal enforcement addressing each threat individually will never keep pace with novel threats — or even threats which fall just outside the definition spelled out in the policy.

In addition, the Act would force app stores to prove that their security protocols are "less discriminatory" than any other possible method of fixing a given issue, a burden which is unreasonable if not impossible to prove. An opportunistic plaintiff could argue that Apple and Google banning his fake tax app was *not* the least discriminatory means of protecting their users. Instead, the plaintiff could argue, the app stores should have merely blocked certain features of the app or

[1] Gerald Gunther, *The Supreme Court, 1971 Term - Foreword: In Search of Evolving Doctrine on a Changing Court: A Model for a Newer Equal Protection*, 86 HARV. L. REV. 1, 8 (1972).
[2] Ryan Whitwam, *Malware Masquerading as Android 2FA App Infected 10,000 Phones Before Removal*, EXTREMETECH (Jan. 31, 2022), https://bit.ly/3IVmXyg.
[3] Andrew Whaley, *Beware of fake tax apps pushing malware*, HELPNETSECURITY (Jan. 25, 2022), https://bit.ly/3upVQHw.

warned users before downloading. As such, the Act disincentivizes app stores from taking all necessary steps to protect their users from scams.[4]

Recommendation #2: Delete § 4(b)(2) ("Pretext", "Unnecessary" & "Discriminatory")

This provision requires an app store to establish, by a preponderance of the evidence, that its actions were "not used as a pretext to exclude, or impose unnecessary or discriminatory terms on, third-party apps, in-app payment systems, or app stores." The second part ("impose…") is duplicative with Section 4(b)(1)'s ban on self-preferencing and is therefore unnecessary. The first part ("not used as a pretext") is, in some cases, duplicative of the carveouts in Section 4(a) or, in other cases, flatly contradictory with their purpose. Thus, both should be deleted.

Section 4(a)(1) excludes from liability four categories of actions. In two categories where line-drawing is hard — "achiev[ing] user privacy, security, or digital safety" and "prevent[ing] unlawful infringement of preexisting intellectual property" — the defendant app store must prove its actions were "necessary." Proving necessity may well be too high a bar even on its own in light of the vigilance required to implement best security practices, but the requirement certainly removes the need for any inquiry into alleged pretext. If, for example, a covered company proves that it was necessary to remove an app serving pirated movies from its app store to protect against infringement of intellectual property, that should conclusively decide the matter.

The other two categories involve preventing conduct where the lines can be drawn much more clearly: any "violation of … Federal or State law" and "spam or fraud." Here, it should not matter what an app store's motive was. And yet even here, Section 4(b)(2) requires an app store to prove a negative: that its actions were not pretextual. This effectively introduces a "necessity" requirement by the backdoor, rendering superfluous the effort in 4(a)(1) to distinguish between these two very different kinds of content. If the purpose of 4(a)(1)(B), for example, is to protect against fraud, surely an app store should remove fraudulent malware even if it cannot prove purity of motivation because such content is self-evidently harmful. Would anyone seriously suggest that app stores should only be allowed to police apps to prevent grooming children for sexual abuse if the app store can prove that it had no other motive? The benefit of removing such an app would clearly outweigh any pretext that could possibly be proven. Requiring a covered company to prove non-pretextual justifications is simply incompatible with expecting companies to protect against unlawful or otherwise harmful activity — which seems to be policy preference underlying the decision not to require necessity for 4(a)(1)(A) and (B). Imposing a backdoor "necessity" requirement only makes app stores less likely to proactively protect against those harms, lest their actions be found "unnecessary" when some bad actor sues them.

[4] In 2021, Apple blocked $1.5 billion in suspected app store fraud. *App Store stopped more than $1.5 billion in potentially fraudulent transactions in 2020*, Apple Newsroom (May 11, 2021), https://apple.co/3J1ptCW. In 2020, "Google Play Protect scanned over 100B installed apps each day for malware across billions of devices," its "machine-learning detection capabilities and enhanced app review processes prevented over 962k policy-violating app submissions from getting published to Google Play," and it "banned 119k malicious and spammy developer accounts." Krish Vitaldevara. *How we fought bad apps and developers in 2020*, Google Security Blog (Apr. 21, 2021), https://security.googleblog.com/2021/04/how-we-fought-bad-apps-and-developers.html.

Moreover, this burden-shifting flips the longstanding conventional rules of civil litigation, and imposes a hurdle even higher than in employment discrimination cases, where First Amendment rights are clearly implicated. Under the *McDonnell-Douglas* framework,[5] an employer facing a plaintiff who establishes a *prima facie* claim of discrimination need only articulate a legitimate, non-discriminatory reason for its actions, but the *plaintiff* still bears the ultimate burden of proving that the employer's reason was pretextual.[6] Here, by contrast, a plaintiff need only allege that an app store engaged in some ostensibly prohibited activity, whereupon the app store has the burden of proving not only that its actions fall under a carveout of Section 4(a), but also that its decision to take that action was motivated by pure intentions. Shifting the burden of disproving allegations of "pretext" to defendants unfairly relieves plaintiffs of the responsibility to prove essential elements of their case. There is no obvious justification for so strongly advantaging plaintiffs in these everyday disputes to a greater extent than even plaintiffs in civil rights cases.

Recommendation #3: Clarify § 4(b)(1) (Consistency) to Focus on Self-Preferencing

Unlike S.2992, Section 4(b)(1) requires an app store to show that its actions were "applied on a demonstrably consistent basis to Apps of the Covered Company or its business partners and other Apps." To make this provision consistent with the overall goal of the bill, preventing self-preferencing, it should be amended as follows:

> (b) Requirements.—Section (a) shall only apply if the covered company establishes by a preponderance of the evidence that the action described in that subsection is—
>
> (1) applied on a demonstrably consistent basis ***as between*** ~~to~~ —
>
> (A) apps of the covered company or its business partners; and
>
> (B) other apps;

This edit is subtle but important. As drafted, this provision could be interpreted to require an app store to prove that it had "consistently" applied its policies on privacy, security and unlawful content *across all apps* — a daunting, if not impossible, task. Content moderation is inherently subjective, imperfect, and impossible to do consistently at the scale of the Internet.[7] Developers of apps removed from app stores for violating policies will always be able to point to examples of other apps not treated similarly despite posing supposedly similar risks. There is no need for courts to grapple with such questions; instead, an app store should be eligible for the affirmative defense only if it cannot show that it did not engage in self-preferencing.

---

[5] *See* McDonnell Douglas Corp. v. Green, 411 U.S. 792, 802–03 (1973) ("The complainant in a Title VII trial must carry the initial burden under the statute of establishing a prima facie case of racial discrimination. . . . The burden then must shift to the employer to articulate some legitimate, nondiscriminatory reason for the employee's rejection.").

[6] *See* Price Waterhouse v. Hopkins, 490 U.S. 228, 245 (1989) ("[E]ven after a plaintiff has made out a prima facie case of discrimination under Title VII, the burden of persuasion does not shift to the employer to show that its stated legitimate reason for the employment decision was the true reason.").

[7] Mike Masnick, *Masnick's Impossibility Theorem: Content Moderation At Scale Is Impossible To Do Well*, TechDirt (Nov. 20, 2019), https://bit.ly/3s8ffKa.

This is also a more focused way of dealing with the core harms addressed by the bill than requiring the defendant to prove that its justifications were "not used as a pretext." Leaving unspecified what would constitute a "pretext" invites abusive litigation by creative plaintiffs. Our edit effectively bars defenses that are "pretextual" for self-referencing clearly defined.

Recommendation #4: Clarify that § 4(a)(2)'s List of Examples Is Not Exclusive

Section 4(a)(2) lists four specific examples of "privacy and security protections" that would qualify for the affirmative defense under Section 4(a)(1)(A). This should be amended to clarify that this is not intended to be an exhaustive list and that, like Section 4(a)(1)(A), it also applies to user safety:

> (2) PRIVACY***,*** ~~AND~~ SECURITY ***AND SAFETY*** PROTECTIONS.—In paragraph (1), the term "necessary to achieve user privacy, security, or digital safety" includes***, but is not limited to***— …

This will ensure that courts interpret this provision to allow app stores to protect privacy and security in ways that cannot be predicted today or codified in legislation. Of course, app stores would still bear the same burden of showing that such protections are "necessary."

—

Thank you for your attention to our concerns. We would be happy to assist your Committee in working to revise Section 4 so that the bill's affirmative defenses do not shield self-preferencing but *do* protect actions taken to protect consumers from privacy and security threats, and unlawful content.

Sincerely,

Berin Szóka
President, TechFreedom
bszoka@techfreedom.org

Ari Cohn
Free Speech Counsel, TechFreedom
acohn@techfreedom.org