31 January 2022

The Honorable Dick Durbin
Chair
Committee on Judiciary
711 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Chuck Grassley
Ranking Member
Committee on Judiciary
135 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Amy Klobuchar
Chair
Subcommittee on Competition Policy,
Antitrust, and Consumer Rights
425 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Mike Lee
Ranking Member
Subcommittee on Competition Policy,
Antitrust, and Consumer Rights
361A Russell Senate Office Building
Washington, D.C. 20510

RE: S.2992 and S.2710

Dear Chair Durbin, Chair Klobuchar, Ranking Member Grassley, and Ranking Member Lee:

I am Bruce Schneier, a longtime security technologist, author, speaker, and thinker; and author of many books, papers, and articles on the topic both Internet security and privacy. I currently teach cybersecurity policy at the Harvard Kennedy School.1 I am writing in support of S.2992 and S.2710, which are attempts to redress the power of dominant technology firms.

S.2992 bars large tech companies from unfairly preferencing their own products on platforms they own or control. S.2710 prohibits forcing app developers to use a specific in-app payment system owned or controlled by the owner of the app store. Both have size thresholds to ensure these limits only apply to extremely large firms.

I would like to address some of the unfounded security concerns raised about these bills. It's simply not true that this legislation puts user privacy and security at risk. In fact, it's fairer to say that this legislation puts those companies' extractive business-models at risk. Their claims about risks to privacy and security are both false and disingenuous, and motivated by their own self-interest and not the public interest. App store monopolies cannot protect users from every risk, and they frequently prevent the distribution of important tools that actually enhance security. Furthermore, the alleged risks of third-party app stores and "side-loading" apps pale in comparison to their benefits. These bills will encourage competition, prevent monopolist extortion, and guarantee users a new right to digital self-determination.

[1] Bruce Schneier, "Schneier on Security." https://www.schneier.com.

1. The bills will not prevent platforms from introducing new privacy and security measures.

Apple claimed in a letter that S.2992 would erect "steep obstacles" in front of new privacy and security protections.2 This is simply not true; the bill only prohibits "unfairly preferencing" a platform's products or services or "unfairly limiting" another business relative to the platform.3 The bill does not prohibit changes that affect all apps, such as Apple's App Tracking Transparency framework, which limits every app's access to personal information until a user has granted their informed consent. Any future changes that a platform makes to enhance privacy and security will still be permitted, as long as those changes are applied fairly to the platform's own products and services as well as to third parties.

2. Alternatives to an app store monopoly will enhance user choice, and will not lead to a wave of malware attacks.

In another section of the letter, Apple attacks S.2710's interoperability requirements, claiming that its requirement to allow "side-loading" of apps will likely lead to "millions" of new malware attacks on Americans. It also claims that this requirement prevents users from "choosing" a secure and private device.

First, nothing in S.2710 requires Apple or anyone else to open its devices to side-loading. (Side-loading refers to the installation of apps that have not been verified by any app store.) The bill only requires that the company "allow and provide the readily accessible means for users of that operating system to . . . install third-party Apps . . . through means other than its App Store."4 This interoperability does not require one-click installation of random apps from the Internet, only that companies relinquish their monopoly control over app stores. Alternative stores could have the same, or even more, security restrictions than Apple. And instead of one app store controlled by Apple, users would be able to choose between many.

Second, Apple's reasoning regarding side-loading is self-interested, oversimplified, and dishonest. Side-loading is not a means for bad actors to vault over a platform's secure walls and into user's private lives; it's a way for users to exercise agency over their own devices. Side-loaded apps bypass the app store moderation process, but moderation is not the only level of protection between users and malware. Sophisticated malware often relies on technical exploit to get around operating system-level restrictions on its behavior, and side-loading wouldn't affect Apple's ability to restrict what rogue apps are capable of doing.

Apple tries to imply that users who want to stay within its trusted ecosystem will be forced to take on new risks, or that non-technical users will be blindsided by new malware. This is simply not true. Side-loading could be implemented in a way that ensures users are aware of the risks they take on before installing a piece of unverified software. Users who do not want to side-load

---

[2] 1/18/22 letter to the Senate Judiciary Committee, available at https://9to5mac.com/wp-content/uploads/sites/6/2022/01/Apple-letter-full.pdf.
[3] S.2992 Section 2(a).
[4] S.2710 Section 3(d)(2).

apps can easily choose not to, just as users today can choose not to jailbreak their phones. (Jailbroken phones are ones that have been modified in a way that contravenes Apple's rules to allow the installation of software the Apple prohibits.)

Finally, Apple's assertion that it is defending user "choice" gets it exactly backwards. Our devices are our own, and interoperability will allow us to use them as we choose. Any user who prefers to use only Apple-approved applications will have no trouble doing so. But S.2710 will finally give users the freedom to leave the walled garden: to build, share, and install software that hasn't been approved by Apple's moderation machine.

3. The bills will help users who are harmed by a single company's moderation decisions.

Arguments against these bills assume that a single company is capable of being an effective moderator for millions of applications affecting billions of users. And, that the same company that builds the platform is necessarily that single company. This is not true. Experience has demonstrated that monopolistic app stores both miss apps that would harm security and reject ones that would help it. Allowing alternative app stores -- and allowing users to choose different moderators -- is the only way to ensure users can configure their devices securely.

App store moderation frequently misses important threats to privacy and security, including data brokers and scammers. Both Apple and Google have approved apps that egregiously violate user privacy and security, often in direct contradiction to their own policies.[5] The incredible volume these marketplaces handle (Apple's App Store receives 100,000 submissions per week) means that they cannot possibly vet every single app as thoroughly as desired. A smaller, alternative app store could set its own policies that are stronger and better enforced than a large platform is capable of.

Furthermore, app store review processes frequently bar apps that would meaningfully improve user privacy and security. For example, Google's Play Store policies prevent the development of ad- and tracker-blocking software.[6] This is a predictable result of Google's misaligned incentives as an advertising company as well as an app store moderator. But Android allows third-party app stores and side-loading of apps, so users have the option to install meaningful privacy tools from outside of Google's approved crop.

Apple has its own misaligned incentives. Apple has removed many VPN apps from its Chinese App Store at the request of the Chinese government.[7] VPNs are a key tool to help users evade

---

[5] Scott Ikeda, "Data Brokers Continue To Use X-Mode Location Tracking in Spite of Ban," 2/5/2021. https://www.cpomagazine.com/data-privacy/data-brokers-continue-to-use-x-mode-location-tracking-in-spite-of-ban/.

[6] Joe Hindy, "Why Google bans ad blockers, but is actually fine with ad-blocking browsers," 1/27/2019. https://www.androidauthority.com/google-play-ad-blockers-ban-945058/.

[7] Saheli Roy Choudhury, "Apple removes VPN apps in China as Beijing doubles down on censorship," 8/1/2017. https://www.cnbc.com/2017/07/31/apple-removes-vpn-apps-in-china-app-store.html.

surveillance and censorship by oppressive governments. Without a sanctioned way to install non-App Store apps, users in China have no easy way of accessing private networks that are not approved by the government. But Apple has made the decision that appeasing the Chinese government is more profitable than protecting its users.

In another incident, Apple removed an app that was intended to detect whether a phone had been secretly jailbroken. Jailbroken phones allow more than just unsanctioned apps to be installed; they can also harbor spyware without their owner's knowledge. Jailbreak detection is a useful function for people who have purchased a used phone, or who may be victimized by someone close to them. But Apple determined that this security app was against its App Store terms of service, depriving at-risk users of a valuable layer of protection.

Giving tech companies a veto over which software users can and can't trust is a system that fails badly. That is: it's one thing to seek a company's recommendations about what constitutes a security risk, and another to let that company's judgment override your own. The former requires that the company be reliable, the latter requires that the company be infallible. And companies are not infallible. One example: for many years, both the Google and Apple mobile app stores routinely approved "stalkerware" apps. These are apps that are used to covertly surveil device owners, tracking their location and communications. Stalkerware is not benign or secure. Rather, it is widely implicated in domestic violence and intimate partner abuse.[8] Eventually, due to unrelenting pressure from organizations like the Electronic Frontier Foundation, the dominant platforms instituted a policy banning stalkerware, but not before many of their customers were placed in harm's way by the platforms' poor judgment.[9] Even today, the platforms continue to list and sell software that is functionally identical to stalkerware, provided that it is marketed as a way for parents to keep tabs on their children or employers to keep tabs on their employees.

Again and again, these platforms have chosen profits over their user's security and privacy. Allowing third-party app stores and interoperability will remove the barriers to independent distribution of niche or unsanctioned tools for security and privacy. We cannot, and should not, trust a single company to make the correct decisions about device security, privacy, and integrity for billions of users.

Conclusion

We already know what a platform that allows any software to be installed looks like: it's how our computers work. Whether we use Windows, or MacOS, or Linux, there is no monopoly dictating what software we can or cannot use. We can run our computers securely, or we can choose not to. Far from it being the dangerous hellscape we're told to fear, the results are actually pretty

---

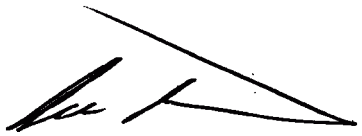
[8] Kim Key, "How Stalkerware Enables Domestic Abuse," 8/4/2021. https://www.pcmag.com/news/how-stalkerware-fits-into-a-tech-assisted-domestic-abuse-cycle https://www.securemac.com/news/how-to-check-for-stalkerware-on-an-iphone.

[9] Catalin Cimpanu, "Google 'formally' bans stalkerware apps from the Play Store," 9/16/20. https://www.zdnet.com/article/google-formally-bans-stalkerware-apps-from-the-play-store/.

good. Yes, there is malware. Yes there are attacks. But there is security and safety as well. Hundreds of companies innovate in this space, developing new security and privacy technologies that we are free to install if we choose.

Out in the real world, we give people the freedom to choose their own level of risk. It might be objectively true that Disneyland is safer than a public park, but that doesn't mean we should outlaw all public parks and give Disney a monopoly on park-like gathering places. People are free to visit Disneyland, and pay for the privilege. They are free to visit other companies' commercial parks. And they are free to visit any of our nation's public parks. Our laptops are like public parks, that we can arrange with whatever amenities and safeguards we choose. There is no reason our phones should not be as well.

Sincerely,



Bruce Schneier

Cc: Senate Judiciary Committee