March 3, 2022

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

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

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

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

Dear Senators:

Apple has previously written to you regarding our concerns with S. 2992, the American Innovation and Choice Online Act, and S. 2710, the Open App Markets Act. Our communications have reflected Apple's views about the potentially negative consequences of these bills, and we have been gratified that some of our concerns have been addressed during the Committee's consideration of the legislation. We hope to continue this dialogue going forward.

Today, however, we write regarding a letter sent to the Committee by cryptographer Bruce Schneier, in which he called Apple's concerns regarding the impact of mandatory sideloading and forced interoperability "unfounded," "disingenuous," and "dishonest." Given our general regard for Mr. Schneier, these accusations are particularly disappointing. In our experience, the work of providing leading security and privacy to a modern computing platform at billion-device scale is among the most enormously complex and challenging engineering and technical policy endeavors, and much about this work remains easy to misunderstand. Mr. Schneier's letter underscores that even talented technical

Apple
One Apple Park Way
Cupertino, CA 95014

T 408 996-1010
F 408 996-0275

practitioners, if they have not worked on key problems in this space, can confound the issues. Accordingly, we would like to offer some additional context in this letter.

Most mobile malware relies on tricking users, not bypassing device-based security controls.

Device-based security controls are an essential pillar of the security and privacy of any computing platform, and perhaps the most well-understood aspect of computer security. But in our experience with actual attacks targeting real users every day, device-based security controls are most effective when fully integrated with human review. Solely focusing on device controls has caused other platforms, and the security industry as a whole, to forgo critical opportunities to impede and stop malicious actors before they can meaningfully target users.

The vast majority of mobile malware fundamentally doesn't rely on any "technical exploits" to bypass device-based security controls. Instead, it relies on tricking the user into willingly surrendering access to their device. Apple recently reviewed the top 20 Android mobile malware apps listed in Nokia's 2021 threat intelligence report, which covered 99% of the Android malware detected by Nokia — and not a single one appeared to use a "technical exploit" to get onto the device or perform its attack. These apps all worked within the security boundary of the operating system, with no exploit required.

Kaspersky came to a similar finding: "[i]n their campaigns to infect mobile devices, cybercriminals always resort to social engineering tools, the most common of these passing a malicious application off as another, popular and desirable one. All they need to do is correctly identify the application, or at least, the type of applications, that are currently in demand."[1] On Android, apps offered outside of the official store and claiming to help protect users' security turn out, with some frequency, to be malware. For example, it was recently found that an Android app claiming to be a two-factor authenticator was also used to deliver malware designed to steal sensitive financial data from the user.[2]

The goal of App Review is to ensure that apps on the App Store are trustworthy and that the information provided on an app's App Store page accurately represents how the app works and what data it will access. This process creates a high barrier against the most common scams used to distribute malware: misrepresenting the malware as a popular app, or claiming to offer enticing features that are not actually provided. This is why the manual review of apps by

---

[1] https://securelist.com/mobile-malware-evolution-2020/101029/

[2] https://arstechnica.com/information-technology/2022/01/2fa-app-with-10000-google-play-downloads-loaded-well-known-banking-trojan/

professionals during the App Store's App Review process has played such an important role in iOS's success against malware.

Mr. Schneier is correct that "sophisticated malware," often used by state-sponsored attackers, can bypass device security controls. But on iPhone, such sophisticated malware is highly complex, costs millions of dollars to develop, and often has a short shelf life. While Apple works hard to protect users from every threat, including this type of malware, the vast majority of users will never be targeted by such attacks. To focus the discussion on this rare threat misses what is actually harming millions of users every day on other mobile platforms: social engineering attacks, a threat that the Apple App Store has been incredibly effective at suppressing.

Following the security model pioneered by iOS, most modern computing platforms have shifted their strategy towards providing secure default policies, and asking the user to provide explicit consent before an app is granted access to sensitive data. However, for this model to be effective, the user must be able to trust that the app is what it claims to be, and that it truly originates from the stated developer. Apple's App Store review and distribution model is designed specifically to address this concern.

As RiskIQ puts it, "[t]hreat actors [on other platforms] have made a living [...] produc[ing] 'rogue apps' that mimic well-known brands or otherwise purport to be something they're not, purpose-built to fool customers into downloading them."[3]

As an example, the Goontact spyware relies on malicious operators who convince users to sideload a well-known chat app, such as Telegram, from a website that mimics the design of a first-party app store. The malware operators guide unsuspecting targets through this process, and convince them to grant the app various access privileges. The experience appears indistinguishable from a legitimate app download, so users are generally compliant: they believe they are conferring privileges to an app they recognize and use. But the website on which they were instructed to download the app is fake, as is the app itself.

Device-based security controls are ineffective against this threat. The only opportunity to protect the user occurs *before they are tricked* to download this fake app in the first place. The Apple App Store is not perfect, but it has been very successful at providing this protection.

[3] RiskIQ p.2

Most meaningful privacy and security innovations require policy enforcement, which cannot be solely implemented through device-based controls.

Pro-consumer programs like Apple's App Tracking Transparency and Privacy Nutrition Labels cannot be achieved on the device alone—that is to say, with controls that would remain effective even absent App Store distribution. When it comes to tracking, there are innumerable ways for apps to track users and devices that device-based controls cannot stop: some examples are tracking via IP address, email address, third-party single sign-on, or device fingerprinting. When Apple announced App Tracking Transparency, advertising technology companies were openly discussing[4] all of these mechanisms as a way to bypass the tracking transparency measure Apple intended to provide its users. And indeed, had App Tracking Transparency been implemented through device controls alone, users would have had no recourse. But the App Store allowed Apple to clarify *by policy* that the tracking prohibition applied to all methods of tracking, not just a single identifier like the Identifier for Advertisers (IDFA).

The centralized distribution model of the App Store provides a clear deterrent – the prevention of future distribution – for apps that would seek ever more inventive ways of skirting or bypassing device controls. Other Apple transparency innovations like Privacy Nutrition Labels cannot be enforced on the device at all; absent the App Store, there would be no mechanism to compel apps to provide this information to users, and to hold them accountable should they misrepresent it. Apple firmly believes that overcoming most key security and privacy challenges that our users will face in the future requires a combination of industry-leading device-based controls *and* policy controls stemming from trusted, centralized App Store distribution.

Successful device-based privacy and security controls often require distinguishing between the platform vendor and third party apps.

Mr. Schneier states that any future device-based privacy and security controls should be applied "fairly to the platform's own products and services as well as to third parties." We agree, which is why we have worked to make sure that Apple apps ask for user consent to access sensitive data when appropriate, just like third-party apps. When a user first opens Apple's Camera app on iOS, for example, they are asked if they wish to provide it with location access so that the app may record with each photo where it was taken. This is the same location prompt that applies to third party apps. But preserving device security and privacy requires that "fair access" for third parties not be mistaken for "identical

---

[4] *See* https://www.adexchanger.com/mobile/apples-policy-is-clear-email-is-not-gonna-take-the-place-of-idfa/ *and* https://www.cpomagazine.com/data-privacy/apple-begins-enforcing-new-privacy-rules-rejects-apps-using-known-device-fingerprinting-techniques/

access". As the device manufacturer and the operating system provider, some Apple software necessarily has access to specific, low-level capabilities that, if opened to third parties, would create disproportionate security or privacy risks that are certain to lead to user harm.

For example, Apple prohibits third-party apps – and nearly all of our own apps and services too – from accessing the whole storage volume of a user device. This is because many types of malware, and in particular ransomware, rely on wide access to device storage in order to effectively attack the user. And if the user were asked to make a decision about this level of access, they could readily be tricked – for example, by an app that presents itself (outside of the App Store) as a trusted storage app, and asks for full storage access in connection with some purported incentive ("free device backup for life if you act immediately!"). We mitigate this risk by strictly limiting full access to device storage and other extremely sensitive, low-level capabilities. As a result, iOS is the only computing platform today where ransomware effectively doesn't exist.

Third-party app stores are a well-established malware problem on other platforms.

S. 2710 would require Apple to provide users with a readily accessible means to "install third-party apps or app stores" outside of Apple's App Store. Mr. Schneier offers a very generous reading of this language, suggesting that Apple could perhaps limit any installation of third-party apps to app stores that have the same or even more security restrictions than Apple. It is far from clear that the legislation would permit this restrictive approach to sideloading, and the bill's narrowly drawn affirmative defenses may well preclude such an outcome. At a minimum, Apple would almost certainly be forced to defend itself in litigation brought by those seeking to reach users without going through any app store at all.

Mr. Schneier's argument also ignores the well-established record of third-party app stores when it comes to security. There is ample evidence showing third-party app stores are a key malware vector on platforms which support such stores. In the Android ecosystem, which has 50 times more malware than iOS[5], Nokia found that "the fact that Android applications can be downloaded from just about anywhere still represents a huge problem, as users are free to download apps from third-party app stores, where many of the applications, while functional, are Trojanized."[6]

---

[5] Nokia Threat Intelligence Report 2021, p.8 https://pages.nokia.com/T006US-Threat-Intelligence-Report-2021.html

[6] Nokia Threat Intelligence Report 2020, p.8 https://onestore.nokia.com/asset/f/210088

According to PurpleSec, "Third-party app stores host 99.9% of discovered mobile malware."[7] And in markets where third-party app stores exist, there is a race to the bottom when it comes to security and privacy. Crowdstrike finds that "[t]he majority of mobile malware is distributed from third-party sources that do not perform comprehensive checks of applications they provide."[8]

RiskIQ found in 2020 that "hundreds of less reputable app stores represent a murky mobile underworld outside of the relative safety of reputed stores. Apps in these stores are far less regulated than official app stores, and some are so overrun with malicious apps that they outnumber their safe offerings."[9] Similarly, Trend Micro found that "[t]he most common infection vector is downloading ransomware-infected apps from third party app stores."[10]

These warnings do not just come from the private sector. The European Union Agency for Cybersecurity cautions users to: "Use the official application marketplace only. Users should ... not [download applications] from third-party sources, to minimise the risk of installing a malicious application." In the United States, the Department of Homeland Security issued an even starker warning: "Additionally, users should avoid (and enterprises should prohibit on their devices) sideloading of apps and the use of unauthorized app stores."

No company has figured out how to sideload apps safely.

Mr. Schneier states that sideloading can be *"implemented in a way that ensures users are aware of the risks they take on before installing a piece of unverified software,"* and that *"[u]sers who do not want to side-load apps can easily choose not to."* This contradicts significant expert consensus in the field, and is in effect advocating that mobile device users be left to fend for themselves.

Users may feel obliged to download a specific chat or social media app from a third party store to communicate with friends or family members, or to download a venue-specific app from a third party store to gain entry to a wedding or a concert. Users may even be required to download apps from third-party stores by institutions that do not have the resources and expertise to ensure their security and privacy.

---

[7] PurpleSec 2021 Cyber Security Statistics, https://purplesec.us/resources/cyber-security-statistics/

[8] Crowdstrike 2019 Mobile Threat Landscape Report, p. 30

[9] RiskIQ 2020 Mobile App Threat Landscape Report, p.3 https://www.riskiq.com/wp-content/uploads/2021/01/RiskIQ-2020-Mobile-App-Threat-Landscape-Report.pdf

[10] Mobile Ransomware: Prevention and Best practice https://success.trendmicro.com/solution/1114298-mobile-ransomware-prevention-and-best-practice

A study by the Center for Cybersecurity Policy and Law that drew on prior research and multi-stakeholder focus groups of cybersecurity experts found the exact opposite of what Mr. Schneier asserts in his letter: "Given the extent and complexity of the risk, expecting end users to have the requisite understanding of security and privacy and how to protect themselves via layered on security, esoteric, or hard-to-find settings, and other methods simply isn't viable at scale."[11]

Indeed, one expert years ago highlighted the limits of security warnings alone to safeguard computer systems:

> Despite researchers' good intentions, [security] warnings just inure people to them. I've read dozens of studies about how to get people to pay attention to security warnings. We can tweak their wording, highlight them in red, and jiggle them on the screen, but nothing works because users know the warnings are invariably meaningless. They don't see 'the certificate has expired; are you sure you want to go to this webpage?' They see, 'I'm an annoying message preventing you from reading a webpage. Click here to get rid of me.'[12]

The expert who said this is Mr. Schneier.

We must not allow the technology industry to become inured to the immense impact of cyberthreats on our society.

Mr. Schneier suggests that personal computers should be seen as a gold standard for device security, presenting a choice where *"[w]e can run our computers securely, or we can choose not to."* Unfortunately, his suggestion both ignores the substantial difference in success against malware between iOS and all other computing devices that rely on this "choice," and significantly understates the increasingly dangerous cybersecurity landscape. The National Security Agency, in its 2021 Year in Review, summarizes plainly: "Cyber threats to our nation rose to national consciousness this past year. We felt the real-world consequences that malicious cyber actors can inflict from cyberspace. We saw how malicious cyber actors will infiltrate global supply chains as well as exploit popular applications for ransomware. We even saw how ransomware attacks can restrict our travel and affect our food supply chain. It hit home that cybersecurity is national security. Our adversaries and cyber criminals continue to push limits in cyberspace, creating more national security threats than we have ever seen."

---

[11] Mobile Future: Pathways to Continued Improvement in Mobile Security and Privacy, Center for Cybersecurity Policy and Law, p.8 https://centerforcybersecuritypolicy.org/s/Mobile-Future-Pathways-to-Security-and-Privacy.pdf

[12] https://www.schneier.com/blog/archives/2016/10/security_design.html

Forty years into consumer computing, iOS stands out because there has never been a widespread, consumer malware attack on the platform. For a consumer computing platform of over a billion devices that is truly remarkable, and it's no accident. We built the iPhone never to share the PC's malware-plagued fate, and we have invested more than 15 years of cutting-edge security engineering to constantly evolve our protections and stay ahead of the threats our customers face.

In Nokia's 2021 threat intelligence report, Android devices made up 50.31% of all infected devices, followed by Windows devices at 23.1%, and macOS devices at 9.2%. iOS devices made up a percentage so small as to not even be singled out, being instead bucketed into "other". We consider this a triumph in protecting our users, and it could never have been done without the industry-leading last line of defense of our device security controls, working in tandem with the front-line security and privacy protections we provide our users through the App Store and App Review.[13]

Mr. Schneier closes his letter by suggesting that "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."

Mr. Schneier's attempted analogy misses the mark. We would be hard-pressed to more clearly articulate the argument *for* Apple's approach to security and privacy. Apple devices comprise only a fraction of mobile devices worldwide. Apple *does not* seek to "outlaw" other platforms and operating systems, nor to have a monopoly on dictating the security of all mobile devices. Users who dislike our approach are free to seek out the approaches of other companies. We wish only to preserve the freedom for users to choose their own level of risk.

We hope Congress will preserve consumers' ability to chose the safest option for themselves and their families.

Sincerely,

Timothy Powderly
Senior Director of Government Affairs, Americas
Apple, Inc.

---

[13] Nokia Threat Intelligence Report 2021, p.8 https://pages.nokia.com/T006US-Threat-Intelligence-Report-2021.html