January 18, 2022

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

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

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

Senator 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

This week, the Senate Judiciary Committee is expected to consider S. 2992, the American Innovation and Choice Online Act, and it may soon consider S. 2710, the Open App Markets Act. Apple has appreciated the opportunity to engage with the Committee on these bills, but we remain concerned that they will hurt competition and discourage innovation.

Apple's App Store has been an incredible engine for economic growth and innovation since its founding in 2008. The App Store is a safe and trusted marketplace for our users and foundational to the iPhone experience they love. It has also been an economic miracle for developers, giving every single developer the same opportunity to reach App Store customers in 175 countries, across 40 languages. In 2020, the App Store ecosystem — more than 90 percent of which pays no commission to Apple — facilitated $643 billion in billings and sales, including $175 billion in the U.S. alone. In addition, the App Store supports more than 2.1 million U.S. jobs across all 50 states.

Apple
One Apple Park Way
Cupertino, CA 95014

T 408 996-1010
F 408 996-0275

The purpose of this letter, however, is to underscore the most serious issue with these bills: the real harm they will do to American consumers' privacy and security.

After a tumultuous year that witnessed multiple controversies regarding social media, whistleblower allegations of long-ignored risks to children, and ransomware attacks that hobbled critical infrastructure, it would be ironic if Congress responds by making it much harder to protect the privacy and security of Americans' personal devices. Unfortunately, that is what these bills would do.

These bills will reward those who have been irresponsible with users' data and empower bad actors who would target consumers with malware, ransomware, and scams.

The most glaring problem with these bills is the risk they pose to the privacy and security of Americans' personal devices. Today, our smart phones are not just phones; they store some of our most sensitive information about our personal and professional lives. We keep them with us wherever we go, and we use them to call and text with loved ones, take and store photos of our children, give us directions when we're lost, count our steps, send money to friends, and so much more.

While both bills ostensibly permit privacy and security protections, they erect very steep obstacles for such safeguards. Specifically, to introduce new and enhanced privacy or security protections under the bills, Apple would have to prove the protections were "necessary," "narrowly tailored," and that no less restrictive protections were available. This is a nearly insurmountable test, especially when applied after-the-fact as an affirmative defense. And it essentially could lead to a lowest common denominator problem in which consumers will no longer have the choice to purchase a smart mobile device that provides them with the highest-level of security and privacy protection.

The bills put consumers in harm's way because of the real risk of privacy and security breaches. In addition to making privacy and security protections nearly impossible to defend, the bills would actually allow predators and scammers to sidestep Apple's privacy and security protections completely. This circumvention is possible because the bills would mandate "sideloading," or the direct installation of software from the internet in a way that circumvents the privacy and security protections Apple has designed, including human review of every app and every app update.

Some mobile operating systems allow users to download unvetted software from the internet. The iPhone's operating system (iOS) is different. Apple offers consumers the choice of a platform protected from malicious and dangerous code. The bills eliminate that choice.

The App Store provides for a central distribution of apps. This design builds on the lessons we learned during the PC-era to offer a more secure and privacy-focused ecosystem to our customers. Through a combination of advanced technology and human review, the App Store is dramatically more secure than systems offering non-centralized, open distribution, including our own MacOS. In fact, iOS has almost 98% less malware than Android. As shown by independent, third-party security analyses—like the Nokia 2021 Threat Intelligence Report—forcing iPhones to allow sideloading could lead to hundreds of thousands of additional mobile malware infections per month.

Apple's recently-released App Tracking Transparency (ATT) program provides an illustrative example of the bills' flaws. ATT is a new feature of the App Store that lets individuals decide whether to allow apps to track their activities across other companies' apps and websites.

The response to ATT from consumers has been overwhelmingly positive, but some of the largest social media and advertising companies have very publicly complained about the impact of these new privacy protections on their profits.

Under the pending bills, this pro-consumer program would be in jeopardy, as it would be extremely challenging to prove that ATT is "necessary," "narrowly tailored," and that no less restrictive protections are available to obtain user consent for tracking. Conversely, companies that collect data would argue that the mechanism currently used to obtain user consent for tracking—a line buried in their terms of service—is sufficient.

Accordingly, Apple supports a more sensible and achievable standard for privacy and security protections—requiring that they be non-pretextual and reasonably tailored to protect consumers. Fortunately, S.2992 and its House companion already use a "reasonably tailored" test for actions taken to protect copyright holders, and making such a change for privacy and security measures would give Apple a fighting chance to protect its consumers.

Regrettably, even if the bills' test for privacy protections is fixed, the bills would still allow apps to circumvent most protections altogether. That's because ATT and similar protections are built into the App Store's terms of service. Yet, as noted above, the bills' sideloading mandate means that apps need not comply with the App Store's requirement that companies honor consumers' decisions not to be tracked—a big loss for consumers, and a big win for those who would profit by collecting even more personal information.

This sideloading threat is even greater when it comes to malicious actors. Some have dismissed this risk, pointing to competing platforms that permit sideloading

and arguing that the "sky has not fallen." But, if Apple is forced to enable sideloading, millions of Americans will likely suffer malware attacks on their phones that would otherwise have been stopped.

This increased risk is not primarily because consumers will *knowingly* choose to accept the risk and download questionable apps; it is because, without a centralized vetting mechanism like the App Store, many consumers will be deceived into installing unwanted malicious software on their devices. This is why cybersecurity experts, including those at the Department of Homeland Security and other government agencies, routinely recommend prohibiting sideloading as a best practice. Accordingly, the bills should be modified to reduce or eliminate the threat of sideloaded malware, rather than increasing this risk as they do now.

Apple agrees that assessing regulatory frameworks in the tech sector is the right thing to do. Without careful consideration, however, efforts to address broader concerns via competition policy could undermine the very consumer benefits—especially consumer privacy and security—we are all striving to protect and enhance. Apple supports efforts to craft comprehensive federal legislation to protect consumer privacy and security. And we believe lawmakers should prioritize passing legislation that addresses the most pressing challenges confronting consumers, including business practices that exploit consumers' data.

The bills should put consumers' welfare first.

The bills should be modified to strengthen—not weaken—consumer welfare, especially with regard to consumer protection in the areas of privacy and security. At a minimum, we recommend the Senate Judiciary Committee adopt language like that approved by the House Judiciary Committee during its markup of companion legislation, which added an affirmative defense for conduct that "increases consumer welfare."

In the iPhone, Apple created a product that consumers *love and depend on*—not merely as a means of communication, but because it provides them with first-in-class, baked-in privacy and security protections that safeguard their welfare. Every day, consumers benefit from Apple's development, curation and management of the App Store, knowing that they can safely download apps that will enhance their productivity or enrich their lives without threatening the integrity of their phone or putting their most personal data out to market (or worse).

Government regulators should not ignore the benefits consumers receive from Apple, including protection from online predators and scammers. In 2020 alone, Apple protected users from more than $1.5 billion in potentially fraudulent transactions. Every day, our team blocks apps that are incomplete or misleading, collect more user data than they need, or otherwise try to trick unsuspecting users. Our

efforts are not perfect, but they provide significant consumer benefits. And this security is also a boon to competition. Our rigorous app review guidelines create a secure space for users to explore nearly 1.8 million apps, with more than 100,000 new submissions each week.

Because consumers have come to trust and rely on Apple's App Store for this protection, software developers *also* receive an extraordinary benefit: they don't have to worry about whether the iOS users they want to become customers will trust them enough to download their apps. Because Apple has built an inherently trustworthy and protected marketplace, consumers freely download whatever apps are in the store based solely on whether they think they will be useful or fun. That's good for consumers and it's *great* for developers.

To be clear, we believe these bills have other serious problems. Among other things, the bills would undo much of the progress Congress has made bolstering American competitiveness, rebuilding supply chains, and encouraging domestic manufacturing by instead codifying a structural advantage for foreign competitors in the vibrant technology sector. At the same time, we acknowledge that these bills include some improvements over their House counterparts. Apple especially appreciates Section 2(c)(1) of S. 2992, which helps ensure that the bill's operative provisions will not be construed to force Apple to give up any of its intellectual property (language that should be added to S. 2710).

As highlighted above, however, the bills' threat to consumer privacy and security—along with their failure to address the harms to our social fabric highlighted by multiple congressional hearings over the last year—are major shortcomings that must be corrected to avoid doing real harm. At the launch of iPhone in 2007, Steve Jobs said that "*we're trying to do two diametrically opposed things at once: provide an advanced and open platform to developers while at the same time protect iPhone users from viruses, malware, privacy attacks, etc. This is no easy task*."

Accordingly, we urge the Committee not to approve S. 2992 or S. 2710 in their current form, and we request the opportunity to continue working with the Committee to find workable solutions to address competition concerns while protecting consumers' privacy and security going forward.

Sincerely,

Timothy Powderly
Senior Director, Government Affairs, Americas
Apple