January 19, 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

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

The Electronic Frontier Foundation (EFF) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, cybersecurity, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. With over 38,000 dues-paying members and well over 1 million followers on social networks, we focus on policies that benefit both creators and users.

For decades the EFF has focused on empowering technology users to control their own devices while protecting privacy and security. We use software development, impact litigation, and grassroots activism to empower the public. For example, EFF is a leader in encrypting the web through "Let's Encrypt," which has issued hundreds of millions of certificates to secure internet user traffic. EFF also helps human rights activists find ways to operate in authoritarian countries around the world while securing their communications,[1] as well as victims of domestic abuse who suffer from stalkerware.[2] In fact, EFF's work in securing user privacy has at times made it the target of state actors such as Russia,[3] which temporarily spoofed EFF's website in an attempt to exploit trust placed in our organization's privacy and security work.

Our commitment to security and privacy underpins all our work. EFF makes no exceptions to user privacy and security in its competition and antitrust work and we urge the Senate Judiciary Committee to move forward with its competition bills S. 2992 (American Innovation and Choice Online Act) and S. 2710 (Open App Markets Act).

Arguments are being made on the false pretense that monopolistic control is an essential component to ensuring user security. Apple in particular is attempting to confuse the Committee by conflating its anticompetitive App Store rules with best practices for protecting users.

---

[1] SURVEILLANCE SELF-DEFENSE, available at https://ssd.eff.org/en.

[2] COALITION AGAINST STALKERWARE; available at https://stopstalkerware.org.

[3] Brandon Stosh, *Russian Hackers Caught Spoofing EFF Site to Serve Espionage Malware for 3+ weeks*, FREEDOMHACKER (Aug. 30, 2015), available at https://freedomhacker.net/russian-hackers-spoof-eff-site-serve-espionage-malware-3-weeks-4584.

Nothing can be further from the truth. In fact, user's security has at times been hindered due to the restrictive rules Apple imposes on app developers. For example, in 2020, Apple prevented Basecamp's new paid email service HEY from making important security fixes, alleging violations of App Store rules.[4] The "violation" was that HEY developers did not route users' subscription payments through Apple to ensure that Apple received a 30% cut. Apple threatened HEY that until changes were made, the security updates would be blocked. This was despite HEY following the same payment pathway that Netflix and Amazon have always used. Following a public pressure campaign and negative press, Apple relented and allowed the security fixes to proceed, but other app innovators face the same threat.

Examples of Apple's total control over the App Store hindering user security efforts does not stop there. Apple has blocked applications that enhance user privacy and security beyond what Apple itself can deliver. This includes applications that scan your phone to detect whether it has been hacked,[5] and parental control applications that limited screen time and access to certain applications and adult content.[6]

Lastly, Apple makes references that its new "App Tracking Transparency" feature is welcomed by users because it prevents tracking of users without their consent. This would indeed be a positive step, but research by the Financial Times has found that Apple's favored partners such as Facebook and Snap are still collecting data that can identify users across different aps, even if those users have not opted in—and Apple is aware of this.[7]

The Committee must recognize the arguments Apple is making against addressing the control it exerts over app developers as self-serving and merely an attempt to maintain its anticompetitive and harmful policies. Much like the AT&T monopoly of the 1960s that asserted that any third-party technologies attached to the phone network would be harmful, Apple is claiming that only Apple can vet applications for privacy and security. Our country rejected these paternalistic arguments in the past and should do so today. The bills explicitly allow Apple to take action to protect security and privacy of its users, while putting an end to anticompetitive conduct.

Nothing in these bills prevents Apple or Google from vetting apps for their phones for privacy and security. Nor does it prevent those giants from instituting privacy and security protective futures. What these bills do is prevent companies from making all of these decisions for users. It also allows apps to compete with large companies without being forced to pay a rent to those same companies.

---

[4] Rainey Reitman, *Apple's Response to HEY Showcases What's Most Broken About the Apple App Store*, Deeplinks Blog (Jun. 22, 2020), *available at* https://www.eff.org/sh/deeplinks/2020/06/apples-response-hey-showcases-whats-most-broken-about-apple-app-store.

[5] Andy Boxall, *Apple Has Pulled an App That Told You if Your iPhone was Hacked*, DIGITALTRENDS, (May 16, 2016), available at https://www.digitaltrends.com/mobile/system-and-security-info-iphone-app-news.

[6] Jack Nicas, *Apple Cracks Down on Apps That Fight iPhone Addiction*, NY TIMES (Apr. 27, 2019), available at https://www.nytimes.com/2019/04/27/technology/apple-screen-time-trackers.html.

[7] Chance Miller, *Report: Snap and Facebook use App Tracking Transparency Loophole to Continue Sharing 'aggregated' user data*, 9TO5MAC (Dec. 8, 2021), available at https://9to5mac.com/2021/12/08/snapchat-facebook-data-sharing-app-tracking-transparency.

Market consolidation has centralized and limited the internet's potential to be a source of innovation, growth, and freedom. Apple's fearmongering about competition policy preventing it from addressing security is disingenuous, because monopoly control over app distribution is simply not necessary to protect users. In fact, it makes users less secure. Competition will reinvigorate the strengths that come from the promise of the internet as an open forum for all ideas where no gatekeeper has the power to dictate our collective future. Today's monopolists have acquired an unassailable position of power that must be remedied with law. Congress has the power to chart a new course, as it has in the past, and reshape the market towards a more competitive future. We urge the Committee to deliver that future.

Sincerely,

Electronic Frontier Foundation