March 28, 2022

U.S. Senate
Washington, DC 20510

U.S. House of Representatives
Washington, DC 20515

Dear Members of Congress,

As the eyes of policymakers around the world turn to addressing concerns in the app economy, dominant mobile platforms continue to falsely claim that any legislative or regulatory effort to create a more competitive, innovative, and open mobile app marketplace would harm privacy and security for developers and consumers. As cybersecurity experts, security professionals, former government officials and advisers, and advocates with decades of experience in these fields, we write to correct the record.

Enacting policies to provide developers and consumers greater freedom and choice will neither reduce security on mobile devices nor increase harm to users. In fact, we believe that competition and accountability will incentivize platforms, payment processors, and app developers to better prioritize security. Lawmakers should therefore consider proposals such as the Open App Markets Act based on the merits of the legislation, not scare tactics or false choices. Given the evidence, it is clear that not only would this legislation advance competition and choice in the digital marketplace, but it would improve security for consumers.

Greater Competition in App Distribution and Payment Processing Improves Security

Apple argues against measures to increase competition in the app marketplace in part by claiming that its app review process protects users from malware and spam. However, security on iOS devices such as iPhones and iPads is provided by the devices themselves rather than the App Store Review process. These devices contain numerous built-in hardware security measures including data encryption, firewalls, antivirus protections, and a 'sandbox' model that limits apps' access to the phone's resources.[1]

Apple's arguments that opening iOS to third-party app stores or allowing alternative payment processing systems would expose iOS to malware are unfounded. In reality, opening the App Store would allow iOS to operate just like another Apple product – the Mac. Mac desktop and laptop computers allow consumers to download and install software outside of the App Store, directly from browsers, and tout the security and safety of the Mac operating system.

Apple also argues against allowing alternatives to its payment platform, Apple Pay, for in-app purchases by alleging that it creates a potential security risk. Once again, Apple's argument is undermined by its

own practices: Apple allows select companies such as Amazon, Uber, and Airbnb to direct consumers to third-party payment processors.[2] However, the company fails to explain why payment alternatives on some apps would pose security risks but are acceptable on others. Further, there is reason to believe that competition in this space would actually *enhance* security. Payment processing companies would not be in business if their services were not safe and secure. Competition would offer developers choices for their apps and drive these payment processors to provide the best customer experience, including security, at the lowest cost.

Existing Security Flaws Plague Dominant App Store Platforms

Apple and Google argue their app marketplaces are tightly controlled and must remain so to protect developers and consumers, yet they ignore the reality that their existing platforms are filled with security flaws. Recent reports found 204 scam apps in the App Store had been downloaded more than one billion times from the App Store and Google Play, adding up to $365 million in revenue.[3] It is easy for scammers to circumvent Apple's rules: Nearly 100,000 submissions for apps are sent to Apple each week, and reviewers spend just 15 minutes reviewing the software.[4] Scam app developers can easily skirt app reviews by submitting seemingly innocuous apps for approval and then transforming them into phishing apps that trick people into providing their information – all before Apple even notices there is a problem.[5]

Take for example the success of the word game, Wordle, which has skyrocketed in popularity in recent months. The explosion of interest in the app has inspired multiple clone apps, which made it past Apple's review process, allowing scam applications to be installed on user devices. Many of these apps charged high monthly subscription fees to users and were only removed following reporting from major media outlets.[6]

Apple's claims of strong protections also likely hurt user security by giving app users a false sense of confidence when installing apps from the App Store. Competition in app distribution would encourage Apple and all other app stores to provide the best user experience and prevent the proliferation of malware and scams on mobile devices.

Self-Preferencing Behaviors Undermine App and Consumer Security

While dominant platforms argue they must maintain complete control of their app stores to protect security, their anti-competitive practices, self-preferencing behaviors, and misaligned incentives run directly counter to improving the security of apps in their marketplaces.

In seeking to stop Basecamp's email app, Hey, from using alternative payment systems, Apple prevented Basecamp from making critical bug fixes. It is clear Apple rejected these changes to ensure it continued to receive the 30 percent commission it collects from in-app purchases in the Hey app. To reject a fix that would have improved usability and protection for consumers for the purpose of generating more revenue

for itself clearly demonstrates how digital gatekeepers are incentivized to prioritize their profits over better products and consumer security.

In June 2018, Apple announced Screen Time, a tool to help users monitor time on their devices and parents track and limit their children's mobile activity, as a default feature. Following the release, Apple removed or restricted the functionality of 11 of the 17 most downloaded screen time or parental control apps. Despite no issues with these apps prior to the release of their own product, Apple used the guise of user security and protection to squash competitors offering competing products that would help consumers. Apple clearly chose revenue over products families relied on to keep their families safe and healthy.[7]

Lawmakers should recognize and reject the inaccurate claims of security and privacy made by dominant mobile platforms, made as a pretext to maintain top-down control of the app marketplace on their respective platforms. As Congress works to design effective policies that foster innovation and improve consumer choice in the digital economy, we urge you to embrace the proven role of competition in benefiting users and security.

Sincerely,

Governor Tom Ridge
First United States Secretary for Homeland Security
Former Governor of Pennsylvania

Secretary Janet Napolitano
Former Secretary of Homeland Security
Former Attorney General and Governor of Arizona

Pat Meehan,
Former Chair of House Homeland Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

Steve Kohler
President of Ridge Global
Former president of Winner Global Defense

Amanda Gorton
CEO and Co-Founder of Corellium