

July 21, 2026

The Honorable Gus Bilirakis
Chair
Subcommittee on Commerce, Manufacturing,
and Trade
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Commerce, Manufacturing,
and Trade
U.S. House of Representatives
2323 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Bilirakis, Ranking Member Schakowsky, and Members of the Subcommittee,

We, the undersigned coalition of public policy groups, think tanks, and nonprofits, write to urge you to reject H. R. 3209, the App Store Freedom Act (ASFA), a bill that would require covered operating systems to permit apps to be downloaded from third-party sources, a process known as sideloading.¹ The Subcommittee will consider this bill on Wednesday, July 22.² Although it is a well-intentioned measure to promote competition, the bill would in practice have the opposite effect—and endanger the cybersecurity of millions of Americans.

The ASFA's fundamental flaw is its requirement that certain mobile operating systems permit sideloading and third-party app stores. These provisions would weaken one of the most important security features of modern smartphones. Today, trusted app marketplaces such as Apple's App Store and Google Play invest enormous resources in reviewing applications, detecting malware, preventing fraud, and removing malicious software before it reaches consumers. Their security teams continually monitor for emerging threats, respond to newly discovered vulnerabilities, and protect users from increasingly sophisticated cybercriminals. Data shows that devices that prevent sideloading altogether fall victim to cybersecurity issues at far lower rates than those with more lax standards.³

In a recent news release, Apple said it “evaluated more than 9.1 million app submissions [in 2025], helping to welcome over 306,000 new developers to the platform. In addition, the team rejected over 2 million app submissions—including over 1.2 million new apps and nearly 800,000 app updates—for failing to adhere to the App Review Guidelines.”⁴ Moreover, “Apple terminated 193,000 developer accounts over fraud concerns and rejected more than 138,000 developer enrollments.” Also in 2025, Google “prevented over 1.75 million policy-violating apps from being published on Google Play and banned more than 80,000 bad developer accounts that attempted to publish harmful apps” (emphasis removed).⁵ These examples are just a part of the work done by these app stores to keep their users safe (more information can be found in the companies' publications cited above). The work of combating malicious or otherwise problematic software is far beyond the technological expertise of the median

¹ <https://www.congress.gov/bill/119th-congress/house-bill/3209/text>

² <https://energycommerce.house.gov/posts/chairmen-guthrie-and-bilirakis-announce-hearing-on-legislation-to-strengthen-consumer-product-and-service-protections>

³ <https://appsecurityproject.org/issues/mandated-sideloading-will-weaken-the-app-ecosystem-and-compromise-existing-privacy-protections/>

⁴ <https://www.apple.com/newsroom/2026/05/the-app-store-stopped-over-2-point-2-billion-usd-in-fraudulent-transactions-in-2025/>

⁵ <https://blog.google/security/keeping-google-play-android-app-ecosystem-safe-2025/>

American user. Yet, by propping up third-party marketplaces, the legislation would expose users to less rigorous or outright negligent app stores and the potentially dangerous apps they purvey.

The dangers of sideloading are known and significant. In Europe, where the Digital Markets Act (DMA) mandated sideloading, government officials in the wake of the mandate quickly “reached out to [Apple] about these new changes, seeking assurances that they will have the ability to prevent government employees from sideloading apps onto government-purchased iPhones.”⁶ In the digital age, cybersecurity is a critical element of security generally—for governments, businesses, and individual users. Governments should not prevent users from accessing the cybersecurity features now commonly available on the market when they themselves find such features essential.

The ASFA will be considered alongside bills to prevent fraudulent schemes and scams, putting the bill at odds with the rest of the Subcommittee’s agenda. Weakening protections against malicious software will only worsen the problem that anti-fraud and anti-scam legislation seeks to solve. It is one thing to say that the bill will “hold Big Tech accountable and promote competition,”⁷ but it is quite another when the cost will likely be paid—literally—by Americans who, as a result of the ASFA’s policies, would lose their hard-earned money to fraudsters and scammers.

This legislation rests on a fundamental contradiction. Its proponents argue that it is intended to increase competition by preventing certain app store policies, yet the bill excludes an entire category of competitors—i.e., those that wish to ban sideloading altogether—from the marketplace. Such companies compete by offering a more secure operating system that restricts sideloading, which, for consumers who want maximal security, can be a selling point. In short, security itself is a competitive feature.

Moreover, the bill would reduce consumer choice, not expand it. Consumers who prefer devices that permit sideloading already have options in the marketplace. Users who want these devices can obtain and use them. The ASFA would simply prevent users who seek a higher degree of security from taking advantage of such features.

In a word, the ASFA’s policies can only be described as European, not American. In recent years, European legislation such as the DMA has drawn increasing scrutiny from American policymakers because of its deeply harmful effects on American innovators and, at times, American users. European-style regulation has rightly been criticized when implemented abroad; it should be opposed when proposed in Washington, D.C.

For these reasons, we respectfully urge you to oppose the App Store Freedom Act.

Sincerely,

David Williams

President

Taxpayers Protection Alliance

Brandon Arnold

Executive Vice President

National Taxpayers Union

⁶ https://appsecurityproject.org/news_post/how-the-dma-will-hurt-consumer-choice/

⁷ <https://cammack.house.gov/media/press-releases/rep-cammack-introduces-app-store-freedom-act-promote-competition-protect>

Daniel Castro

President

Information Technology and Innovation Foundation

James Czerniawski

Head of Emerging Technology Policy

Consumer Choice Center

Jon Decker

Executive Director

American Commitment

Ryan Ellis

President

Center for a Free Economy

James Erwin

Executive Director

Digital Liberty

Daniel J. Erspamer

Chief Executive Officer

Pelican Institute for Public Policy

Kristian Fors

Technology and Innovation Policy Analyst

Libertas Institute

Tom Giovanetti

President

Institute for Policy Innovation

Vance Ginn, Ph.D.

President

Ginn Economic Consulting

Jessica Melugin

Director, Center for Technology and Innovation

Competitive Enterprise Institute

Chuck Muth

President

Citizen Outreach

Grover Norquist

President

Americans for Tax Reform

Kevin Riffe

Chairman

West Virginia Center-Right Coalition

John Tamny

Founder and President

Parkview Institute

Josh Withrow

Fellow, Tech & Innovation Policy

R Street Institute