July 20, 2026

The Honorable Brett Guthrie
Chairman
U.S. House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, District of Columbia 20515

The Honorable Frank Pallone
Ranking Member
U.S. House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, District of Columbia 20515

The Honorable Gus Bilirakis
Chairman
U.S. House Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade
2125 Rayburn House Office Building
Washington, District of Columbia 20515

The Honorable Jan Schakowsky
Ranking Member
U.S. House Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade
2125 Rayburn House Office Building
Washington, District of Columbia 20515

RE: ***Legislative Proposals to Strengthen Consumer Protection in a Changing Marketplace***

Dear Chairman Guthrie, Ranking Member Pallone, Chairman Bilirakis, Ranking Member Schakowsky, and Members of the Committee:

Thank you for the opportunity to submit testimony for the record on your hearing titled, *Legislative Proposals to Strengthen Consumer Protection in a Changing Marketplace*.[1]

The Association for Competitive Technology (ACT) represents small business innovators and startups in the software development and high-tech space in the United States and around the world. As the world embraces mobile technologies, our members create the innovative products and services that drive the global digital economy by improving workplace productivity, accelerating academic achievement, and helping consumers lead healthier lives. Today, the

[1] *Chairmen Guthrie and Bilirakis Announce Hearing on Legislation to Strengthen Consumer Product and Service Protections*, energycommerce.house.gov/posts/chairmen-guthrie-and-bilirakis-announce-hearing-on-legislation-to-strengthen-consumer-product-and-service-protections. Accessed 17 July 2026.

global app economy is worth more than $1.8 trillion and supports over 6.1 million American jobs.[2]

Among the bills before the Committee today, the App Store Freedom Act (ASFA) warrants particular concern because of its potential to significantly reshape the digital marketplace.[3] Under the bill, covered companies would be required to take several steps to open their ecosystems to third parties. For example, among other provisions, companies would have to let users install third-party apps or app stores through channels other than the company's default app store. In practice, this effectively permits a process known as sideloading, by which users can bypass major app stores and download apps from alternative, unvetted sources. Covered companies would also have to give developers access to the interface and hardware and software features of the operating system. Finally, the bill would also prohibit covered companies from requiring app developers to use the company's in-app payment system or pricing structure.

Although these provisions are framed as necessary measures to boost competition and online safety, they would instead undermine the tools and safeguards that help protect children online, support consumer privacy and cybersecurity, and sustain confidence in the applications consumers use and download every day. Congress should reject the ASFA and instead promote a secure, trusted, and innovative digital ecosystem that benefits consumers and small businesses.

The ASFA undermines parents' ability to protect children online

Major app stores currently provide parents with a range of tools that offer greater control and visibility into their children's online activity. For example, Apple allows parents to impose screen time limits, restrict access to websites, approve app downloads and purchases, and manage other content and privacy settings.[4] Its App Store also offers a curated children's category featuring apps designed for younger users.[5] The Google Play Store offers similar protections, including purchase approvals, screen time limits, parental controls, and additional content and functionality requirements for apps directed to children.[6]

Requiring covered companies to support third-party app stores risks fragmenting these protections and making it more difficult for parents to manage their children's activity. Alternative app stores may not provide safeguards equivalent to those provided by major platforms or may apply different standards or settings. As a result, parents could be required to identify, understand, and separately manage online safety tools across multiple stores. By requiring the decentralization of these protections, the ASFA would reduce parental visibility and place a greater burden on families trying to protect children online.

Third-party app stores may also apply less rigorous or consistent processes for reviewing apps directed to children. As a result, children could inadvertently access deceptive applications, malware, inappropriate content, or software that collects sensitive personal information without

---

[2] "State of the App Economy." *ACT | The App Association*, ACT | The App Association, actonline.org/wp-content/uploads/APP-Economy-Report-FINAL-1.pdf. Accessed 13 Jan. 2026.

[3] Rep. Cammack *H.R.3209: App Store Freedom Act*, 6 May 2025, www.congress.gov/bill/119th-congress/house-bill/3209/text.

[4] *Child Safety - Apple*, www.apple.com/child-safety/. Accessed 18 July 2026.

[5] *Design Safe and Age-Appropriate Experiences - Apple Developer*, developer.apple.com/kids/. Accessed 18 July 2026.

[6] *Google Play Families Policies*, support.google.com/googleplay/android-developer/answer/9893335?hl=en. Accessed 18 July 2026.

adequate safeguards. If harm occurs, weaker monitoring and enforcement systems could slow efforts to remove problematic applications promptly and prevent similar incidents from occurring again. These risks are particularly concerning for children, who may be less able to recognize deceptive practices, understand privacy and cybersecurity disclosures, or evaluate the consequences of granting an app's permission requests.

The ASFA places consumers' privacy and security at risk

App stores help protect consumers from unsafe or fraudulent software by screening applications before they can be downloaded. Major app stores review submitted apps for safety, functionality, and compliance with established terms of service before making them available to consumers.[7] As part of this process, app stores evaluate apps for content, advertising practices, privacy disclosures, developer authenticity, and whether an app's requested permissions are necessary for its stated purpose. Applications that fail to meet the necessary requirements may be rejected or removed. Although no review process can catch every threat posed to consumers, this vetting substantially reduces the likelihood that consumers will encounter malicious or fraudulent software.

Major app stores also continue to provide cybersecurity protections after an app has been installed, such as monitoring for emerging threats, distributing security updates, investigating misconduct, and disabling or removing malicious or noncompliant apps. These ongoing processes ensure that vulnerabilities or security threats can be promptly addressed before consumers face real harms. Enabling third-party distribution and update platforms could fragment these protections and make it more difficult to protect consumers from malicious or compromised software on their devices.

In practice, the requirement to enable the use of third-party app stores creates alternative pathways that bypass these protective measures and places consumers' privacy and security at risk. Third-party app stores may employ weaker or inconsistent security, authentication, or monitoring standards, and may fail to respond to security threats in the same timely manner that protects consumers today. Bad actors could exploit this insecure environment to distribute malware, commit financial fraud, or access consumers' sensitive personal information. By facilitating the use of third-party apps and the installation of apps from unvetted sources, the bill would place consumers at risk and make it more difficult to effectively identify, remove, or mitigate cyber threats.

The ASFA replicates the EU's costly digital regulatory model

The ASFA closely resembles the European Union's Digital Markets Act (DMA). Both frameworks require major platforms to accommodate third-party app stores, sideloaded apps, and alternative in-app payment systems. These measures risk importing the same regulatory complexity, market fragmentation, and uncertainty that have plagued the EU's ability to foster technological innovation and growth.[8]

---

[7] *App Review Guidelines - Apple Developer*, developer.apple.com/app-store/review/guidelines/. Accessed 18 July 2026; *Developer Policy Center*, play.google/developer-content-policy/. Accessed 18 July 2026.

[8] *The future of European Competitiveness: Report by Mario Draghi*, commission.europa.eu/topics/competitiveness/draghi-report_en. Accessed 18 July 2026.

The EU's broader regulatory environment already places disproportionate burdens on small businesses.[9] Smaller firms often do not have dedicated legal or compliance teams and must divert limited resources towards interpreting complex, overlapping regulations. These efforts then take away from the resources necessary to hire employees, develop products, reach new customers, or expand operations. Paradoxically, while the DMA and other EU digital regulations were intended to boost competition, they often instead reinforce incumbents or larger firms that possess the resources necessary to navigate complex regulations instead. The result is higher costs and lower quality for developers as they source distribution.

Congress should not import this regulatory model into the United States. Adopting EU-style regulations would impede the U.S. digital economy, risk discouraging innovation, and ultimately undermine U.S. technological competitiveness. Rather than leveling the playing field, this regulatory model would subject small businesses to the same compliance burdens that have imposed significant costs on their European counterparts. Instead, Congress should preserve the conditions that have enabled small technology businesses and independent app developers to grow and innovate.

The ASFA undermines investment in consumer trust that benefit small businesses

Major app stores invest in functions that earn consumers' trust in the software they host. This trust capital helps small businesses compete in the digital marketplace. Through application reviews, developer verification, security standards, and ongoing enforcement, these stores can provide consumers with greater confidence that the applications they download have met baseline standards for safety, functionality, and content. This trust is especially valuable to small businesses, which often lack the name recognition, advertising budgets, or longstanding customer relationships that larger brands rely on. Approval by a trusted app store serves as an important signal of credibility that enables small businesses to attract customers and compete with larger firms.

The ASFA risks weakening this advantage by fostering the development of a fragmented app ecosystem with inconsistent review processes, security standards, and consumer protections. In such an environment, consumers may hesitate to trust unfamiliar applications or app stores, and that uncertainty would likely make them less willing to download applications from smaller, unfamiliar developers. As a result, small businesses would have to spend more on marketing and customer acquisition to establish the same level of consumer confidence that major app stores currently help provide.

Conclusion

The ASFA would replace today's trusted and secure app ecosystems with a more fragmented model that exposes consumers and small businesses to greater privacy, cybersecurity, and online safety risks. By weakening market-driven, centralized safety protections, increasing privacy and cybersecurity concerns, and undermining the trust that helps small businesses reach customers, the bill would impose substantial costs without offering a commensurate benefit to the digital marketplace. It would also import a European regulatory approach that has replaced technological growth and innovation with complexity and uncertainty. Congress should reject the

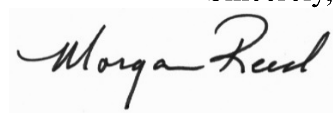
---

[9] *EU Digital Markets Act: One Year Later*, actonline.org/wp-content/uploads/DMA-One-Year-Later.pdf. Accessed 18 July 2026.

ASFA and preserve the digital infrastructure that enables consumers and small businesses to compete in the digital economy.

Thank you for your time and consideration. We appreciate the Subcommittee's focus on strengthening consumer protection and welcome the opportunity to further engage as the legislative process moves forward.

Sincerely,



Morgan Reed
President
Association for Competitive Technology