January 27, 2026

The Honorable Adrian Smith
Chairman
Subcommittee on Trade
Committee on Ways and Means
Washington, District of Columbia 20515

The Honorable Linda Sánchez
Ranking Member
Subcommittee on Trade
Committee on Ways and Means
Washington, District of Columbia 20515

Dear Chairman Smith and Ranking Member Sánchez:

Thank you for the opportunity to submit comments for the record for your hearing, titled "The Role of Trade Policy in Maintaining American Innovation and Technology Leadership." Trade agreements are key to maintaining the United States' edge in innovation and ensuring businesses have the support they need to experiment with new ideas. We applaud the Subcommittee for looking into the ways trade policy can further support small businesses in the technology industry.

ACT | The App Association (ACT) is a global trade association for small and medium-sized technology companies. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. Many of our member companies use the patent system and other intellectual property laws to protect their ideas and products. They need protection from predatory international actions in the intellectual property (IP) system, as well as protections from required compliance with privacy-inhibiting laws and regulations.

Key Digital Trade Protections for Small Tech

Trade policy can have an outsized impact on small businesses and their ability to enter new marketplaces. A wide variety of national and international policies can impede small businesses from growing, thus decreasing the American economy and our power abroad. Strong competition from American businesses allows us to continue to project power around the world. Small American technology companies like the members of ACT need digital trade agreements to prioritize several foundational policies:

> *Enabling Cross-Border Data Flows.* The seamless flow of data between economies and across political borders is essential to the functioning of the global economy and for American small business technology developers as they seek access to new markets.

Prohibiting Data Localization Policies. American companies looking to expand into new markets often face regulations that force them and other foreign providers to build and/or use local infrastructure in the country. Data localization requirements seriously hinder imports and exports, reduce an economy's international competitiveness, and undermine domestic economic diversification.

Prohibiting Customs Duties and Digital Service Taxes on Digital Content. American innovators must take advantage of the internet's global nature to reach customers who live outside of the United States. However, the tolling of data crossing political borders with the purpose of collecting customs duties directly contributes to the balkanization of the internet. These practices jeopardize the efficiency of the internet and effectively block innovative products and services from market entry.

Ensuring Market Entry is Not Contingent on Source Code Transfer or Inspection. Some governments have proposed policies that require companies to transfer, or provide access to, proprietary source code as a requirement for legal market entry. Intellectual property is the lifeblood of app developers' and tech companies' innovation; the transfer of source code presents an untenable risk of theft and piracy. Government policies that pose these requirements are serious disincentives to international trade.

Preserving the Ability to Utilize Strong Encryption Techniques to Protect End User Security and Privacy. Global digital trade depends on the use of strong encryption techniques to keep users safe from harms like identity theft. However, some governments continue to demand that backdoors be built into encryption keys for the purpose of government access. These policies jeopardize the safety and security of data, as well as the trust of end users, by creating known vulnerabilities that unauthorized parties can exploit. From a privacy and security standpoint, the viability of a technology developer's product depends on the trust of its end users.

Securing Intellectual Property Protections. The infringement and theft of intellectual property and trade secrets threatens the success of American innovators and hurts the billions of consumers who rely on their products and services. Our members routinely use a wide range of intellectual property protections to support their businesses, and violation of those protections can be catastrophic for businesses. The adequate and effective protection and enforcement of intellectual property rights is critical to innovation and growth in the digital economy.

Avoiding the Misapplication of Consumer Protection and Competition Laws to New and Emerging Technology Markets. Various regulators, including key trading partners, are currently considering or implementing policies that would put mandates on nascent and developing emerging technology markets. For example, some regulators are jeopardizing small businesses' ability to compete by upending the functionality of digital platforms that lower overhead costs, provide greater consumer access, simplify market entry, and

strengthen intellectual property protections. Others are considering interventions into undefined and emerging technology markets, such as artificial intelligence. Foreign governments upending technology markets through misguided regulations inconsistent with U.S. law will disadvantage American innovators and serve as significant trade barriers.

Avoiding the Misapplication of Competition Laws to Unfairly Target U.S. Companies: Similarly, there is a risk of foreign governments enforcing competition and consumer protection laws in ways that tend to unfairly disadvantage American competitors versus their rivals based in foreign countries. South Korea stands out in particular in this regard. Despite agreeing not to move forward with platform regulations as part of the Korea Strategic Trade and Investment Deal, the Korean government continues to push forward with the misleadingly-named *Online Platform Fairness Act*, which would functionally target U.S. companies. Through sector-specific scoping it ensures that leading U.S. companies that provide the platforms ACT members utilize, like Google, Apple, Coupang, Meta, Netflix, and Uber, bear the overwhelming share of the burden. The downstream effect could be devastating for both American small businesses and Korea's vibrant domestic startup community. The legislation is also unprecedented compared to regulatory frameworks in other global jurisdictions, combining strict operational mandates with aggressive penalties including massive fines for non-compliance, while giving the Korea Fair Trade Commission (KFTC) broad discretion to enforce its provisions under vague "fairness" standards. Given the KFTC's history of targeting U.S. technology companies with intrusive investigations and onerous fines under existing legislation, this new legislation would simply give it even more firepower to double-down on these tactics.

ACT has further concerns with related enforcement by Korean authorities that are shaking the confidence of small innovators. Korean officials have recently leveraged a data security incident to target Coupang, a U.S. technology company, including arbitrary enforcements, fines, and threats of criminal charges against its American executives, with the apparent intent of hampering a U.S. company's ability to compete in the Korean market. Korean authorities' approach in this instance undermines needed confidence in integrated platform services and marketplace management tools small businesses rely on when doing business overseas. Small business innovators succeed when domestic laws welcome competition from overseas, but they encounter difficulty when laws and their application target their preferred business partners and distribution channels, many of which happen to be based in the United States.

Of all these policies and enforcement tactics, protection for intellectual property and avoiding the misapplication of competition and consumer protection laws stand out as areas for increased scrutiny by Congress. In the Subcommittee's effort to ensure U.S. trade policy promotes strong technology leadership, we urge you to consider these key tenets of digital trade, as well as to

consider specific legislation that incentivizes Korea not to use the misapplication of competition policy to discriminate against U.S. technology companies.

Intellectual Property and Small Businesses

The global digital economy holds great promise for small app development companies, but our members face a diverse array of trade barriers when entering new markets. These barriers may take the form of laws, regulations, policies, or practices that protect domestic goods and services from foreign competition, artificially stimulate exports of domestic goods and services, or fail to provide adequate and effective protection of intellectual property rights (IPR). While these barriers have different forms, they all have the same net effect: impeding U.S. exports and investment at the expense of American workers. Trade agreements must support American businesses by punishing the common types of IP theft, including copying, misappropriation of trademarks, and government-mandated technology transfer. They must also prohibit and punish frivolous lawsuits against IP holders and licensees.

The infringement and theft of IP online threatens consumer welfare by undermining the ability of creators of digital content to innovate, invest, and hire. App developers that drive the global digital economy are subject to an estimated loss of $46.3 billion in revenue due to pirated apps. Such a loss of revenue presents a major threat to the success of ACT's members, their customers, and the workforce that supports the creation and growth of digital products and services. Each kind of IPR (copyrights, trademarks, patents, and trade secrets) represents distinct utilities upon which ACT members depend. IPR violations lead to customer data loss, interruption of service, revenue loss, and reputational damage – each alone is a potential "end-of-life" occurrence for a small app development company.

Many stakeholders, including the ACT community, are deeply concerned with the U.S. Trade Representative's (USTR) October 25, 2023, announced withdrawal of support for foundational digital trade policies, including those that enable cross-border data flows, avoid forced data localization mandates, protect source code, and ensure that digital products are not unduly discriminated against. The USTR's position significantly impacts U.S. leadership across various global industries and platforms, enabling countries like China to secure their position and dictate matters on global trade. We are concerned that stepping back on crucial digital trade priorities that support U.S. businesses will set a harmful precedent for other U.S. trade interests. We urge the Subcommittee to work with USTR to reinstate their position for crucial digital trade priorities that allow small and large businesses alike to reliably operate and strengthen the United States as a global powerhouse for important and emerging trade objectives.

In addition, we note a continued concern with third-party litigation funding (TPLF) used as a mechanism to abuse patent processes in the United States and internationally against U.S. companies. While this issue is faced globally, we focus on its impact to the U.S. market. Non-practicing entities (NPEs) initiate a majority of the abusive and frivolous patent infringement suits in the United States, and many NPE suits are financially backed by unnamed investors

hidden through shell corporations or wealth funds that may have a real interest in the outcome of litigation. TPLF has affected critical U.S. technology industries, including telecommunication, automotives, and semiconductors. Funders may be individual entities seeking economic gain or competing countries strategically undermining essential U.S. industries and U.S. national security. The serious harms to the U.S. market evidenced by TPLF will undermine equity for U.S. businesses, workers, and consumers.

The Chilling Effects of the Digital Markets Act

The European Union's (EU) Digital Markets Act (DMA) has a variety of problems that U.S. policymakers must not allow to enter the domestic market in trade agreements. It severely disadvantages small business innovators, despite its intent to target large online marketplaces and platforms; pokes holes in privacy and security policies; forces delays and mandates that are not in the best interests of businesses, their customers, or the public; and makes regressive changes to existing fee structures in online marketplaces. Many of our EU-based members have experienced significant problems with the implementation of the DMA and have concerns about ongoing issues with the regulation.

Privacy and Security Challenges. DMA requires smart devices to accept third-party app stores and open access to an individual's device for any device maker or service provider. This circumvents the curation and vetting of mobile apps or connected devices that major platform operators currently undertake to prevent malware and criminals from getting access to a user's device or data. This erosion of security and privacy reduces customer trust in the safety of downloading apps. That loss of trust disproportionately impacts ACT members, which depend on consumers having some level of assurance that apps made by companies they have never heard of are safe and work as intended. Our members say this about their concerns around privacy in the DMA:

> *Mitchel Volkering, founder of Netherlands-based Vaic.at:* "There is no such thing as perfect security, but I can guarantee that individual smartphone users' privacy and security will get worse if you mandate the existence of additional threat vectors. You do not deal with a hole in a boat by shooting another hole in it."
>
> *Clément Sauvage, founder of France-based Bits 'n Coffee:* "Smart devices have very sensitive data. They're now repositories of healthcare information, precise location, personal photos, and confidential messages that people do not expect to be shared. DMA's interoperability mandates are being applied to require support for notifications to third-party wearable devices in ways that subvert consumers' expectations. Meta's business model is to make money on my data. I know that, and that's why I don't share information with them. These mandates would take that choice out of my hands."

DMA-Caused Delays. The DMA has built-in periodic reviews attempting to assess the impact and address lessons learned about unintended consequences. One of those reviews is scheduled to finish in May 2026, and, unfortunately, rather than signaling changes that would reduce the burden of DMA, the European Commission (EC) has talked about expanding it to "the artificial intelligence (AI) sector." The DMA and other European tech regulations have already delayed the introduction of the latest AI models in Europe, forcing small business innovators in the EU to rely on older models and U.S. app companies to build the delays into their products in order to continue reaching EU customers. These delays have already had a detrimental impact on our EU member companies, and we are concerned that a DMA-style framework in the U.S. would have similar worrisome results for our American members. In fact, both U.S.- and EU-based members are concerned about these delays:

> *Clément Sauvage, founder of France-based Bits 'n Coffee:* "EU developers shouldn't be blocked from using tools like Llama 4 and Apple Intelligence. **The delay puts us at a distinct disadvantage against our U.S. and other global rivals, who get to use the latest technology has to offer.** DMA shoots us in the foot in this regard."
>
> *Mitchel Volkering, founder of Netherlands-based Vaic.at:* "We're restricted from accessing innovative new tools and features that Apple and other companies release in the U.S. and other regions. These include Apple Intelligence and iPhone Mirroring. In the EU, when these tools do arrive, they're often late and degraded versions. **Competing with rivals based outside the EU has never been more challenging than it is today.**"
>
> *Sebastian Holst, founder of New Jersey-based Fool Me Once, LLC*: "We've already seen how trusted marketplaces convey security and scale to small business offerings, opening markets and fueling growth. Assuring responsible AI raises the stakes and the expectations by orders of magnitude, making the stabilizing and standardizing influence of trusted platforms more important than ever before. I would be hard-pressed to find a worse time to impose DMA-style obligations. High-speed trains are not limited by their engines. It's the quality and trust in the tracks that hold them back. **The wrong kind of regulation will have small businesses moving at 20th-century speeds in a 21st-century race.**"

Fee Structures. Right now, the two major consumer-facing app stores have progressive fee structures for companies distributing their apps on the store. Almost all apps and app developers, in non-DMA jurisdictions, pay no commission on revenue in exchange for developer services, including distribution of apps. Apple's App Store and the Google Play Store charge developers making more than $1 million in digital-only goods and services 30 percent on those sales, but these developers only account for a tiny fraction of all developers. Some of these multi-billion dollar companies are proponents of DMA because the law eliminates the distribution costs these companies bear now in non-DMA jurisdictions. Right now, the only DMA-compliant fee

structure shifts the costs of maintaining and improving digital platforms downward to smaller developers like ACT members.

> *Sveatoslav Vizitiu, Romania-based founder of Rhuna:* "Let's get something straight. Most of us don't pay any commission. My business is centered on improving the events and entertainment industry by tokenizing products, services, and experiences. That's not a digital-only service, so I don't pay a commission on sales. These companies complaining and agitating for DMA sell digital-only services, and that's just not the majority of developers. Even most developers who pay a commission recognize they get value for the money. **Distribution isn't free, so I don't appreciate that the bigger companies are trying to shift more of those costs to my business through regulation.**"

Wi-Fi Mandates. The DMA would alter the current structure for sharing Wi-Fi passwords on Apple devices. As of now, iOS devices can share Wi-Fi passwords with nearby devices through a simple tap. This sharing is possible through the device-level storage of Wi-Fi passwords and other sensitive information, a structure which keeps the passwords secure. The DMA would require Apple to collect all the Wi-Fi passwords stored on your device and allow sharing with any other device, even those made by adversary countries which are known to steal such information. The goal of this provision in theory is to force Apple to not have a monopoly on this device feature, but in reality, it will open up your personal device to infiltration by nefarious actors, increasing privacy risks.

> *Mitchel Volkering, founder of Netherlands-based Vaic.at:* "I provide services for job search candidates who trust me and their smart devices with their personal information. If they go to an interview and their device connects to the Wi-Fi, DMA mandates that a third-party device has access to that information. After the interview, if the candidate is connected to that same Wi-Fi regularly, a third-party device now has that information too and can ascertain they must have gotten the job. **The fact that this information is now potentially for sale undermines my competitive position by giving all my competitors potential access to my client's information and also exposes my client to privacy risks associated with their Wi-Fi connection history.** Their movements can be tracked. It is not appropriate for government to create these problems. It certainly doesn't help my EU-based company, and it should serve as a warning for U.S. policymakers."

These real-time concerns of EU entrepreneurs give a preview of what could come if the U.S. adopts a regulatory framework similar to the DMA. We urge the Subcommittee to remember these concerns when working with trade negotiators on digital trade issues.

The American Innovation and Choice Online Act: USA's DMA

At a high level and through a strong filter, the American Innovation and Choice Online Act (AICOA, H.R. 3816, 117th Congress) and DMA may seem different. And drafters are undoubtedly making refinements to AICOA ahead of its broader unveiling. However, closer inspection reveals that the two frameworks share too much in common to be considered substantively distinct, from the common proponents seeking their enactment and implementation to the same effects they have (or would have) on "Small Tech" prospects. Heeding small business innovators' warnings in the EU as they caution other jurisdictions of the DMA headaches they are experiencing will be crucial to help us understand what's at stake with AICOA.

Open Access or Must-Carry Mandates. Just like DMA, AICOA's provisions act like a belt and suspenders— both mandating open access to core technologies, and prohibiting "self-preferencing" by companies providing those core technologies. These overarching cornerstones work together to prohibit day-to-day online marketplace management functions and wraparound services that small businesses tend to rely on. For example, the EC's requirement that Apple's mobile operating system, iOS, "future proof" the openness of its features requires that they be built in a way that satisfies any possible, potential use of iOS. Notably, the exception to this mandate only allows for safeguards to the "integrity" of the operating system, which according to the EC, may not include privacy or security protections. These same open access provisions could potentially be applied to online retail marketplaces as well, requiring that seller services be provided in one-size-fits-all formats. Meanwhile, DMA's prohibitions on "self-preferencing" serve to eliminate any concomitant app store and operating system protections since by limiting access to bad actors, the relevant gatekeepers are effectively preferencing the platform's own offerings. Likewise, the provision of seller services, such as two-day shipping fulfillment and AI-driven Seller Assistants to certain sellers may be considered a form of self-preferencing, since the gatekeeper to making those options available as complements to its core distribution service. Finally, the self-preferencing prohibition has also mandated a less curated experience on Google Search, adding friction, devaluing the experience for consumers in the EU, and making ACT members less discoverable. The results DMA's open access mandates and self-preferencing prohibitions have precipitated can be expected in the U.S. if AICOA were to become law because its provisions largely mirror DMA's.

Outlawing the Progressive Fee Structure. Both AICOA and DMA would effectively outlaw the app stores' current progressive fee structure, allowing only alternatives that charge small businesses more, while charging the largest businesses relatively less. Outside of Europe, the main app stores charge no commission for about 85 percent of apps, which are typically part of an offering involving "real-world" goods and services. For the remaining 15 percent of apps, the stores generally charge 15 percent of revenue made on "digital-only" goods and services, while revenue over $1 million each year generates a 30 percent commission. According to estimates, less than 1 percent of apps on the stores are subject to this higher fee. Thus, under the current fee structure, most developers, including ACT members, pay no commission to the stores. Meanwhile, a small group of apps with digital-only services as their main revenue generator—such as dating and gaming apps—pay a commission that presumably goes toward maintenance of the stores and provision of the distribution services ACT members leverage. The proponents of DMA and AICOA are looking to outlaw the current fee structure so that they pay less, leaving smaller businesses to pay more.

AICOA attacked fee structures in several ways, including by prohibiting "tying" payment processing to access to the platform and making it unlawful for a "systemically important platform … to materially restrict or impede users from changing default settings that direct or steer users to products or services offered by the systemically important platform operator…" A few of the largest businesses with apps on the stores have sought to avoid having to pay for distribution, including by trying to use complicit third-party payment processing services that would help them avoid paying the fees they owe. These AICOA provisions are designed to require that they be allowed to evade the enforcement of any fee structure on an app store.

Similarly, DMA's Article 5(4) provides that covered gatekeepers "shall allow business users, free of charge, to communicate and promote offers, including under different conditions, to end users acquired via its core platform service." While this provision may seem only tangentially related to fee structures, the EC has in fact implemented the requirement in a manner that declares the current fee structures illegal. For the stores, the only available path appears to be the creation of *more regressive* fee structures that charge developers by the download and or otherwise begin to require distribution commissions on revenue generated from *real-world* goods and services.

Standards and Standard-Essential Patents

A lesser known but critical aspect of the international IP system is the creation and maintenance of voluntary standards. Each standard is a collection of features that innovators and manufacturers can implement in their devices to ensure their interoperability with other devices. For example, billions of devices access wireless internet through Wi-Fi standards, cellular data availability rests on 4G and 5G standards, and even electrical outlets have standards to ensure devices from lamps to supercomputers can connect to the electrical grid. Many standards require the use of patented technology to implement, and a patent holder may voluntarily offer their technology to the standards-setting organization (SSO) for inclusion in the standard. If a patent is selected for inclusion in the standard, making it a standard-essential patent (SEP), the patent holder agrees to license the patent to any willing licensee on fair, reasonable, and non-discriminatory (FRAND) terms as a compromise for holding a monopoly on technology required to implement the standard. SEPs and FRAND licensing are key to the global digital economy.

Unfortunately, some bad actors abuse SEP licensing to generate illicit revenue or to force companies to settle frivolous lawsuits. Most recently, a variety of streaming services have been sued by Dolby and others alleging the infringement of their patent licensing agreement. The license in question relates to "codecs," devices or programs that compress and decompress data to enable faster transmission. Dolby alleges that the license for these "codecs" only covered the compression function, not the decompression for streaming on end users' devices. ACT filed an amicus brief in favor of the streaming service in this case, given our members' interest in protecting strong SEP licensing and FRAND commitments for those licenses.

Small businesses, including those ACT represents, are particularly dependent on the predictability of SEP licenses on reasonable terms. These entrepreneurs, innovators, and

developers can incorporate standardized features in their products by purchasing off-the-shelf modules without the need to invest in internal expertise. Instead, they can dedicate their R&D resources to developing the features that set their products apart and bring them to market more swiftly. This is particularly true in the context of the internet of things (IoT) products, which are typically specialized devices focused on one or two distinct and innovative features. Small business developers often have an advantage in this area because they can develop these specialized products without the costly overhead and infrastructure of larger organizations.

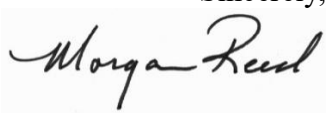
Injunctions can present an acute problem for small businesses wishing to license SEPs for use in their own products. Once a patent is declared "essential" to a standard, the alternatives become unavailable for manufacturers seeking to adopt the standard. The inability of manufacturers to walk away means that the threat of injunctions give SEP holders significant leverage. Since standards are frequently used in multi-functional devices and frequently contain thousands or tens of thousands of essential patent families, the cost of market exclusion can be orders of magnitude greater than the value attributable to the SEP. As a result, potential licensees faced with the prospect of an injunction are under substantial pressure to enter into licenses at above-FRAND royalties. This pressure is particularly acute for smaller companies who cannot afford to engage in costly litigation. Above-FRAND royalties paid for SEPs may ultimately be passed on to consumers through higher prices or reduced investment in R&D.

Despite the prohibition of injunctive relief, many SEP holders frequently pursue the remedy and, in certain foreign jurisdictions, frequently obtain it. SEP injunctions are routinely used to pressure implementers into accepting above-FRAND terms. This reality makes the role of courts in enforcing FRAND remedies indispensable to preserve competitive access to standards across jurisdictions. Congress must include strong FRAND commitments in trade agreements, especially with countries likely to engage in predatory lawsuits or otherwise ignore IPR.

Conclusion

American businesses need U.S. trade policy that supports them, protects their IPR, and punishes malicious actors. They also need the USTR to push back on harmful policies in the DMA and its imitators around the world, ensuring American companies can keep their data safe and continue to build trust with customers. Congress should continue to support American businesses by not implementing laws that copy problematic policies from the DMA and by pushing for stronger digital trade protections in trade agreements. We urge the Subcommittee to continue its oversight of trade policy and ensure the needs of small businesses are met.

Sincerely,



Morgan Reed
President
ACT | The App Association