ACT'S ANNUAL

GLOBAL APP ECONOMY CONFERENCE

POLICY PRIORITIES FOR STARTUPS, SCALEUPS, AND SMALL BUSINESSES

UNITED STATES

2026

Contents

Contact Us

For more information about our global policy issues, reach out to:

Graham Dufault
General Counsel
gdufault@actonline.org

Taylor Downs
Federal Policy Manager
tdowns@actonlineorg

Visit us online at: actonline.org

About ACT

Who We Are

ACT is a global technology trade association representing startups, scaleups, and small businesses. We work directly with our members worldwide to advocate for a policy environment that takes into account their real-world challenges and supports innovation, access to capital, job creation, and the ability of small technology companies to grow and compete globally.

Who Our Members Are

Our members are entrepreneurs, independent developers, and small firms building software, hardware, and digital services across the global economy. They develop mobile and AI applications, manufacture connected devices, and deliver B2B and B2C solutions across sectors including agriculture, cybersecurity, education, healthcare, entertainment, and hospitality. While their business models vary, they share common priorities on global tech policy issues that directly affect their companies, along with concerns about innovation, competition, and economic growth.

Our Policy Issues

ACT's policy agenda is driven by our members and focused on advancing clear, scalable regulatory frameworks that enable small technology companies to innovate and grow. We engage with policymakers on issues critical to the future of technology and innovation including artificial intelligence, online safety and privacy, competition, digital trade, and digital health. We also advocate on core small business priorities such as mergers and acquisitions, tax policy, and workforce development.

What We Do

ACT connects policymakers with the real-world perspectives of small tech entrepreneurs by:

- Providing direct insight from startups, scaleups, and small businesses on how policy decisions affect innovation, jobs, and competitiveness
- Educating policymakers and staff through briefings, roundtables, and events focused on the needs of small tech businesses
- Advocating on specific policy proposals through letters and formal communications to government leaders
- Meeting directly with regulators and officials worldwide to explain the practical impacts of regulatory and legislative priorities
- Participating in formal consultations and providing detailed comments with on-the-ground feedback on global technology policies

Privacy, Age Assurance, and Data Security

AGE ASSURANCE

Certain social media platforms and adult content providers are attempting to offload their responsibility to assure the ages of their users. These stakeholders are trying to sell lawmakers on an alternative regime that shifts liability and compliance burdens onto small business app developers instead of social media and adult content websites.

During this session of Congress, both chambers are considering the App Store Accountability Act (ASAA, S. 1586 / H.R. 3149, 119th). This measure roughly tracks similar state proposals and would expose small business app companies to untenable new liability risks and compliance costs. Fortunately, Congress is also considering an alternative, the Parents Over Platforms Act (POPA H.R. 6333, S. 4349, 119th), which would keep parents in the driver's seat of sharing their kids' sensitive information and would only apply age assurance requirements on apps that specifically provide a different experience for minors than they do for adults.

PRIVACY AND DATA SECURITY

Unfortunately, the United States lacks a federal data privacy law. Unlike many jurisdictions around the world, the United States does not have a nationwide statute providing rules of the road for how companies should handle and protect consumer data. Instead, American companies must operate in an environment with several sectoral laws governing certain types of data (health, banking, etc.) with large gaps in between. Worse, those gaps are increasingly being filled by conflicting state laws, creating a complex patchwork that gets more difficult to navigate by the year.

Why Privacy and Age Assurance Policies Matter to Startups, Scaleups, and Small Businesses

AGE ASSURANCE

Bills like ASAA would impose unnecessary new mandates and sources of liability on any entity with an app on the store, leading to costs that could exceed $280 billion. These ASAA mandates are unnecessarily punitive, unfair, and would give parents less control, not more. The ASAA would:

- Require every app, even if it has nothing to do with social media or children, to create new systems to receive and verify flags from app stores indicating the age category of every single user;
- Replace the current parental consent system, where downloads are prevented at the operating system level when parents reject them, with a clumsier, more failure-prone system;
- Force any entity with an app on the stores to create compliance programs under the federal Children's Online Privacy Protection Act (COPPA), an expensive proposition from both a compliance and potential liability standpoint, that is intended only for online services directed to children.

PRIVACY

Small software and connected device companies like ACT members handle millions of terabytes of data per day, putting them on the front lines of protecting and enabling responsible use of data. In fact, a competitive dynamic has developed among our members to meet customer expectations regarding privacy. However, without a federal comprehensive privacy law, businesses of every size are stuck in limbo caused by the failure of Congress to act. And unlike the biggest companies, small businesses do not have large, expensive compliance departments that can handle the ever-growing patchwork of state and international privacy laws.

What Startups, Scaleups, and Small Businesses Need from Policymakers

01. Oppose legislation like ASAA because it is a blatant attempt to distribute the responsibilities of providers of age-sensitive materials onto the rest of the ecosystem. This legislation would impose substantial, unnecessary costs and liabilities on small business developers, while letting social media platforms and adult content providers that are the source of the problem off the hook. Perhaps worst of all, the bill also puts parents last, requiring that they accept parental control tools at the speed and flexibility of government.

02. Support POPA, which would reinforce parents' ability to make use of the extensive, granular, and ever-improving tools for both parents and developers. For parents, these tools allow for access and control of every application, including web browsers—all from their own devices. While ASAA would undo these features, POPA would reinforce them and include additional age assurance responsibilities for apps that provide different experiences for minors than for adults.

03. Support a federal data privacy law with the "4 Ps of Privacy:" Preemption, no Private right of action, a Path to compliance, and Protection against unauthorized access. If Congress strikes the right balance on these concepts, it can help small businesses avoid the impending compliance tsunami from differing state laws and better enable our members to continue innovating, creating jobs, and revolutionizing industries.

Artificial Intelligence

Startups and small businesses are creating, adapting, and using artificial intelligence (AI) to drive the next wave of innovation. ACT's members are applying AI to solve real-world challenges in healthcare, finance, education, infrastructure, and more. Our members are streamlining government processes, enhancing cybersecurity, and making services more accessible and efficient. However, a surge of contradictory and overlapping policy proposals at every governmental level threatens to hinder responsible innovation.

Why AI Policy Matters to Startups, Scaleups, and Small

Unfortunately, the regulatory morass we are seeing across the United States and globally puts American small business leadership at risk. Here are four of our key policy concerns:

01. REGULATORY OVERREACH

In general, current laws already apply to the development, deployment, and use of AI technologies. In addition, standards-setting organizations (SSOs) are developing technical standards to address risks in ways that supplement or translate current legal frameworks. For fast-moving technologies like AI, standards are often better suited than rigid rules. They can adapt more quickly, reflect technical expertise, and translate high-level governance goals into practices that companies can actually implement. For example, the Coalition for Content Provenance and Authenticity (C2PA) participants are working on standardization to assure the provenance of content in the generative AI era; the International Standards Organization and International Electrotechnical Commission (ISO/IEC) have developed a standard for age assurance methods; and IEEE is working on security and trustworthiness standards for generative AI models that likewise address issues such as transparency, privacy, bias, and system safety.

Certainly, government is a part of this ecosystem. For example, the National Institute for Standards and Technology (NIST) plays an important role in coordinating the federal government's participation in SSOs and in providing guidance and frameworks like the one it's developing for AI agents. The federal government also should invest in AI research to promote access to trainable data and foundational resources. However, too often lawmakers are jumping to conclusions, ignoring the laws and standards efforts that are already in place. To date, more than 1,400 new AI bills have been introduced across state legislatures and Congress. Moreover, the European Union (EU) has already passed AI regulations that are yet to be fully implemented or understood. Many propose regulating AI technologies themselves, potentially requiring premarket audits or assessments to evaluate risks of harmful bias, regardless of the likelihood or intent of such use. States have also introduced proposals for outright behavior bans and new liability frameworks tied to potential downstream misuse regardless of likelihood or intent. This kind of intervention would shut down broad swaths of beneficial AI system development by eliminating the development of tools that may possibly introduce risks if misused, a requirement that virtually no other technology is expected to meet.

02. ANTITRUST OVERSENSITIVITY

Aggressive antitrust regulators are attempting to pick winners and losers before the field of participants is fully known. Global antitrust authorities are threatening to close off the flow of investment dollars into the development of AI.

Regulators are completely missing the fact that these markets are highly competitive, involve truly small businesses, and are rapidly evolving. Many of the most significant investments come from large incumbent cloud service providers (CSPs). Small AI innovators often leverage CSPs not only for access to capital, but also for cloud infrastructure, compute, model access, developer tools, distribution channels, and commercial partnerships that help them build and scale. Regulators who fail to understand this important interdependency can destroy the future of AI for small business. Restricting access to capital and these broader relationships with CSPs will harm small business competitors by limiting essential funding sources, infrastructure, and pathways to growth, ultimately reducing the number of competitors in the market.

03. AI AND COPYRIGHT

The increasing ubiquity of AI has introduced uncertainties around the copyright protection of content like images as well as software developed through both open- and closed-source models. For small business software developers, like ACT members, who both deploy and use AI, these uncertainties disproportionately harm their ability to create competitive products across markets. In the United States, recent Copyright Office guidance and court decisions are beginning to draw lines around issues such as human authorship, fair use, market harm, and the use of lawfully acquired versus pirated training materials, but the legal framework remains unsettled. While courts around the world test the boundaries of the lawful use of a copyrighted work, policymakers are attempting to create frameworks that allow for emerging technology to exist alongside strong intellectual property (IP) laws.

04. DATA CENTERS

Data centers are a crucial input in the AI revolution, but they're also necessary for any kind of internet traffic. At the state and local levels, debates are raging over data center placement. Federal policymakers must also understand what's at stake if data centers are blocked unnecessarily. They are part of the infrastructure layer on which ACT members build their cutting-edge technologies. Robust data center access lowers small business innovator input costs, enables broader customer reach, and accelerates deployment of the latest

innovations. Pro-competitive data center policies not only better position the United States to compete with rivals in the AI race but also serve as a catalyst for small business innovation and growth.

What Startups, Scaleups, and Small Businesses Need from Policymakers

By fostering a regulatory environment that balances innovation with responsible oversight, we can ensure that our members are able to utilize AI to deliver widespread benefits across all industries. Specifically, we urge Congress and federal agencies to:

Support congressional measures like:

- **The Small AI Innovators Empowerment Act,** which would equip policymakers with a clearer picture of which obstacles, including regulatory impediments, stand in the way of small business AI innovators.

- **The Promoting U.S. Leadership in Standards Act (S. 1269, 119th),** which would provide resources for standards-development organizations (SDOs) to host standards development meetings in the United States, where U.S. small businesses can better access them.

- **The Standardizing Permitting and Expediting Economic Development (SPEED) Act (H.R. 4776, 119th)**, which passed the House in December 2025 and is pending in the Senate. The bill would rationalize and remove overlapping environmental review requirements to streamline the buildout of new energy projects, including those intended to fuel AI.

- **The CREATE AI Act (H.R. 2385, 119th),** which would establish the National Artificial Intelligence Research Resource to broaden access to the compute, data, software, and other tools needed to support AI research and experimentation across a wider range of institutions and innovators.

- **The NSF AI Education Act (H.R. 5351, 119th)**, which would expand AI education and workforce development efforts through scholarships, fellowships, Centers of AI Excellence, and partnerships designed to strengthen the domestic AI talent pipeline.

- **The Future of AI Innovation Act (S.3952, 119th),** which would strengthen U.S. AI innovation by establishing voluntary AI standards, metrics, evaluation tools, and testbeds, while also identifying regulatory barriers that may be slowing deployment and competition.

Support agency actions like:

- **The National Institute of Standards and Technology (NIST) and the Center for AI Standards and Innovation (CAISI)'s ongoing work on voluntary AI guidance, standards, and technical resources,** including the AI Risk Management Framework, the Generative AI Profile, the Cybersecurity Framework Profile for AI, and recent work on AI agent security, evaluations, and post-deployment monitoring, which can help promote practical, risk-based, and interoperable approaches to AI governance that organizations of all sizes can use.

- **Administration actions proposing an alternative to a patchwork**, including the March 20, 2026, National Policy Framework for Artificial Intelligence, which proposes a roadmap for Congress that takes a balanced approach on protecting innovation, kids, privacy, intellectual property, and promoting workforce development.

- **The Ratepayer Protection Pledge on AI data centers, announced on March 4, 2026,** which seeks to support continued investment in AI infrastructure while ensuring that new power delivery and related upgrade costs required to serve data centers are borne by hyperscalers and AI companies rather than passed on to ordinary households.

Additionally, Congress and federal agencies should:

01.
Support a federal AI framework that preempts state laws that unnecessarily regulate the inherently interstate aspects of the technologies themselves and seek to duplicate what existing law already does in consumer protection, civil rights, copyright, and a wide range of other areas.

02.
Reject antitrust measures that treat AI markets as already overly consolidated before they have developed and ensure that small business innovators can continue to access integrated services—and even investment—from well-resourced incumbents in adjacent or upstream markets.

03.
Approach proposals to change copyright law with caution and ensure that they avoid taking away important intellectual property rights while safeguarding legitimate AI use and development.

04.
Support policies that enable efficient placement of data centers and sensible permitting processes for the energy that powers them.

Competition, Antitrust, and Marketplace Policies

Washington's antitrust conversation has become detached from the realities of the app economy. Policymakers are advancing a range of proposals, from legislation like the American Innovation and Choice Online Act (AICOA, S. 2033, 118th) to aggressive merger enforcement doctrines that treat all large platforms as monopolists and all acquisitions as suspicious.

Marketplace Competition

The antitrust maximalist narrative ignores the economics of trust: the long-term accretion of consumer confidence won by well-managed marketplaces, and how this trust supports a path for ACT's members. They leverage curated online marketplaces (COMs), including app stores, cloud platforms, and e-commerce hubs, to reach customers efficiently. They also rely on the possibility of acquisition as a critical exit path and funding mechanism. And in fast-moving sectors like artificial intelligence (AI), they need the ability to move quickly, without regulatory uncertainty casting a shadow over every transaction.

Unfortunately, the interests of large, well-funded competitors, not consumers—and certainly not small business innovators—are too often the driving force behind antitrust debates. AICOA and the Open App Markets Act (S. 2153, 119th), for example, would prohibit COMs from performing basic marketplace management functions that create trusted ecosystems for small business innovators. The bills would treat platform design choices that benefit consumers and small sellers alike as anticompetitive conduct, just because a small handful of the largest competitors say they are inconvenienced.

Meanwhile, the European Union's Digital Markets Act (DMA) has shown what happens when regulators prioritize specific competitors over consumers. Platforms are forced to set aside security and privacy protections to open up infrastructure, leading to reduced trust, slower innovation cycles, and fewer choices for consumers and startups. All of this translates to higher costs for small business innovators.[1]

[1] ACT | The App Association, The Hidden Cost of AI Regulations for EU and UK Startups and SMEs, Oct. 2025, available at https://actonline.org/the-hidden-cost-of-ai-regulations-a-survey-of-eu-uk-and-u-s-companies/ (finding that the European Union's digital regulations cause delays in newer technologies that cost small tech businesses between $109,000 and $375,000 on average).

Mergers and Acquisitions (M&A)

Enforcers have grown reflexively hostile to tech acquisitions, treating them as presumptively harmful rather than as legitimate growth pathways. For a startup founder seeking to scale, sell, or bring on strategic partners through an acqui-hire (where a larger company acquires the startup primarily for its team and intellectual property) this regulatory hostility is paralyzing. In dynamic markets, a barrier to exit is a barrier to entry.

Why Antitrust Policy Matters to Startups, Scaleups, and Small Businesses

MISMATCHED MARKETPLACE REGULATION AND ENFORCEMENT

Startups in the app economy choose to distribute software and other goods and services through COMs because they provide an advantage in three areas:

01.
Immediate access to global markets and consumers.

02.
Built-in consumer trust in the COM and in the businesses distributing through it.

03.
Offloading overhead costs to free up resources on the core aspects of startups' businesses.

These benefits are critical for small businesses in the app economy. They enable our members to compete with companies of all sizes and reach customers across the United States and around the world. However, many of the competition policies under consideration would tear down the services and capabilities that small businesses need to compete. Small businesses want COMs to continue to improve and expand these benefits, but unfortunately, much larger competitors are spamming policymaker inboxes with requests to undermine or completely eliminate COMs' ability to offer these benefits.

More well-resourced interests want policies that would harm trustworthiness by mandating unfettered access to digital shelf space as well as mobile smart device functionalities such as access to camera and microphone, and even personal information like precise location. This forced distribution and access regime would leave consumers to fend for themselves, resulting in consumers turning away from small business developers without a trusted, recognizable brand and removing platform-provided legal, tax, and trade support.

M&A Policy

Merger review has become a barrier to startup growth and liquidity. Enforcers at the Federal Trade Commission (FTC) and Department of Justice (DoJ) have adopted an aggressive posture toward tech acquisitions, scrutinizing transactions that pose no plausible threat to competition and imposing lengthy review timelines that kill deals.

This is especially damaging in fast-moving sectors like artificial intelligence, where timing is everything. An AI startup that develops a breakthrough model needs to move quickly either to raise capital, partner with a larger firm, or be acquired outright. If the regulatory process drags on for months, the competitive window closes. Competitors catch up, the technology becomes commoditized, and the acquisition target loses its strategic value. Small businesses need enforcers to adopt a more balanced approach that distinguishes between harmful consolidation and pro-competitive transactions.

Acqui-hires and strategic partnerships are critical funding mechanisms that current policy threatens. Not every startup is destined to become a standalone unicorn. Many founders build a talented team and innovative technology but lack the business model or market position to scale independently. In these cases, an acqui-hire provides a valuable exit. The founders get liquidity, the acquiring company gains talent and technology,

and the team's work finds a broader audience. Yet the current enforcement climate treats acqui-hires with suspicion, as if they are anticompetitive by definition. This is backward. Acqui-hires are a feature of a healthy innovation ecosystem, not a bug. Small businesses need policymakers to recognize that not all acquisitions are about eliminating competition. Some are about enabling it.

What Startups, Scaleups, and Small Businesses Need from Policymakers

Small technology companies need a competition policy framework that distinguishes between genuine anticompetitive conduct and legitimate business practices that benefit consumers and developers alike. That means rejecting legislative proposals that dismantle COMs, adopting a balanced approach to merger review that recognizes acquisitions as pro-competitive growth pathways, and resisting the temptation to import European-style access mandates that fragment ecosystems and harm small developers. Above all, it means remembering that antitrust enforcement exists to protect competition and consumers, not competitors.

Specifically, ACT urges Congress and federal enforcers to:

01.
Reject legislation, like AICOA, that would prohibit basic marketplace management practices and undermine the consumer trust small businesses lean on to reach customers.

02.
Pursue trade levers that explicitly oppose the spread of DMA-style access mandates and interoperability requirements that impose compliance costs on small developers and fragment app ecosystems.

03.
Focus enforcement on actual consumer harm rather than competitor protection, and distinguish between anticompetitive conduct that forecloses market access and legitimate business practices that improve user experience and help small developers succeed.

04.
Ensure that antitrust policy does not inadvertently privilege large, well-funded competitors at the expense of startups, scaleups, and small businesses that make up the app economy.

05.
Recognize that the possibility of acquisition is a critical driver of startup formation and early-stage investment, and that aggressive enforcement postures cast a shadow of uncertainty over transactions, harming the entire innovation ecosystem.

06.
Adopt a balanced approach to merger review that recognizes acquisitions, including acqui-hires and strategic partnerships, as beneficial growth pathways for startups, rather than treating all tech transactions as presumptively harmful.

07.
Ensure merger review timelines are swift and predictable, particularly in fast-moving sectors like markets around AI, where delays can destroy the strategic value of a transaction and close competitive windows for small companies.

Standard-Essential Patents

The United States is home to a huge array of talented and innovative small businesses that benefit from strong patent protections and build on technical standards. This system has worked for years, encouraging interoperability and innovation. The America Invents Act (AIA) has played an important role, helping to weed out overly broad patents with robust post-grant review processes at the United States Patent and Trademark Office (USPTO). Unfortunately, recent policy changes by USPTO and proposals in Congress threaten to undo the progress made to strengthen patent protections and turn back the clock to policies that enable, rather than stop, harmful litigation that preys on small business innovators.

Similarly, a handful of patent holders are hijacking the standards system through abusive standard-essential patent (SEP) licensing practices, creating a barrier to innovation and economic growth. Technical standards provide common protocols that serve as a baseline for products to interoperate. As standards are built,

companies often voluntarily contribute patents to a standard that must be practiced in order to use a standard, referred to as SEPs. In return for accepting a patent into a standard (making it a SEP), patent holders commit to license their SEPs to any willing licensee on fair, reasonable, and non-discriminatory (FRAND) terms.

Why Patent and SEP Policy Matters to Startups, Scaleups, and Small

STANDARD-ESSENTIAL PATENTS

Trusted standards-setting organizations (SSOs) convene stakeholders from around the ecosystem to develop standards, which promote interoperability between products and services and ensure safety and efficacy. Because standards establish a baseline to innovation, small businesses need to utilize them to compete in the market. Additionally, this interoperability allows small businesses to focus on what they do best rather than having to build an entire stack of solutions for every product.

A SEP confers significant market power on a SEP holder since they, by definition, control access to any market the standard serves. Recognizing this, SSOs have introduced requirements for SEP holders who voluntarily choose to participate in standardization to commit to license those SEPs to all on FRAND terms. This FRAND commitment mitigates the potential of SEP holders to abuse their inherently dominant

position and prevent the same from excluding or gouging innovators that need to use standards. FRAND promises are a vital check on anticompetitive abuse and ignoring them can constrain competition and harm consumers.

Legislation like the Realizing Engineering, Science, and Technology Opportunities by Restoring Exclusive (RESTORE) Patent Rights Act (H.R. 1574, S. 708, 119th) threatens small businesses' ability to leverage standards. Specifically, the bill would undo the Supreme Court's eBay test under which federal courts determine whether and in which circumstances grant of an injunction is appropriate and replace the rule with a default to injunctions. Additionally, the USPTO and Department of Justice have attacked the eBay precedent in recent statements of interest filed with federal courts. Notably, this is the wrong approach for FRAND-encumbered SEPs because SEP holders have, as part of the FRAND commitment, voluntarily traded their right to exclude willing licensees for the ability to license to any implementer of the standard.

U.S. competitiveness and national security hinge on the ability to protect businesses from SEP abuses and ensure diverse supply chains. SEP abuses put the nation at greater risk by enabling a handful of licensors to abuse their dominant positions as SEP holders and weaken U.S. supply chains by forcing American businesses to rely on fewer suppliers of critical components. Chinese companies have a demonstrated track record of buying up large volumes of SEPs and engaging in anticompetitive SEP licensing practices that have and will continue to force out other suppliers if U.S. enforcers fail to stop them. Support for well-established SEP law and policy principles that make sure SEP holders stick to their FRAND promises is needed to maintain U.S. leadership in standards and to prevent abuses by foreign competitors.

PATENTS

Artificial intelligence (AI) has dramatically improved the efficiency of all kinds of applications, including for patents. A wave of lower-quality applications is crashing over USPTO, and while examiners at the agency are working hard, newer technologies like generative AI can make it difficult to judge quality. It is more important than ever for USPTO to maintain robust post-grant review processes where improperly granted patents can be rightfully invalidated.

What Startups, Scaleups, and Small Businesses Need from Policymakers

01.
Oppose the RESTORE Patent Rights Act, which would enable SEP abusers and block small business innovators from being able to leverage technical standards effectively.

02.
Promote technical standards-driven innovation and SSO-developed FRAND commitments by implementing national mechanisms to support and restrict harmful licensing tactics involving SEPs.

03.
Support the Promoting United States Leadership in Standards Act of 2025 (S. 1269, 119th) which would support U.S. competitiveness and national security through improved access to standards participation, including for small businesses.

04.
Reinforce that violations of FRAND commitments harm competition and small business.

05.
Congress and the administration must support patent review processes at the Patent Trial and Appeal Board (PTAB) to ensure American business is not overwhelmed by a wave of costly litigation defending frivolous patents.

Federal Tax Incentives and Small Business Innovation Research Funding

For America's app economy startups, scaleups, and small businesses, tax policy is not an abstraction. It is the difference between surviving a few bad quarters or shutting down, between hiring a fifth engineer or plateauing at four, and between scaling into a federal contract or staying stuck in bootstrap mode. Over the past three years, federal tax policy has lurched from punitive to partially remedied, leaving small tech firms in a state of whiplash.

The Research and Development (R&D) Tax Deduction

The 2017 Tax Cuts and Jobs Act (TCJA) delivered meaningful relief for pass-through businesses and investors, but it also introduced a poison pill that began choking startups in 2022: the mandatory capitalization and amortization of Section 174 research and development (R&D) expenses. Instead of deducting R&D costs in the year they were incurred, as companies had done for decades, startups were suddenly forced to spread those deductions over five years for domestic R&D and 15 years for foreign R&D. For cash-strapped companies running on venture capital fumes or bootstrapped revenue, this was catastrophic. It turned profitable companies into tax liabilities overnight and made the already-difficult work of innovation economically untenable.

After years of advocacy by ACT and allies including through ACT's Small Software Business Alliance (SSBA), Congress finally acted in 2025, reinstating the immediate deduction of R&D expenses and providing retroactive relief for small businesses from tax years 2022 through 2024. This was a hard-won victory, but the work is not done. The IRS must now issue timely, clear guidance on how small businesses can actually access those retroactive deductions and do so in a way that does not penalize firms for tax positions they took in good faith under the old, broken rules.

The Small Business Innovation Research (SBIR) / Small Tech Business Tech Transfer (STTR) Programs

Meanwhile, Congress recently preserved another critical part of the startup ecosystem, the SBIR and STTR programs. These programs provide early-stage funding that allows small tech companies to prototype solutions, land federal contracts, and scale into viable government partners. We appreciate Congress's agreement in April to reauthorize these programs with measures that strike a balance between supporting innovation and the needs of small businesses with program integrity.

Why Innovation Incentives Matter to Startups, Scaleups, and Small Businesses

The reinstatement of immediate expensing of R&D under Section 174 is a lifeline, but only if the IRS

makes it workable. Startups operate in a world of tight margins, quarterly survival calculations, and tax advisors who charge by the hour. Retroactive relief spanning three tax years is complex by definition, and small businesses need clear answers on the thorniest questions: How do companies that filed under the old amortization regime claim refunds? What documentation is required? Will amended returns trigger audits or penalties for firms that reasonably interpreted an ambiguous law? The IRS has not always issued guidance that speaks to the realities of small business operations. Too often, the agency writes for Fortune 500 tax departments, not for the two-person accounting team at a 15-employee software company. ACT urges the IRS to issue plain-language guidance that answers these questions and provides a safe harbor for taxpayers who acted in good faith under the prior capitalization regime. Delay is not neutral. Every month without clarity is a month that small businesses cannot access capital they are owed.

Beyond immediate relief, Congress must ensure that the R&D deduction remains permanent and does not revert to amortization in future years. The reinstatement legislation was a critical fix, but the app economy needs certainty, not a perpetual legislative cliff. Startups cannot plan hiring, investment, or growth strategies around a tax code that might change every two years based on the national budget. Congress made immediate R&D expensing a permanent feature of the tax code in 2025. However, there will always be temptations to undo tax incentives like these, and Congress must continue to hear from companies that are benefiting from the provisions. Stability is a competitive advantage; uncertainty is a tax on innovation.

What Startups, Scaleups, and Small Businesses Need from Policymakers

R&D DEDUCTION

The app economy cannot afford more tax uncertainty. Congress and the IRS have an opportunity and an obligation to lock in the recent R&D deduction victory and preserve the pro-growth tax architecture that has allowed small tech companies to compete, scale, and hire. Startups, scaleups, and SMEs need policymakers to act decisively on the following:

01.
Direct the IRS to issue plain-language guidance on how small businesses can claim retroactive R&D deductions for tax years 2022–2024, including safe harbor provisions for taxpayers who acted in good faith under the prior capitalization regime.

02.
Oppose any future proposals to re-impose capitalization or amortization requirements on R&D expenses, which would undermine the competitiveness of U.S. small tech firms.

03.
Monitor IRS implementation of the retroactive R&D deduction and hold the agency accountable for timely, accessible guidance that reflects the operational realities of small businesses.

The Wearable Equipment Adoption and Reinforcement and Investment in Technology Act

Doctors, patient groups, and consumers support using health saving accounts and flexible spending accounts (HSAs/FSAs) to cover wearable devices that track multiple parameters and have multiple marketed health functions. As health technology evolves, Congress must address the needs of patients and their caregivers by allowing coverage of devices and software that can manage or collect physiologic data, such as heart rate, pulse oximetry, blood glucose, EKG, and activity levels. These measures are directly linked to chronic conditions and diseases such as COPD, heart failure, diabetes, atrial fibrillation, and hearing loss. However, current policy around HSAs/FSAs generally limits coverage for medical devices to ***single-use*** **devices.** As a result, current Internal Revenue Service (IRS) policy only recognizes a few wearable devices as eligible: WHOOP (fitness tracker), Oura Ring (sleep tracker), and Aura Strap 2 (body composition tracker). Unfortunately, this case-by-case approach encourages the purchase of **several, separate, covered devices** marketed for **single** functions instead of a **single device** that has multiple functions.

The WEAR It Act (H.R. 4203, 119th) would help address this issue by clarifying that HSA/FSA reimbursement includes certain wearable devices and associated software that track multiple parameters and use physiologic data to diagnose, cure, mitigate, treat, or prevent diseases and conditions for more than a single purpose.

Reps. David Schweikert (R-AZ), Ami Bera (D-CA), and Eugene Vindman (D-VA) introduced the WEAR IT Act in June of 2025.

Why Access to Wearables Matters to Startups, Scaleups, and Small Businesses

01. WE NEED COVERAGE FOR SOFTWARE, NOT JUST DEVICES

So far, the IRS has only allowed for coverage of a few devices and their native apps. Many smaller health tech businesses don't have the manufacturing or marketing capacity to design, build, and market their own devices in competition with big national brands. Instead, many design software that works on top of the existing devices. These businesses will lose out on customers for their products if only the device qualifies for reimbursement.

02. INDIVIDUAL COVERAGE IS COSTLY

While large companies with significant funding have the money and legal firepower to navigate the difficult IRS process for reimbursement approval, small businesses do not. We need Congress to move this process away from a case-by-case approach to ensure all devices and software that fit the criteria are covered, not just those with enough money to get the IRS's attention.

03. WE CAN'T AFFORD INNOVATION AT THE SPEED OF GOVERNMENT

In addition to being costly, the current process for approval is inefficient and time-consuming. Small businesses innovate at a rate that would make individual approvals for every device or new software application unsustainable. The WEAR IT Act would **future proof the process,** ensuring that new innovations are covered.

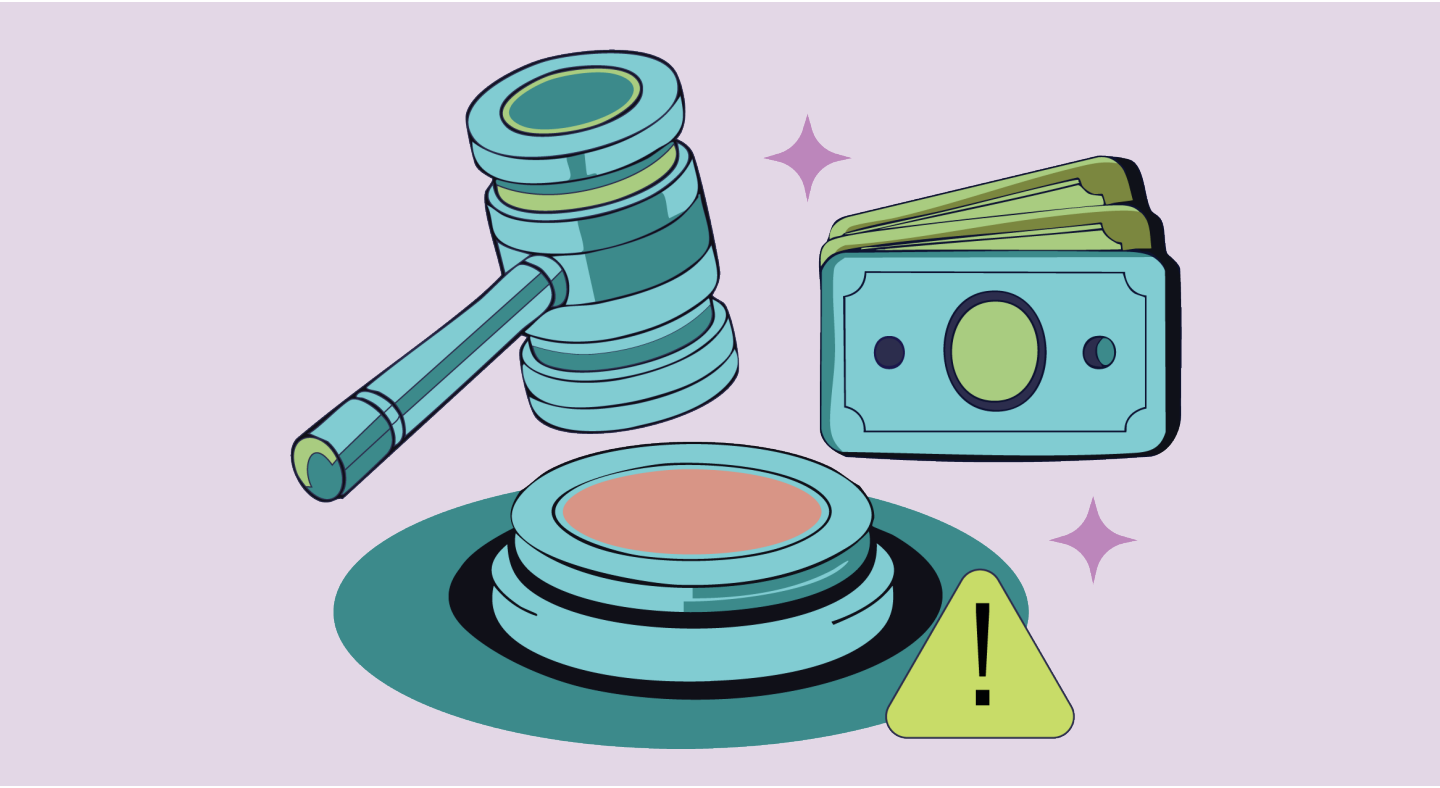
What Startups, Scaleups, and Small Businesses Need from Policymakers

01.

Cosponsor and support passage of the WEAR IT Act.

02.

The IRS has some authority to declare certain wearable devices eligible for FSA and HSA expenditures, if they are used for the "prevention" of disease. Congress should conduct oversight of the IRS and ensure that it takes the necessary steps to update its interpretations of current law.



Digital Health Policy Essentials

COVERAGE AND PAYMENT

Coverage and payment policy rules the day in American healthcare. How and whether public and private insurers cover digital health tools, plus clinicians' time and other input costs associated with using them, will decide whether the U.S. healthcare system can sustain itself or go bankrupt.

INTEROPERABILITY AND INFORMATION BLOCKING

In order for digital health to successfully curb costs and improve quality of care, patients must be able to access their own data. Thanks to digital health tools and the AI that powers them, patients and consumers have more control than ever over their own health outcomes. However, legacy barriers already expressly prohibited in federal legislation persist. Without the portability and interoperability of their health records, the benefits of digital health will remain out of reach.

PRIVACY AND SECURITY

Federal policy must ensure patients' access to their own records, but not at the cost of their privacy. The most accessible and interoperable health data is useless unless it is adequately protected from unauthorized access and from harmful uses that subvert consumers' expectations. In large part because the United States lacks a single, federal privacy law, lawmakers perceive gaps in privacy law coverage and have enacted patchworks of privacy requirements.

Why Digital Health Policy Matters to Startups, Scaleups, and Small Businesses

COVERAGE AND PAYMENT

Medicare accounts for over $1 trillion in healthcare expenditures and is the largest insurer in the United States. The policies the Department of Health and Human Services (HHS) sets for Medicare reverberate throughout the health ecosystem and are foundational elements of private insurer coverage and payment decisions. Thus, it is critical for HHS and Congress, as the authorizer of HHS activities, to ensure that Medicare covers the use of digital health tools, from remote physiologic monitoring to artificial intelligence (AI) tools.

INTEROPERABILITY AND INFORMATION BLOCKING

The federal Health Information Portability and Accessibility Act (HIPAA) sought to empower patients to port their health data from one provider to another. Unfortunately, some electronic health record (EHR) companies working for health providers continue to systematically block the flow of healthcare data, including patients' access to their EHR records. To bolster HIPAA's portability mandate, Congress enacted the 21st Century Cures Act, which specifically prohibits EHR companies from "information blocking" practices that deny patients access to their own records. In order for AI to successfully play the integral role it is destined for in healthcare, health data must flow throughout the healthcare ecosystem and enable patients to access their own records.

PRIVACY AND SECURITY

While HIPAA is designed to mandate portability of health records, it also authorizes HHS to protect patient privacy and security. HIPAA's privacy rules apply specifically to "covered entities" that process health insurance claims and their "business associates (BAs)" that carry out activities on their behalf. Because HIPAA is entity-based, it applies only to core health businesses and organizations and does not apply to digital health companies, except to the extent they are BAs or process insurance claims themselves. In the absence of a federal general policy law, states have created a patchwork of general and health-specific privacy laws to regulate digital health companies. This leaves small business digital health firms to manage compliance across a wide range of privacy frameworks that apply to consumer health in a variety of ways.

What Startups, Scaleups, and Small Businesses Need from Policymakers

In order to ensure that patients, providers, and the healthcare ecosystem as a whole can make beneficial use of digital health and AI tools, we recommend the following:

01.

Support modernization of HHS' approach to software and connected health solutions.

02.

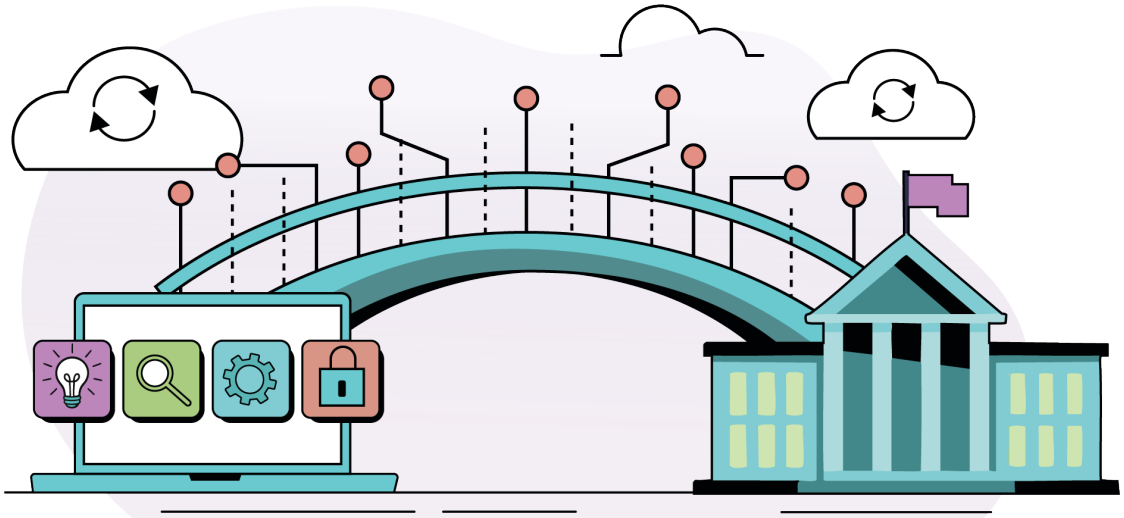
Encourage HHS to enforce the information blocking rules vigorously and ensure that EHR companies honor their responsibilities to patients.

03.

Reintroduce and cosponsor the Better Interoperability for Devices (BID) Act (H.R. 1557, 118th), to empower the Food and Drug Administration with a clear picture of the state of data interoperability across devices in and out of the care setting and with EHR systems.

04.

Enact a federal, risk-based consumer privacy law calibrated to address the heightened privacy and security risks associated with sensitive health information that covers digital health activities outside the scope of HIPAA.



GLOBAL APP ECONOMY CONFERENCE

For more information on ACT, please visit our website.
actonline.org