Dear U.S. Policymakers:

We, the members of ACT, are innovative small technology businesses and independent developers driving growth and competition in the global digital economy. From AI-enabled tools, IoT-driven solutions, encrypted services, safer online experiences, and standards-based technologies that enable interoperability, our teams build consumer and enterprise products that solve everyday problems.

However, to continue building innovative products, creating jobs, and powering the digital economy, startups and small businesses like ours need a regulatory environment that rewards innovation and provides the market certainty required to sustain investment. For small tech, policy volatility does not remain confined to legislative text or agency dockets, it quickly becomes a material business constraint.

When lawmakers don't consider small businesses in the regulatory process the impact is felt immediately. Unclear, fragmented, or overly expansive regulations cause burdensome compliance costs, delayed product development, and increased liability exposure. But the downstream consequence is often even more damaging. As compliance roadblocks mount and timelines become harder to predict, investors view the policy environment as an added risk, causing capital investment to pause or interest to disappear altogether. For startups and independent developers, that shift can determine whether a company can survive long enough to compete. This is not only a challenge for small tech companies, but also a competitive challenge for the United States. An investment environment characterized by regulatory uncertainty weakens the broader innovation pipeline that the U.S. relies on to lead in emerging technologies.

As policymakers consider proposals aimed at some of our larger counterparts, we urge balanced, forward-looking approaches that do not impose disproportionate burdens on small tech innovators. Sound policy should establish clear expectations, practical paths to compliance, and scalable rules that strengthen trust and security while preserving the conditions for small businesses to attract investment and compete. Below is an outline of our top policy priorities for U.S. leadership at the local, state, and federal levels in 2026.

Market Access and Capital Formation

> For small businesses and independent developers, growth depends on two things: the ability to access capital and reach customers. Digital trade rules that protect cross-border data flows and prevent discriminatory or protectionist barriers are essential for U.S. small tech companies competing in global markets.
>
> At the same time, capital formation in the digital economy depends on predictable pathways to scale and achieve liquidity, particularly through pro-competitive mergers and acquisitions. For startups, a barrier to exit is a barrier to entry. When merger policy

becomes overly expansive, slow, or unpredictable, it doesn't simply affect dealmaking at the end of a company's journey. It raises perceived risk at the beginning, reducing investor appetite, tightening terms, and leaving small businesses with fewer viable options to finance growth, hire, and bring new products to market.

Member Ask: Policymakers should reassert U.S. leadership on digital trade by defending cross-border data flows, resisting data localization mandates, and reducing unnecessary barriers to global market access for small businesses. Policymakers should also ensure that merger policy is grounded in demonstrated harms and provides clearer, more predictable review processes, so that pro-competitive deals are not discouraged, and small innovators can access the investment needed to scale and compete globally.

Age Verification

We support measures that protect children online from privacy violations and harmful content. However, dozens of age-verification mandates at the state and federal levels equate "protection" with data collection by requiring the surrender of IDs, birth certificates, and biometrics. Some ACT members use age assurance services as part of their efforts to address age-related risks and requirements. Age verification is the most restrictive and definitive level of age assurance, requiring the most intrusive level of data collection and posing the greatest risk among age assurance methods. For this reason, age verification is typically reserved only for situations where it is needed and to restrict access to categories of content that pose the most significant age-related risks. Similarly, even lower levels of age assurance present risks because some data collection is involved. Conducting any level of age assurance is typically considered an unnecessary risk if it is proposed for services, products, or goods that themselves present no specific age-related issues.

As a result, sweeping age assurance mandates, especially those that insist on higher levels of assurance like verification, on broad lines of business or categories of content pose unnecessary risks while providing no concomitant child protection benefits. That approach raises breach risk and actually increases the real-world harm users face when (not if) a breach occurs. Recent state-level and congressional proposals would also impose massive compliance and liability burdens on virtually any entity with a mobile app. This web of age assurance and verification mandates threatens to put ACT members between an age verification rock and an existing kids' privacy law hard place. For these companies, a failure to balance the potentially competing requirements on assuring age and protecting privacy could result in a liability quagmire that turns them away from solving real-world problems and creating app economy jobs.

Member Ask: Any child-safety policy that lawmakers at the state and federal levels consider should minimize data collection, reduce patchwork compliance burdens, and

target risk where it is highest. Protecting kids online should not require building a surveillance infrastructure that puts users, especially children, at greater risk.

Artificial Intelligence

Small businesses and independent developers are driving AI innovation across sectors, building tools that improve services, strengthen security, and increase productivity. But in the United States, the policy environment is moving in the wrong direction. Without a clear, risk-based federal AI framework, states are creating a fragmented landscape, which small businesses lack the resources or large compliance teams to navigate. The burden is greatest when requirements dictate how AI systems must be built, not just how they are used, forcing costly re-architecture or state-by-state versions that small teams simply cannot sustain.

This patchwork is exacerbated by the AI talent gap in the United States. Startups rely on highly specialized technical workers, including H-1B professionals, to build and deploy responsible AI. When workforce bottlenecks tighten while fees and compliance demands multiply, participation narrows to only the largest firms, and U.S. competitiveness suffers.

Member Ask: Congress should establish a clear federal baseline with risk-based obligations and a practical path to compliance for small businesses. States should avoid conflicting AI mandates that deepen fragmentation. Congress should also address H-1B and other talent pipeline constraints to enable startups to access the expertise needed to compete, scale, and lead in the global AI economy.

Competition and Curated Online Marketplaces

Curated online marketplaces (COMs) provide services that allow startups and independent developers to grow their businesses by reducing distribution friction, building consumer trust, and providing secure infrastructure. However, many U.S. proposals, like the App Store Freedom Act (ASFA) and the Open App Markets Act (OAMA), are targeting COMs by increasingly borrowing from the EU's Digital Markets Act (DMA) playbook. By pushing sideloading, alternative app stores, and broad access mandates, these kinds of proposals will limit how marketplaces manage security, payments, fraud, and consumer trust. The lessons learned from the EU show that when "gatekeeper" regulations seek to prohibit the services and management functions small businesses rely on most, ACT members bear the costs while their largest rivals are able to weather that storm. Similarly, when these COM services shrink to fit shifting DMA enforcer requirements and expectations, the downstream impact lands on small developers first. Workflow and API changes, onboarding rebuilds, and sudden compliance pivots create delays that can reshape an entire release cycle.

Member Ask: Any competition reforms that lawmakers consider should strengthen choice without weakening the safeguards that make curated marketplaces work. Congress and enforcers should avoid DMA-style mandates that require sideloading or broadly restrict marketplace protections, and instead advance targeted, evidence-based solutions with clear guidance and workable timelines.

Standard-Essential Patents

Standards for interoperability and safety provide a baseline for competition and innovation across consumer and enterprise markets. As small tech companies increasingly innovate in rapidly advancing fields like AI and the internet of things (IoT), many are not only implementing standards, but also contributing to the next generation of standardized technologies.

When standards include patented technology and the standard cannot be used without exercising the patent, they become standard-essential patents (SEPs). Because SEP holders are inherently positioned as arbiters of who can and cannot use the standard, standards bodies require those choosing to contribute their patents to a standard to license them to all on fair, reasonable, and non-discriminatory (FRAND) terms. A licensing framework that advances transparency, fairness, and predictability by ensuring that FRAND promises are kept is therefore crucial for ensuring small businesses can indeed use standardized technologies to interoperate and compete.

Unfortunately, some SEP holders who have voluntarily contributed their patents to a standard aren't living up to their commitments. When SEP holders break their promises to license on FRAND terms, it harms competition and creates significant problems for small innovators. SEP licensing rules must work for both sides of the ecosystem by guaranteeing the ability to use standardized technologies while ensuring fair and reasonable compensation for the value of the SEP for licensors. A balanced SEP framework is vital to both U.S. economic and national security.

Member Ask: U.S. policymakers must support clear and balanced SEP licensing frameworks, which uphold the integrity of voluntary FRAND commitments and prevent anti-competitive SEP licensor abuses. This will empower small businesses like ours members, particularly in areas where emerging technologies like AI and IoT play a pivotal role in economic growth and consumer value.

Privacy and Encryption

Privacy is a core condition for trust in the digital economy; for startups, trust is a crucial foundation for growth. Yet the absence of a comprehensive federal privacy law continues to leave consumers and small tech navigating a fragmented, state-by-state landscape. That fragmentation drives up compliance costs, complicates product development, and makes it harder to scale across the U.S. market with confidence.

Strong encryption is inseparable from effective privacy policies. It is the technical foundation that makes privacy protections real in practice, limiting unnecessary access to sensitive data, reducing the amount of data exposed in a breach, and enabling secure communications and transactions. Proposals that weaken end-to-end encryption or mandate exceptional access do not create "balanced" safety. They create systemic vulnerability by expanding the number of points where data can be accessed, retained, or exploited.

Member Ask: Federal policymakers should enact a strong national privacy framework aligned with the "4 Ps of Privacy" that delivers clear, consistent protections and a workable path to compliance, while preempting conflicting state requirements that drive fragmentation. State policymakers should avoid expanding patchwork privacy mandates that create duplicative compliance burdens without improving outcomes. At both levels, lawmakers should protect strong encryption as essential infrastructure for privacy and trust and reject proposals that would weaken end-to-end encryption.

Connected Health

Digital health innovations are essential to improving patient outcomes, reducing costs, augmenting population health management, and supporting the healthcare workforce. Their development and uptake are particularly critical for improving both disease prevention and treatment in rural and underserved communities. While coverage and regulatory reforms have incrementally advanced across Administrations, stark issues persist that only Congress can fix.

Tens of millions of Americans already rely on health savings accounts (HSAs) and flexible spending accounts (FSAs) to manage healthcare expenses, with HSAs being used by more than 59 million Americans and FSAs available to 47 percent of private-industry workers and 72 percent of state and local government workers. Yet federal policy is woefully out of touch, restricting HSA and FSA eligibility for wearables by using an absurdly narrow definition and requiring eligibility assessments to be made on a device-by-device basis, favoring single-use tools and excluding the software subscriptions that make many wearables effective. The problem is clear: patients are not able to use their own HSA and FSA dollars to get the digital health tools they need to get healthy.

Member Ask: Congress should enact the WEAR IT Act to modernize HSA/FSA policy so eligible wearable devices and associated software can be purchased with tax-advantaged funds.

Innovation thrives when policymakers create clear, durable rules that allow businesses of all sizes to compete and succeed. Overly broad, fragmented, or unpredictable requirements raise compliance costs, delay product development, and chill the investment small tech businesses need to grow. We remain committed to working with Congress, the Administration, and state

leaders to advance these priorities and ensure that small tech can continue to create jobs and deliver real-world solutions.

Sincerely,

ACT and our members