

November 17, 2025

The Honorable Brett Guthrie
Chairman
Committee on Energy and Commerce
United States House of Representatives
Washington, District of Columbia 20515

The Honorable Frank Pallone
Ranking Member
Committee on Energy and Commerce
United States House of Representatives
Washington, District of Columbia 20515

The Honorable John Joyce
Chairman
Committee on Energy and Commerce
Subcommittee on Oversight & Investigations
United States House of Representatives
Washington, District of Columbia 20515

The Honorable Yvette Clarke
Ranking Member
Committee on Energy and Commerce
Subcommittee on Oversight & Investigations
United States House of Representatives
Washington, District of Columbia 20515

RE: Committee hearing, “Innovation with Integrity: Examining the Risks and Benefits of AI Chatbots”

Dear Chairman Guthrie, Ranking Member Pallone, Chairman Joyce, and Ranking Member Clarke,

Thank you for the opportunity to submit this statement for the record. Small businesses are leading the way on artificial intelligence (AI). As some of the leading consumers, developers, and adapters of AI tools, ACT | The App Association members have a major stake in how policymakers view AI markets. ACT represents a domestic ecosystem valued at approximately \$1.8 trillion, supporting 6.1 million American jobs.¹ ACT members are innovators that create the software bringing your smart devices to life. They also make connected devices that are revolutionizing healthcare, agriculture, public safety, financial services, and virtually all other industries. As conversational AI becomes integrated into services used by millions of Americans, including children and teens, we

¹ ACT | The App Association. *State of the App Economy*. (2023), <https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL-1.pdf>

support efforts to understand the risks and benefits of these tools and to ensure that innovation proceeds with integrity and user safety at the center.

AI is an evolving constellation of technologies that enable computers to simulate elements of human reasoning. Consumers encounter these systems incrementally, often through computer-based services that streamline processes, improve accessibility, and provide information more efficiently. Chatbots are one such interface. They enable natural language interaction and can support education, customer service, and the delivery of digital tools that benefit consumers and small businesses. At the same time, chatbots can raise unique considerations for policymakers, particularly when minors engage directly with these systems. We understand these challenges and appreciate that policymakers are looking for approaches to address them, but in doing so they should keep in mind the following principles, grounded in existing legal frameworks and designed to support continued responsible innovation by small businesses.

Existing Law Already Provides Strong Consumer Protection Guardrails

A wide range of federal and state laws already prohibit harmful conduct regardless of whether AI is involved,² and there is no AI exemption in the law. Section 5 of the Federal Trade Commission Act³ prohibits unfair or deceptive acts or practices (UDAP), and state consumer protection statutes apply similar unfair or deceptive acts or practices standards to digital services, including chatbots. These authorities reach a broad set of practices relevant to children and teens, such as misleading claims about safety, failing to mitigate reasonably foreseeable risks, implying therapeutic or clinical capabilities, or designing systems that expose minors to known harm. The Children’s Online Privacy Protection Act (COPPA) also restricts how companies collect, use, share, or retain minors’ personal data, and many state privacy laws place additional limits on selling or monetizing minors’ data or targeting them with advertising.⁴ Together, these existing frameworks already provide meaningful guardrails for chatbot providers when they make claims to users, process minors’ data, or design systems in ways that create foreseeable harms. Congress could take meaningful action by passing a comprehensive federal data privacy law, laying out a single set of rules for how companies should handle consumer data. In the absence of a federal privacy law, we urge Congress and federal agencies to continue evaluating the application of these longstanding authorities before considering new legal structures.

² How Existing Laws Apply to AI Chatbots for Kids and Teens, Georgetown Law Institute for Technology Law & Policy (Nov. 10 2025), <https://www.law.georgetown.edu/tech-institute/insights/how-existing-laws-apply-to-ai-chatbots-for-kids-and-teens/>.

³ Federal Trade Commission Act § 5(a), 15 U.S.C. § 45(a) (prohibiting “unfair or deceptive acts or practices in or affecting commerce”).

⁴ For example, **Maryland** and **Connecticut** prohibit selling or processing the personal data of minors under 18 for targeted advertising. **Louisiana** bars social media companies from selling minors data. **Oregon**, effective January 1, 2026, prohibits selling personal data of minors under 16 and gives consumers the right to request a list of third parties who received their data. States including **California**, **Colorado**, **Delaware**, **New Hampshire**, **New Jersey**, **Minnesota**, and **Montana** require affirmative consent before selling teens data or using it for targeted advertising. And nearly all state privacy laws provide consumers, including minors, the ability to opt out of targeted advertising and data sales.

A Risk-Based Framework and Shared Responsibility Model

Existing law is not applied in a vacuum. Evolving technical standards, best practices, and industry norms inform enforcers' calculus when determining whether AI deployers, users, or developers run afoul of broad laws like UDAP. Enforcers must apply the law based on the risks presented by conduct, anchored in recognized frameworks, including the National Institute of Standards and Technology (NIST) Artificial Intelligence Risk Management Framework.⁵ By relying on recognized frameworks, developers and deployers benefit from understanding the distribution of risk and responsibility in the building, testing, and use of AI tools. A shared responsibility model across the value chain helps ensure that those with the ability to minimize risks, based on their knowledge and skills, have appropriate incentives to do so. To this end, we urge that enforcement of existing law and the development of any policy proposals align with our recommendations on the roles and interdependencies in the AI value chain, which support the theme of a shared responsibility for safety and efficacy.⁶ In this framework we:

- 1) Propose clear definitions of stakeholders across the AI value chain, from development to distribution, deployment, and end use; and
- 2) Discuss roles for supporting safety, ethical use, and fairness for each of these important stakeholder groups that are intended to illuminate the interdependencies between these actors, thus advancing the shared responsibility concept.

Thoughtful Design and Clear Representations to Users

We also support thoughtful design of AI systems that account for real world workflows, human-centered design, and end user needs. Chatbots should provide truthful and clear representations regarding intended use and risks that would be reasonably understood by those expected to rely on the system. Developers should be able to document their methods and results. Deployers should adopt appropriate safeguards to reduce the likelihood that users, especially minors, will receive or act on harmful outputs. Products that involve chatbots should remain accessible and affordable for consumers, and developers should be able to build accessibility features into their offerings.

Modernized Privacy and Security Frameworks

While the types of data items analyzed by AI and other technologies are not new, this analysis will provide greater potential utility of those data items to other individuals, entities, and machines. Thus, there are many new uses for, and ways to analyze, the collected data. This raises privacy issues and questions surrounding consent to use data in a particular way (e.g., research, commercial product/service development). It also offers the potential for more powerful and granular access controls for consumers. With proper protections in place, policy frameworks should promote data access, including

⁵ National Institute of Standards and Technology. *AI Risk Management Framework*. U.S. Department of Commerce, <https://www.nist.gov/itl/ai-risk-management-framework>.

⁶ ACT | The App Association. *AI Roles & Interdependencies Framework* (May 2024), <https://actonline.org/wp-content/uploads/ACT-AI-Roles-Interdependencies-Framework-final-text-May-2024-UK-English.pdf>.

open access to appropriate machine-readable public data, development of a culture of securely sharing data with external partners, and explicit communication of allowable use with periodic review of informed consent.

Supporting Transparency, Privacy, and Mitigation of Data Bias

We also emphasize the importance of supporting research and transparency that improves safety without requiring the disclosure of proprietary information or trade secrets. Transparency mechanisms can help users understand intended use, limitations, and circumstances in which additional oversight or human judgment is needed. Data bias remains a pressing challenge for AI systems, and agencies should continue to examine data provenance and bias issues to ensure that bias does not result in harm or unlawful discrimination.

The Need for a National AI Framework to Avoid a Patchwork of State Laws

Finally, Congress should avoid a fragmented AI regulatory environment. States are already advancing a growing number of AI and chatbot-specific laws, many of which would impose overlapping or inconsistent requirements for disclosures, data practices, and risk assessments.⁷ This patchwork is already creating significant uncertainty for developers and deployers, especially small businesses that lack the resources of their larger competitors to navigate 50 different compliance regimes. Early evidence shows that even small deviations in state requirements can trigger substantial compliance costs, diverting limited resources from product development to legal review, recordkeeping, and bespoke technical implementations. Recent analyses show that state AI laws modeled on European-style precautionary approaches can impose unknown and potentially significant costs to companies,⁸ while delays in state-level implementation underscore the difficulty of managing complex AI obligations at the state level. A single national baseline is preferable to a system where the most restrictive state rules dictate outcomes nationwide. Federal preemption of conflicting state AI requirements, paired with state attorney general enforcement of that federal baseline, would give consumers clarity, reduce compliance burdens, and ensure that small business innovators can safely build and deploy conversational AI without being constrained by inconsistent or extraterritorial state mandates.

Conclusion

ACT appreciates the Subcommittee's leadership on these issues. We look forward to supporting continued oversight that protects consumers, advances responsible AI practices, and ensures that small businesses can continue contributing to American innovation.

⁷ Stevens, Morgan. "State of Confusion: How a Patchwork of AI Laws Hurts Small Businesses and U.S. Competitiveness." ACT | The App Association, Oct. 2025, <https://actonline.org/2025/10/10/state-of-confusion-how-a-patchwork-of-ai-laws-hurts-small-businesses-and-u-s-competitiveness/>

⁸ The Hidden Cost of AI Regulations: A Survey of EU, UK, and U.S. Companies." ACT | The App Association, Oct. 2025, <https://actonline.org/the-hidden-cost-of-ai-regulations-a-survey-of-eu-uk-and-u-s-companies/>.

Thank you for your consideration.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Graham Dufault". The signature is fluid and cursive, with a long horizontal stroke at the end.

Graham Dufault
General Counsel
ACT | The App Association

A handwritten signature in black ink, appearing to read "Kedharnath Sankararaman". The signature is cursive and includes a long horizontal stroke at the end.

Kedharnath Sankararaman
Policy Associate
ACT | The App Association