September 16, 2025

The Honorable Ted Cruz
Chair
Committee on Commerce, Science, and Transportation
United States Senate
254 Russell Senate Building
Washington, D.C. 20510

The Honorable Maria Cantwell
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate
254 Russell Senate Building
Washington, D.C. 20510

Re: S. 2714, the Children Harmed by AI Technology (CHAT) Act

Dear Chair Cruz and Ranking Member Cantwell,

We, the undersigned organizations, write to express our concerns with S. 2714, the Children Harmed by AI Technology (CHAT) Act of 2025, introduced by Sen. John Husted (R-Ohio).[1] Despite its noble intentions to protect children in a world of digital services, the CHAT Act would in practice do the opposite: it would endanger the privacy and data security of children and families nationwide. As artificial intelligence (AI) becomes an ever more prominent feature of modern life, the harms that would likely be imposed by the bill are especially grievous.

First, it must be noted that the CHAT Act's definition of "companion AI chatbot" is hopelessly broad, encompassing "any software-based artificial intelligence system or program that exists for the primary purpose of simulating interpersonal or emotional interaction, friendship, companionship, or therapeutic communication with a user." Of course, the distinguishing feature of many generative AI tools is their ability to interact with users in an "interpersonal" fashion—to simulate the patterns of a conversation that might be had between human beings. Therefore, the Act would cover essentially all major chatbots, including ChatGPT, Google's Gemini, Anthropic's Claude, among others.

But the Act's definition reaches still further. AI-integrated features that "simulate…interpersonal… interaction" are hardwired into many common products and devices. Among many others, the Act could regulate access to Siri (the assistant native to Apple devices), online customer-support chats, and AI-voice-enabled devices such as Amazon's Echo. It could even regulate AI-driven characters in videogames that interact with the user based on user inputs. In short, the Act would regulate countless everyday products on which Americans rely for work, recreation, and their home lives.

While the scope of the CHAT Act alone is extreme, so too are its effects on the cybersecurity and privacy of American users, which is likely to be deeply dangerous.

The CHAT Act's fundamental fault is its requirement that users of AI tools submit to age verification. Age verification requires users to submit a tremendous amount of sensitive, personal information, which then becomes stored in large databases, liable to be hacked or to fall victim to data breaches. This information usually takes the form of scans of government-issued identification documents or biometrics, such as facial scans. It would directly contradict the goal of ensuring children's safety in the digital world for the federal government to mandate that children serve up their data to technology platforms and expose that data to bad actors.

Children already face vast privacy dangers. As noted by the R Street Institute last year, "The problem is so extensive that research by Experian suggests that 25 percent of children will be victims of identity fraud or theft by the time they are 18."[2] Moreover, R Street continues, "More than half of minors who were victims of identity theft report being denied access to credit at least once because of it, and some deal with the consequences for a decade or more. Some have even acquired a lifelong criminal record for an offense committed by the thief that

[1] https://www.husted.senate.gov/wp-content/uploads/2025/09/CHAT-Act-Leg-Text2221.pdf
[2] https://www.rstreet.org/commentary/child-identity-theft-is-a-huge-problem-the-solutions-are-simple/

stole their identity." Requiring children to provide sensitive personal information to access AI tools—which are becoming ever more ubiquitous in many parts of life—would only compound these dangers.

Unfortunately, the privacy dangers of the CHAT Act do not end there. Parents would be further required to give parental consent before their children are allowed to use chatbots. While parental oversight of, and control over, their children's online lives is unquestionably desirable, the process outlined in the Act would compound risks to data security and privacy. First, the parent would have to prove his or her relationship to the child; this would inevitably require even more intrusive data gathering to prove both the identity of the parent and his or her status as the child's legal guardian.

Recent experience demonstrates the dangers of exposing large amounts of sensitive information in vulnerable databases—even those purported to be secure. In the digital age, hacks and data leaks are ubiquitous. Indeed, a Duke University analysis found that more than four in five of companies say they have dealt with a hack.[3] Tech companies—including some of the largest and best protected companies—routinely fall victim.[4] Even third-party age verifiers, which specialize in the business of age verification, also experience cyber incidents. "[T]hese services have suffered cyber events, too," as the Taxpayers Protection Alliance noted in its recent amicus brief to the Supreme Court in NetChoice v. Fitch, "Outabox, which provided facial-recognition services to various in-person businesses, announced a massive cybersecurity breach in 2024 resulting in the piracy of more than one million consumer records. AU10TIX, an identity-verification service used by recognizable platforms like Uber, TikTok, X, and LinkedIn, is another victim of cybercrime."[5] Supreme Court justice Alito may have put it best during the oral arguments in Free Speech Coalition v. Paxton: "There have been hacks of everything."[6]

Small and new developers, which often lack the disposable capital and expertise to manage large amounts of user data responsibly, would be the ones to feel the burdens of the CHAT Act especially heavily; the users of AI products designed by small and startup developers would, consequently, be especially endangered.
For example, TeaOnHer (a recently released app that allows men to share dating stories) inadvertently left sensitive user information exposed and accessible to anybody who endeavored to find it. Journalists at TechCruch accessed this information.[7] "The records returned from TeaOnHer's server contained users' unique identifiers within the app (essentially a string of random letters and numbers), their public profile screen name, and self-reported age and location, along with their private email address," TechCrunch reported. "The records also included web address links containing photos of the users' driver's licenses and corresponding selfies." The process of finding these records took about 10 minutes.

It should also be noted that regulatory burdens that fall disproportionately on upstart developers are likely to have regrettable consequences for competition. Large companies can absorb compliance costs; small companies often cannot. To ensure that America's tech sector continues to thrive, and that free competition remains robust, lawmakers should eschew policies that prevent new competitors from challenging large incumbents.

Users widely understand the cybersecurity and privacy risks attendant on age verification mandates. In the United Kingdom, which recently enacted a broad age verification mandate in its Online Safety Act (OSA), vast numbers of users flooded app stores to download virtual private networks (VPNs) to avoid the mandate. In just the first days after the OSA's provisions went into effect, VPN use skyrocketed. Proton VPN reported a 1,400-percent surge in new user registrations.[8] NordVPN reported a "1,000 percent increase in purchases," and many other VPNs reported increased user demand.[9]

There is a better way forward. Instead of rushing to impose ill-fitted and likely dangerous regulations on AI tools and their users, lawmakers investigate how existing laws, and existing legal frameworks can best be applied to the

[3] https://cfosurvey.fuqua.duke.edu/press-release/more-than-80-percent-of-firms-say-they-have-been-hacked/
[4] https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html
[5] https://www.protectingtaxpayers.org/press/watchdog-group-files-amicus-brief-defending-mississippian-social-media-users/
[6] https://www.supremecourt.gov/oral_arguments/argument_transcripts/2024/23-1122_7m58.pdf
[7] https://techcrunch.com/2025/08/06/a-rival-tea-app-for-men-is-leaking-its-users-personal-data-and-drivers-licenses/
[8] https://x.com/ProtonVPN/status/1948773319148245334
[9] https://www.wired.com/story/vpn-use-spike-age-verification-laws-uk/

digital age. Over the course of the nation's history, the U.S. has developed a large body of law to mitigate consumer harms, and this tradition should not be shelved or bypassed with respect to digital technologies. The way forward should be seen as an evolution, not a revolution; the dangers of the latter approach are illustrated above.

Moreover, many consumers—of all ages—are still adjusting to AI and other digital technologies due to the simple fact that these technologies are very new, and consumer knowledge and understanding are still lacking. The education of American users, parents, children, and families will be a crucial development in the navigation of new technological waters.

AI is too promising of a technology to be badly regulated. Lawmakers should avoid imposing policies that would force users to submit to cybersecurity and privacy dangers as a precondition of using everyday digital services. America is a free country, and its freedom has made it the world's leading economy and given it the world's leading technology sector. Of course, as new problems arise, it may be necessary to respond, but the CHAT Act seeks to set the country on a dangerous and unsustainable path.

Sincerely,

David Williams
President
Taxpayers Protection Alliance

Taylor Barkley
Director of Public Policy
Abundance Institute

Logan Kolas
Director of Technology Policy
The American Consumer Institute

Adam Kovacevich
Founder & CEO
Chamber of Progress

Jessica Melugin
Director of the Center for Technology & Innovation
Competitive Enterprise Institute

James Czerniawski
Head of Emerging Technology Policy
Consumer Choice Center

Vance Ginn
President
Ginn Economic Consulting

Ash Johnson
Senior Policy Manager
Information Technology and Innovation Foundation

Caden Rosenbaum
Senior Policy Analyst
Libertas Institute

Amy Bos
Director of State and Federal Affairs
NetChoice

Daniel J. Erspamer
CEO
Pelican Institute for Public Policy

Mark Dalton
Director of Technology & Innovation Policy
R Street Institute

Stacie Rumenap
Founder & CEO
Stop Child Predators