TECHNET
THE VOICE OF AMERICAN INNOVATION

TechNet Mid-Atlantic | Telephone 717.585.8622
P.O. Box 203, New Cumberland, PA 17070
www.technet.org

November 10, 2025

The Honorable David Argall
Chair
Senate Republican Policy Committee
Pennsylvania Senate
177 Main Capitol Building
Harrisburg, PA 17120

RE: Artificial Intelligence

Dear Chairman Argall and Members of the Committee,

On behalf of TechNet, I'm writing to share comments on how businesses are helping to mitigate the harmful effects of artificial intelligence impacting minors.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes 104 dynamic American businesses ranging from startups to the most iconic companies on the planet and represents five million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

Artificial intelligence (AI), machine learning (ML), and the algorithms that often support artificial intelligence have generated significant policymaker interest. We acknowledge that as technological advances emerge, policymakers' understanding of how these technologies work is vital for responsible policymaking. Our member companies are committed to responsible AI development and use. TechNet will advocate for a federal AI framework that brings uniformity to all Americans regardless of where they live, encourages innovation, and ensures that consumers are protected.

TechNet and its member companies are committed to providing a safe experience for children and adults who use their products online. As a trade association, TechNet speaks for all of our members. For the purposes of today's hearing, TechNet will be using data from some of our members' public reports; however, it is important to note that we represent several additional companies not explicitly mentioned. Committee members can view the full list of our members on TechNet's website.

Keeping children safe online from the harms of artificial intelligence is a multi-faceted approach including business practices, parental involvement, and education and digital literacy.

Business Efforts to Combat Negative Effects of AI

Child Sex Abuse Material (CSAM)

A growing concern among policymakers is the prevalence of child sex abuse material, or CSAM, and the role AI can play in its creation and dissemination. Our member companies prohibit CSAM on their platforms and have a federal mandate to report any CSAM to the National Center for Missing & Exploited Children (NCMEC). Platforms do not allow content that endangers or sexually exploits children. When platforms discover these types of content, they remove it, regardless of the context or the bad actor's motivation to share it. Our member companies may also disable the account of the person who shared it if it was believed to be with malicious intent.

Our member company, Meta, acts on adverse content in a variety of ways, such as removing a piece of content from their platforms, covering photos or videos with a warning that says some content may be disturbing to certain audiences, or disabling accounts. When Meta acts on a piece of content, they label the content with the policy it violated.

Another member company, Amazon, has a suite of services, tools and technology to identify and remove CSAM. Those technologies include machine learning, keyword filters, automated detection tools, and human moderators to screen images, videos, or text in public-facing content for policy compliance before it is allowed online. These measures enforce multiple policies, including prohibitions on CSAM, and they appear to be an effective deterrent, as reflected in the lower number of reports for CSAM. As one example, Amazon Photos uses Thorn's Safer technology to detect hash matches of images uploaded to the service and verifies positive matches using human reviewers. Amazon also makes Thorn's Safer technology available to businesses via the Amazon Web Services (AWS) Marketplace so they can proactively identify and address CSAM.

Depending on the specifics of the service, Amazon will remove or disable, as applicable: URLs, images, chat interactions, resources, services, or accounts. In 2024:

- Amazon and its subsidiaries collectively submitted 64,195 reports of CSAM to NCMEC in 2024. These reports related to content found in 3,959 accounts.
- Amazon Photos reported 30,778 images (affecting 3,758 accounts) using Safer—a 24.8% increase year over year. As part of their commitment to safeguard their large language model (LLM) datasets from CSAM and responsibly host models, they automatically detected and reported 30,744 pieces of content.
- Amazon received 337 reports from third parties for potential CSAM content including chat interactions and URLs. Hotlines, such as those administered

by NCMEC, IWF, Canadian CyberTipline, and INHOPE, submitted a total of 752 reports (in 273 accounts) for content that they promptly reviewed and actioned as appropriate (average time to action any hotline report was 2.6 days). For all content reported by hotlines, they found 391 were CSAM (relating to 200 accounts), actioned them, and reported them to NCMEC. For reports involving AWS customers, customers resolved the issue without additional intervention 87% of the time.

In Amazon's models, they scan for known CSAM on data sets that are used to build their generative AI models and remove and report that content to NCMEC. They design and test their models and generative AI applications to reduce the risk that they will produce exploitative content. Amazon Bedrock makes models available for customers to use and train. This product includes automated detection for known CSAM and rejects and reports positive matches. Additionally, customers can configure Amazon Bedrock Guardrails to provide additional protections, including for sexual content, and help enforce their own acceptable use policies.

Amazon also provides NCMEC millions of dollars in AWS technology and services to reliably operate mission-critical infrastructure and applications to help missing and exploited children. In 2024, Amazon continued to provide financial support to NCMEC's Exploited Child Division to advance their hash sharing and Notice and Tracking initiatives that help remove CSAM from the internet. Amazon continues to partner closely with Thorn, including by providing millions of dollars in free advanced cloud services and technical support from AWS for Thorn to develop and operate their services. In 2024, with financial support from AWS, Thorn enhanced Safer Predict and Safer Portal to better support customers to easily detect and manage known and unknown CSAM.

Some of our member companies are also mandated to do transparency reports. Annual transparency reports outline how many instances of CSAM were caught. The numbers have decreased over the years as technology has gotten better to prevent CSAM from even being posted. AI and human technology can catch and report any CSAM from between the time the bad actor clicks "post" and the instant the post gets published.

Chatbots

Like preventing and removing CSAM, we conceptually agree with the intent of proposed chatbot legislation: to create strong, sensible guardrails for children using AI companion chatbots. However, it is vital to maintain the balance between consumer protection and business innovation. Well-intentioned regulations of companion chatbots have the potential to be overly broad. As such, we recommend that any definition for an AI companion be for the primary purpose of simulating social human companionship interaction and emotional support. This is an evolving issue that TechNet is presently engaging on in the Commonwealth with Senate and House bill sponsors.

Parental Involvement

To protect kids online from the harmful effects of artificial intelligence, it is imperative that parents play a role in their child's safety online. Our member companies provide the tools to help parents and children navigate the internet. Google, for example, has Family Link, which helps parents manage their children's accounts and devices as they explore online through parental controls. Parents can manage apps, keep an eye on screen time, and help set digital ground rules for their families. Family Link has an app activity report to see which apps a child is using the most, and allows parents content control, such as approving or denying certain app downloads or purchases.

Smart devices generally contain various tools for parents to monitor and control how much screen time and content their minor children are accessing. These parental controls are a vital part of the online safety picture. Controls offer parents and guardians the option to choose how and how often their children use their devices. Many smart devices contain built-in parental controls that help with managing downloads and purchases, who children can communicate with, and the apps and other content minors can access. Additional parental control features include preventing explicit content and inappropriate web browsing, restricting intelligence and virtual assistant capabilities, and preventing changes to privacy settings.

Education and Digital Literacy

Another way to keep young people safe online and from the negative impacts of AI is by promoting the education of safe internet practices. We support policies that help prepare young people to be a successful part of a global, interconnected, and technology-driven economy. Such policies include supporting digital learning resources and technology integration in student learning environments, fully funded K-12 education, and rigorous computer science standards. Digital citizenship education is a top priority for TechNet and its member companies. Several businesses participate in the Digital Trust & Safety Partnership (DTSP), which outlines best practices for those operating in the digital space.

Another program, Be Internet Awesome, in partnership with Google, empowers kids with tools and education to confidently and safely explore, grow, and play online. Be Internet Awesome helps children communicate responsibly, be aware of what's real and what's fake, secure personal information, and encourage positive interactions online with others.

Thank you for your consideration of our comments and please don't hesitate to reach out with any questions.

Sincerely,

Margaret Durkin

Margaret Durkin
TechNet Executive Director, Pennsylvania & the Mid-Atlantic