



1600 20th Street, NW • Washington, D.C. 20009 • 202/588-1000 • www.citizen.org

To: Interested parties

From: J.B. Branch, Big Tech accountability advocate, Public Citizen

Date: December 10, 2025

Re: Dangers posed by AI-powered toys

With the holiday season quickly approaching, Public Citizen anticipates Artificial Intelligence (AI) companies pursuing toys as a lucrative opportunity to expand their market. A recent [Pew Research](#) survey shows that one-in-ten parents say their 5 to 12-year-old children are using AI chatbots, while [Common Sense Media](#) reports that nearly 3 in 4 teens have used AI companions. Toy companies are eager to pursue this new trend too — for example, Mattel and OpenAI announced a [partnership](#) to develop toys that feature AI technology.

This holiday season is one of the most important for shoppers to be vigilant with AI-powered toys flooding the market, or disguising themselves by calling them “push-to-talk” or “voice activated” features. **This is concerning because AI enabled toys have little regulatory oversight and parents need to be aware of the risk they pose to children.** Whether it’s toys speaking inappropriately with children or data being collected, the risks of AI-powered toys are too great to ignore. **Parents should avoid purchasing any toys powered by AI**, at the very least until adequate safeguards are put in place to ensure the safety of children

We have already seen the harm AI-powered toys can expose children to. Last month, FoloToy’s [AI-powered teddy bear](#) was pulled from the shelves after reports that it engaged in explicit sexual messages, informed users where to find knives, and how to make knots for tying people up. U.S. PIRG has highlighted a [number of toys](#) that have problematic AI technology embedded. **Importantly, this company used an OpenAI large language model (LLM), the same family of models that will be used in the Mattel partnership.** AI-generated content is rampant in the video gaming community with little regard for transparency. [Epic Games CEO](#) suggested that disclosure of AI-generated content is unnecessary: **“It makes no sense for game stores, where AI will be involved in nearly all future production.”**

Why Parents Should Monitor Their Children’s Usage of AI

- AI is [powered by data](#) that often contains language inappropriate for minors and some models have been trained with data sets that include child pornography.
- Many AI models have a tendency to tell users what they want to hear which can [create](#) unrealistic expectations and unhealthy relationships
- AI toys can [record video and audio](#) of children, which can often be used to train future models, causing privacy concerns for parents and their kids.



1600 20th Street, NW • Washington, D.C. 20009 • 202/588-1000 • www.citizen.org

- AI products and toys can be hacked, the stolen data can then be used for illicit purposes like creating audio and video deepfakes of children.
- Some AI-powered toys force parents to share their children's data by becoming non-operational if parents opt out of data collection.

Protecting Children from AI Harms this Holiday Season

- **Do not buy children toys that are powered by AI.**
- Before allowing children to use AI-powered technology, review privacy agreements or opt out of sharing sensitive data.
- Be aware of features, like “voice activation” which can be used to record children and use the data for training.
- Monitor toys that use this technology, and offer prompts to see how it might respond.
- Check for toys that have offline modes, or can work without cloud-based connections.
- Teach children about AI and its inability to have feelings, even if it acts like it does.
- Tell Congress to protect children’s rights by regulating AI.