DATA PRIVACY & GOVERNANCE HUB

AI Toys & Data Privacy for Children

APRIL 7, 2026

Key Takeaways

- There is a growing trend of toy companies collaborating with AI partners to produce smart toys that use Wi-Fi, microphones, and large language models to interact with children.
- These toys collect sensitive data about the child and their family, including names, faces, preferences, voices, and locations, without clear security measures.
- Manufacturers currently operate without meaningful oversight or regulation, allowing them to determine what data they collect, retain, and utilize from child users.
- Regulation has failed to keep pace with the rapid development of AI toys, and meaningful security mechanisms should be built into the toy from the start.

What Happened

Artificial intelligence is rapidly transforming the landscape of playrooms across the country, bringing to life a once futuristic idea of smart toys that listen, process, learn, and respond to children. Mattel, one of the most iconic toy brands in stores, is now teaming up with OpenAI, hoping to "bring a new dimension of AI-powered innovation and magic to Mattel's iconic brands," revealing a new trend in children's entertainment. AI toys use a microphone to hear and understand requests from the children playing with them, connect to the Internet via Wi-Fi, and leverage Large Language Models (LLMs), such as those from OpenAI, to generate responses to the children. This reply often comes in the form of verbal communication from a speaker built into the toy. These products are often manufactured in China, leaving U.S. officials concerned about potential data privacy risks for children. Advocates are urging public representatives to initiate campaigns in hopes of raising public awareness "on the potential misuse of the data collected" with these toys.

Privacy and Governance Concerns

A central concern for parents and policymakers alike is the uncertainty surrounding the amount of information AI toys collect and store. The scope of this data – particularly, sensitive data like "children's names, faces, voices, and locations" – and the security measures used to safeguard it are often unclear. When the toy is in use, parents are blind to the amount of privacy they do – or don't – have. Many others have warned that this data is vulnerable to hacking and security breaches. In some instances, these risks have materialized, notably with the brand Bondu. As part of the brand's launch, Bondu's AI toys included a portal that allowed parents and staff to view conversations between the child and the toy for parental control and product performance monitoring. This portal exposed 50,000 transcripts of virtually every conversation Bondu's child users had with their toys to anyone with a Gmail account, revealing personal preferences such as pet names, favorite snacks, and preferred activities. The data was left unprotected, disclosing children's names, birthdays, family member names, and logs of intimate conversations to anyone who could create an email. Bondu quickly took down the site after the error was reported and relaunched the portal the following day with proper authentication measures.

Why It Matters / Policy Considerations

The lack of robust security regulations and effective proactive protective measures for children's data privacy leaves children and families across the United States vulnerable to risks to the data privacy of AI toys. Security should be preventative, built into the toy from the start, and treated as a core aspect of its successful design – not as an afterthought only addressed and applied after a breach occurs. The rapid development of large language models and the growing popularity of AI toys have outpaced regulatory safeguards, effectively allowing companies to dictate what data they gather, store, and monitor on children who use their toys. In California, Senator Steve Padilla introduced a bill in early January that would "prohibit the manufacture and sale of toys that include an artificial intelligence-powered chatbot" for the next four years. The Senator reiterated in a press statement that he hopes this delayed market introduction would allow time to develop safety measures to protect children from potentially harmful interactions.