Some tips for Parents when considering an AI enabled toy for Christmas this year

1. All AI Smart toys are connected to the Internet

Smart or Internet-connected toys typically contain sensors, microphones, cameras, data storage components, speech recognition, and GPS options. Such toys collect information, which is further sent and stored by the manufacturer or developer via a server or cloud service. The collected data can include voice recordings, toy web application passwords, home addresses, Wi-Fi details, or sensitive personal data. Therefore, these hi-tech features could put the safety and security of the children at serious risk—the possibility of hackers exploiting these toys to spy on users.

2. Bluetooth enabled toys are not as safe as you might think

While pointing out that toys using encrypted communications are vital in alleviating the security risk, the FBI said that not all toys implement such features. Unprotected Bluetooth-connected toys that do not require PINs or passwords when pairing with a mobile device. These also pose a significant risk for unauthorized access.

3. Toy Companies themselves may be open to hacks of the data they are collecting when your child is using the toy.

Another data risk involves the toy companies themselves. These companies collect "*large amounts of additional data, like voice messages, conversation recordings, past, and real-time physical locations, Internet use history, and Internet addresses/IPs*." Hence, they could be promising targets for hackers.
Parents should, therefore, review the toy company user agreement disclosures and privacy practices to find out where their family's data is sent and stored and if it's sent to third-party services.

4. AI toys have been shown recently to give young children inappropriate information like where to find matches and knives in your house and how to use them.

Some AI toys have also been shown to give young children sexually explicit content or other inappropriate and psychologically harmful responses. These might not show up right away so test the toys for at least five minutes since vulnerabilities in this area often show up after the toy has been used for several minutes and not right away.

What you can do as a parent:

Precautions to take when buying Smart Toys

1.Check if there are any known security issues for any Internet-connected toys they intend to buy or have already purchased.

2.Check the toy's security measures like Bluetooth authentication and encrypted data transmission.

3.Check if the company behind the toy issues firmware/software updates in cases where they don't make sure to have it installed.

4.Finally, research where data from the toy is stored and whether the company storing it has a good reputation for security.

A STATEMENT FROM THE TOY ASSOCIATION:

Toy safety is the top priority of the toy industry and protecting children and maintaining the trust of parents are part of that mission. Indeed, all toys sold in the U.S. are required to comply with over 100 different safety standards and tests to ensure the physical safety of children at play.

At the same time, The Toy Association recognizes that Artificial Intelligence (AI), internet-connected products, and Internet of Things (IoT) technologies and services are becoming increasingly common in all types of household products, including those offered by toy companies. Our focus on safety extends to online safety as well. In this regard, toy companies adhere to the principles outlined in the Children's Online Privacy Protection Act (COPPA), which includes provisions governing children's privacy and data security and is overseen by the U.S. Federal Trade Commission (FTC). Toy Association members take seriously their obligation to comply with COPPA in all operations that may involve the online collection of personal information from children, just as they take seriously their obligation to comply with additional laws, such as the EU General Data Protection Regulation (GDPR). Additionally, there is an ASTM standard to provide guidance to companies making connected products of all kinds, providing added reassurance to parents and families on the safety of their children's connected toys.

Recognizing that data minimization concepts are central to safeguarding privacy, the toy industry applauds the FTC for confirming a privacy-friendly approach to voice-activated internet-connected toys. The FTC has recognized that when companies adopt careful procedures to manage voice recordings associated with voice-activated toys by promptly deleting the recording once the request has been recognized, they strike an appropriate balance of fostering an engaging experience while protecting children's privacy.

As The Toy Association tracks new technologies, including the growth of AI, we are committed to educating our members about the potential applications of connected technologies in toys and how to maintain the safety of children and families above all else. The toy industry always prioritizes the safety of children.

This statement was reaffirmed by The Toy Association in October 2025.

How Hackers Exploit Smart Toys

Smart toys, as part of the Internet of Things (IoT), can be exploited in various ways:

Unauthorised Access: Weak or non-existent authentication protocols can allow hackers to gain control over the toy's functions.

Data Interception: Unencrypted data transmissions can be intercepted, leading to the theft of personal information.

Remote Surveillance: Compromised cameras and microphones can be used to spy on children and their surroundings.

Manipulative Interactions: Hackers can send inappropriate messages or commands to children through the toy, posing psychological risks.

The Dark Side of AI in Smart Toys: Emerging Threats

Beyond data breaches, AI-powered toys introduce new dangers:

AI-Generated Child Exploitation Material: Predators are using AI to create deepfake child sexual abuse material (CSAM) from innocent photos kids post online. These fake images can be used for sextortion or grooming.

AI-Driven Grooming: Chatbots in smart toys can be manipulated to engage in inappropriate conversations with children. Hackers can use AI to mimic a child's friend, building trust before exploitation.

Dataveillance: Profiling Kids for Life: Smart toys collect data that could later be sold to colleges, employers, or advertisers, influencing a child's future opportunities without their consent.

The Ethical and Psychological Implications

Beyond technical vulnerabilities, smart toys raise ethical concerns:

Data Privacy: Children's interactions with toys are often recorded and stored, and sometimes shared with third parties without explicit consent.

Behavioural Influence: AI-driven responses can shape children's behaviour and perceptions, potentially leading to dependency on technology for social interactions.

Lack of Transparency: Complex terms of service and privacy policies make it difficult for parents to understand what data is collected and how it's used.

What Parents Can Do: Protecting Kids from Hacked Toys

While regulators struggle to keep up with technological advancements, parents can take proactive steps:

Research Before Buying: Check if the toy complies with COPPA (Children’s Online Privacy Protection Act) or GDPR. Avoid toys with always-on microphones or cameras.

Secure Home Networks: Change default passwords on smart toys and Wi-Fi routers. Use strong encryption (WPA3) for home networks.

Monitor and Limit Usage: Turn off toys when not in use to prevent unauthorized access. Regularly check for firmware updates.

Educate Kids on Digital Safety: Teach children not to share personal information with smart toys. Encourage skepticism about unexpected toy behaviors (e.g., talking unprompted).