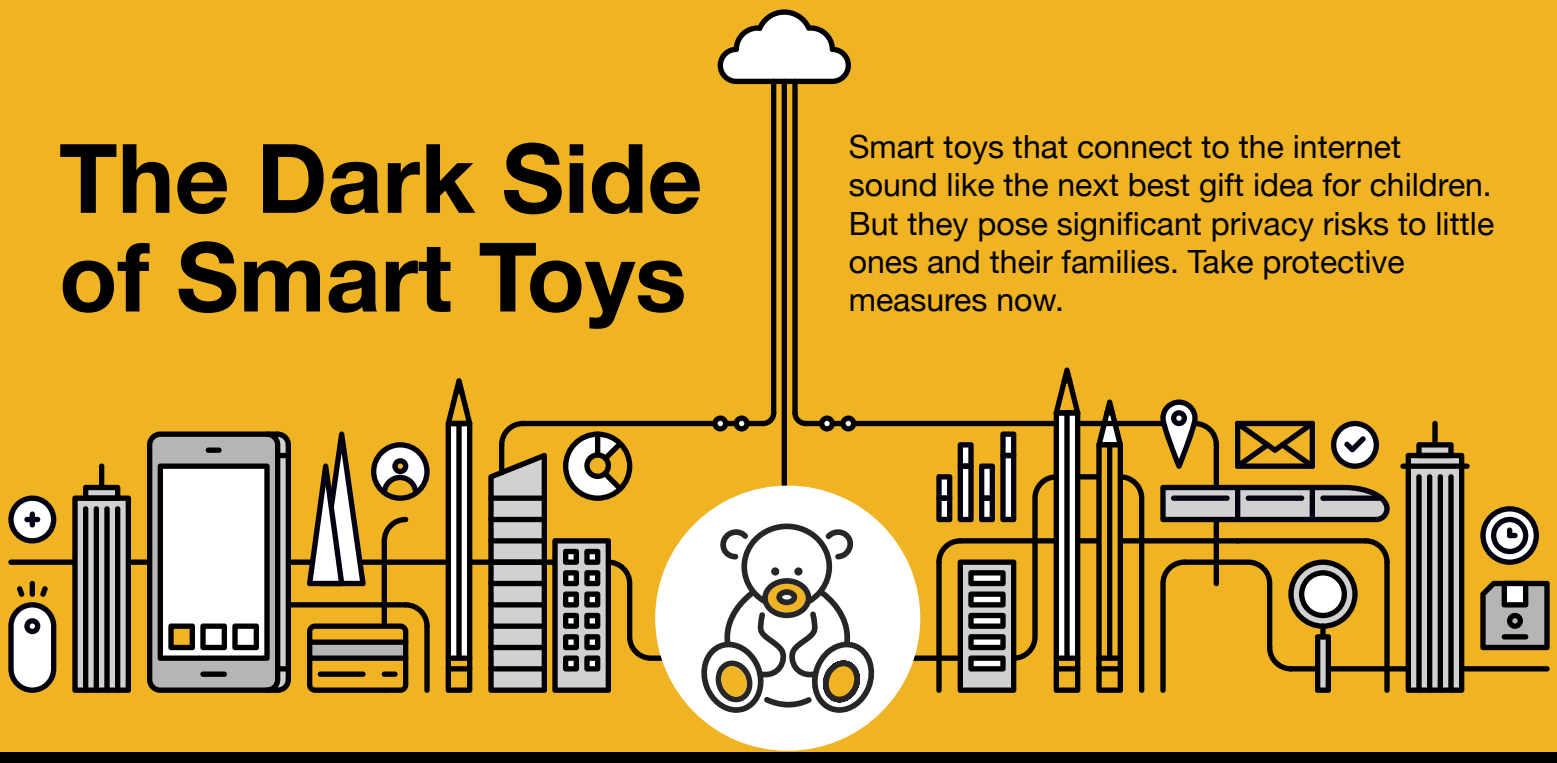
The Dark Side of Smart Toys

Smart toys that connect to the internet sound like the next best gift idea for children. But they pose significant privacy risks to little ones and their families. Take protective measures now.



A Growing Industry

65% of parents would pay more for a smart toy[1]

2015 **$2.8 billion**
2020 **$11.3 billion**[2]

Examples of Smart Toys

+ Smart Toy Bear by Fisher-Price
+ Innotab3 Tablets by VTech
+ Hello Barbie by Mattel
+ My Friend Cayla by Genesis Toys

Hidden Dangers

Targets. Toys can be targets for hackers. Toy makers may be lax about security. Some dolls can be turned into listening devices with free apps.[3]

Marketing manipulation. Smart toys can be used to gather information about your child and your family for targeted marketing and advertising purposes.[4]

Confusing terms of service and privacy agreements can make it difficult to know what's being tracked from day to day.[5]

Protection tips

Research. Google the product to look for red flags about security or privacy.

Educate. Teach children what types of information are okay to share with the toy and to turn it off when not in use.

Monitor. Keep an eye on how your child uses the toy and turn it off during private discussions.

1 "Parents, Kids Drive Billion-Dollar Smart Toy Market," February 2016, BSM Media.
2 "The Future of Smart Toys and the Battle for Digital Children," The Guardian, Sept. 22, 2016, https://www.theguardian.com/technology/2016/sep/22/digital-children-smart-toys-technology.
3 "This is Why Tech Toys are Dangerous," Computerworld, December 2015.
4 "Connected Toys Violate European Consumer Law," Norwegian Consumer Council, December 2016.
5 "These Toys Don't Just Listen To Your Kids; They Send What They Hear to a Defense Contractor," Consumerist, Dec. 6, 2016.

CYBERSCOUT™
WE'LL TAKE IT FROM HERE™