A Little 'Too Smart' Toys

By Reg P. Wydeven
December 31, 2017

I hope everyone had a merry and fun-filled holiday. A week ago, I'm sure millions of kids awoke to find all kinds of goodies under their Christmas trees. I'm sure there were classic toys like dolls and footballs. There were probably even good old-fashioned dangerous toys, like the official Red Ryder, carbine action, 200-shot, range model air rifle, with a compass in the stock and the thing that tells time, that could shoot a kid's eye out.

But I'm sure there were plenty of new techy toys, too. I'm betting kids got video games, tablets, smart phones, smart TVs, smart watches and even smart toys. Unfortunately, when it comes to smart toys, some of us parents might feel pretty dumb, especially after learning they can be far more dangerous than BB guns.

Earlier this year, the FBI actually issued an alert about how smart toys that connect to the internet can present huge privacy concerns for children – especially those with microphones, cameras and GPS. The alert warned that smart toys are "increasingly incorporating technologies that learn and tailor their behaviors based on user interactions."

Some of these toys store personal information on the cloud, such as a child's voice or image, or data like names, email and home addresses. As a result, this information is prone to be hacked. Unlike computers, tablets and phones that are constantly downloading updates to guard against unauthorized access, many smart toys are rarely updated. If the toy has a GPS, hackers not only can find out your child's name and what they look and sound like, but they can track the toy's location as well.

Not only can hackers get a glimpse into our personal lives, but the toy manufacturers can, too. Earlier this year I wrote about several advocacy groups that jointly filed a complaint with the Federal Trade Commission against two specific products made by Genesis Toys: My Friend Cayla and i-Que Intelligence Robot. The complaint alleged that the toys "unfairly and deceptively collect, use, and share audio files of children's voices without providing adequate notice or obtaining verified parental consent."

The FTC implemented the Children's Online Privacy Protection Rule ("COPPA"), which requires operators of websites or online services that have actual knowledge that they are collecting personal information online from children under 13 years of age to first obtain their parents' consent. However, in the excitement of setting up the toy, many parents unwittingly give such consent.

So this holiday season several consumer watchdog organizations advised parents to examine the toy's privacy settings and make sure it's made by a responsible manufacturer. To help, the FTC approved multiple organizations to certify smart toys. These include: Aristotle International Inc., Children's Advertising Review Unit, Entertainment Software Rating Board, iKeepSafe, kidSAFE, Privacy Vaults Online, Inc., and TRUSTe.

If your child did receive a smart toy this year, be sure to update it regularly and use a password that would be difficult to crack (alpha and numeric, with capital letters and symbols).

It's a great deterrent to being naughty when we warn our children that Santa Claus "sees when you're sleeping, he knows when you're awake." But it's downright creepy if we're talking about a toy.

Have a happy and blessed 2018.