Issued 7/19/17

The FBI Alerts Parents to Dangers of Internet of Thing Toys

The FBI issued a warning Monday advising parents to carefully check internet- connected toys for possible privacy and security concerns. In this startling alert [link], the Feds gave America's families the grim news: many toys sporting cloud-backed features such as speech recognition or online content hosting "could put the privacy and safety of children at risk due to the large amount of personal information that may be unwittingly disclosed." "Security safeguards for these toys can be overlooked in the rush to market them and to make them easy to use," the FBI warns. "Consumers should perform online research of these products for any known issues that have been identified by security researchers or in consumer reports."

This comes after a number of kids' toys were found to be indirectly spying on kids by collecting and storing data, including audio conversations and personal information, without parents' knowledge. In addition to eavesdropping toys, a number of app developers and websites have been called out for inadequate protections on accounts and data for children. Under the Children's Online Privacy Protection Act (COPPA), companies are required to get permission from parents before collecting any personal information on a user who is under the age of 13.

The FBI warning advises parents to not only review what exactly the toys can collect and transmit, but also the privacy policies they operate under. Additionally, parents are advised to only operate connected toys on trusted Wi-Fi networks and to make sure the firmware and patches are installed for apps and connected devices. "Bluetooth-connected toys that do not have authentication requirements (such as PINs or passwords) when pairing with the mobile devices could pose a risk for unauthorized access to the toy and allow communications with a child user," the FBI warns. "It could also be possible for unauthorized users to remotely gain access to the toy if the security measures used for these connections are insufficient or the device is compromised."