Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

July 17, 2017

Alert Number
I-071717(Revised)-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field

CONSUMER NOTICE: INTERNET-CONNECTED TOYS COULD PRESENT PRIVACY AND CONTACT CONCERNS FOR CHILDREN

The FBI encourages consumers to consider cyber security prior to introducing smart, interactive, internet-connected toys into their homes or trusted environments. Smart toys and entertainment devices for children are increasingly incorporating technologies that learn and tailor their behaviors based on user interactions. These toys typically contain sensors, microphones, cameras, data storage components, and other multimedia capabilities – including speech recognition and GPS options. These features could put the privacy and safety of children at risk due to the large amount of personal information that may be unwittingly disclosed.

WHY DOES THIS MATTER TO MY FAMILY?

The features and functions of different toys vary widely. In some cases, toys with microphones could record and collect conversations within earshot of the device. Information such as the child's name, school, likes and dislikes, and activities may be disclosed through normal conversation with the toy or in the surrounding environment. The collection of a child's personal information combined with a toy's ability to connect to the Internet or other devices raises concerns for privacy and physical safety. Personal information (e.g., name, date of birth, pictures, address) is typically provided when creating user accounts. In addition, companies collect large amounts of additional data, such as voice messages, conversation recordings, past and real-time physical locations, Internet use history, and Internet addresses/IPs. The exposure of such information could create opportunities for child identity fraud. Additionally, the potential misuse of sensitive data such as GPS location information, visual identifiers from pictures or videos, and known interests to garner trust from a child could present exploitation risks.

Consumers should examine toy company user agreement disclosures and privacy practices, and should know where their family's personal data is sent and stored, including if it's sent to third-party services. Security safeguards for these toys can be overlooked in the rush to market them and to make them easy to use. Consumers should perform online research of these products for any known issues that have been identified by security researchers or in consumer reports.

WHAT MAKES INTERNET-CONNECTED TOYS VULNERABLE?

Data collected from interactions or conversations between children and toys are typically sent and stored by the manufacturer or developer via server or cloud service. In some cases, it is also collected by third-party companies who manage the voice recognition software used in the toys. Voice recordings, toy Web application (parent app) passwords, home addresses, Wi-Fi information, or sensitive personal data could be exposed if the security

of the data is not sufficiently protected with the proper use of digital certificates and encryption when it is being transmitted or stored.

Smart toys generally connect to the Internet either:

- Directly, through Wi-Fi to an Internet-connected wireless access point; or
- Indirectly, via Bluetooth to an Android or iOS device that is connected to the Internet.

The cyber security measures used in the toy, the toy's partner applications, and the Wi-Fi network on which the toy connects directly impacts the overall user security. Communications connections where data is encrypted between the toy, Wi-Fi access points, and Internet servers that store data or interact with the toy are crucial to mitigate the risk of hackers exploiting the toy or possibly eavesdropping on conversations/audio messages. 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. 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.

WHAT CONSUMER LAWS EXIST TO PROTECT MY CHILDREN?

The Children's Online Privacy Protection Act (COPPA) imposes requirements on Web site and online service operators directed to children under the age of 13 and on operators of other sites and services who knowingly collect personal online information on children under 13 (for further details on COPPA and protecting children online, refer to https://www.consumer.ftc.gov/topics/protecting-kids-online). On 21 June 2017, the Federal Trade Commission (FTC) updated its guidance for companies required to comply with COPPA to ensure those companies implement key protections with respect to Internet-connected toys and associated services, to include the use of mobile apps, Internet-enabled location-based services, and voice-over IP services (https://www.ftc.gov/news-events/blogs/business-blog/2017/06/ftc-updates-coppa-compliance-plan-business). In addition, a manufacturer's failure to implement reasonable security measures for data collected by its Internet-connected toys could subject that company to an FTC enforcement action under Section 5(a) of the FTC Act, which prohibits unfair or deceptive practices in the marketplace. The FBI is encouraging all consumers to research areas and circumstances concerning the toys and Web services where laws may or may not provide coverage.

WHAT SHOULD I DO?

The FBI encourages consumers to consider the following recommendations, at a minimum, prior to using Internet-connected toys.

- Research for any known reported security issues using online resources from sites that conduct cyber security research, consumer product reviews, and child and consumer advocacy
- Only connect and use toys in environments with trusted and secured Wi-Fi Internet access
- Research the toy's Internet and device connection security measures
    - Use authentication when pairing the device with Bluetooth (via PIN code or password)
    - Use encryption when transmitting data from the toy to the Wi-Fi

access point and to the server or cloud
- Research if your toys can receive firmware and/or software updates and security patches
  - If they can, ensure your toys are running on the most updated versions and any available patches are implemented
- Research where user data is stored – with the company, third party services, or both – and whether any publicly available reporting exists on their reputation and posture for cyber security
- Carefully read disclosures and privacy policies (from company and any third parties) and consider the following:
  - If the company is victimized by a cyber-attack and your data may have been exposed, will the company notify you?
  - If vulnerabilities to the toy are discovered, will the company notify you?
  - Where is your data being stored?
  - Who has access to your data?
  - If changes are made to the disclosure and privacy policies, will the company notify you?
  - Is the company contact information openly available in case you have questions or concerns?
- Closely monitor children's activity with the toys (such as conversations and voice recordings) through the toy's partner parent application, if such features are available
- Ensure the toy is turned off, particularly those with microphones and cameras, when not in use
- Use strong and unique login passwords when creating user accounts (e.g., lower and upper case letters, numbers, and special characters)
- Provide only what is minimally required when inputting information for user accounts (e.g., some services offer additional features if birthdays or information on a child's preferences are provided)

If you suspect your child's toy may have been compromised, file a complaint with the Internet Crime Complaint Center, at www.IC3.gov.