Smart Toys & Location Trackers: Privacy and Safety Concerns with Children and Pets

"Smart" and "connected" toys that promise to entertain, increase safety, and connect us to our kids and pets while we're away from home are rushing into the marketplace. These devices may offer survivors ways to increase privacy and safety, with knowledge about privacy settings and strategic use. Unfortunately, they can also provide yet another, highly invasive way that technology can be misused to monitor, harass, threaten, or harm survivors.

What is "IoT"?

The Internet of Things refers to devices connected to each other and to a device or app that can control them. These devices may be connected through a home network, a website, or an app through the Internet, Bluetooth, or other means.

Smart Toys

We now have the ability to buy toys that listen and speak to your children, reading stories, asking them questions, and searching for information on the Internet. Some toys come equipped with cameras, microphones, and speakers so the toys can interact with the child.

Safety and privacy risks related to voice recognition are of concern. It is important to understand the difference between "voice recognition" and "speech recognition." *Speech recognition* is the ability of a device to understand spoken words. This may be familiar from smart phones or home automation personal assistants like Amazon's Alexa or Google Home. *Voice recognition* is the ability of a device to determine who is speaking: an adult vs. a child, for example, or even specific people in the house.

The main risk associated with these toys is surveillance from an abuser, a neighbor, or other third party. Many devices are not built with strong security protections. For example, some devices can be connected through Bluetooth, allowing for people in close proximity, such as neighbors, to access the toy.

Others offer security against third parties or strangers, but might give unauthorized video or audio access to someone who gives the toy as a gift, for example. The information gathered could be used to stalk, control, or harass a survivor.

Small drones used for recreation are another increasingly popular toy. Tiny devices often called “nano drones” fit in the palm of the hand and can cost under $50. Larger drones for racing or other competition are much more expensive and may include microphones or cameras. Some drones are controlled remotely much as the older generation of remote-control toys, but some new drones can be controlled by mobile devices.

Other IoT Devices for Families

In addition to smart toys, many other devices are currently marketed to parents and families that are designed to increase children’s safety, but may not have adequate security features, or may be purposely misused to monitor or harm a child or other family member.

- Baby monitors, which have long been vulnerable to monitoring through radio waves in their older versions, are now connected through the Internet to a handset or a parent’s mobile device.
- Location tracking devices have long been marketed as a way to keep children or aging parents safe from wandering off. Previously based on GPS technology, newer devices use more energy-efficient, longer-lasting technologies paired with the convenience of a connection to a mobile device or web interface.

These new devices, being Internet-connected, open up new risks for monitoring by a domestic violence abuser or child sexual abuse offender either within the home or not living with the child.

IoT Devices for Pets

Another growing market for connected devices is targeted at pet owners.

- Food and water dispensers are being combined with cameras and speakers so that owners can check in on their pets when they are away, even playing with them through the device or tossing a treat.
- Some devices track a pet's location or vital signs, relaying the information over the Internet or via an app.
- As with devices for children, location tracking devices for pets were previously based on GPS technology. Newer devices use more energy-efficient, longer-lasting technologies paired with the convenience of a connection to a mobile device or web interface.

These devices, like smart toys, often have inadequate security features, or do not encourage owners to change default security settings. The devices could be used to monitor the home through a camera or track the location of the person while walking their pet, for example.

Benefits of Connected & Smart Devices

Connection to kids and pets from a distance can be an important part of emotional well-being. Being able to track the location and safety of kids and pets can help reassure a survivor that their loved ones are safe and healthy. In the event of violence or harassment towards the survivor, children, or pets, cameras in these devices might capture useful footage for evidence.

Questions About IoT Devices

When considering purchasing connected toys or bringing these devices into the home, there are a few questions to consider. First, does that particular device need to be "smart" or "connected"? Do the benefits outweigh the risks? How secure is the device and the app that runs it? Are there features that allow the user to individualize and increase privacy and security?

Strategies to Increase Privacy and Safety

Steps to increase the privacy and safety of smart toys include learning about the built-in security options of the device, turning it off when not in use, and changing the default passwords or other security settings.

If a survivor suspects that a device is being misused, they can begin to document the incidents. Our technology abuse log is one way to document each occurrence. These logs can be helpful in revealing patterns, determining next steps, and may potentially be useful in building a case if the survivor chooses to involve the legal system.

Survivors might also try to access evidence through the device, or the app or website that controls it. They can also try to reach out to the manufacturer to try to regain control over a device or the account associated with it. With these devices and others, it is also important to take steps to increase network and WiFi security. For more information, see our handout on WiFi security.

Supported by US DOJ-OVC Grant # 2016-TA-AX-K069. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ.

This is one in a series of handouts describing the risks and potential benefits of IoT devices. We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.