Smart Toys and Location Tracking: Privacy and Safety Concerns with Children and Pets

A Note on Language

In this toolkit, we will sometimes use the word woman/women and feminine pronouns for simplicity and to recognize the significant impact technology-facilitated violence has on women and girls. We recognize that TFGBV also impacts trans, non-binary, and Two-Spirit people. We hope that all people impacted by TFGBV will find these documents useful.

"Smart" and "connected" toys that promise to entertain, increase safety, and connect us to our kids and pets while we're away from home fill today's marketplace. These devices and systems offer potential tools survivors can use to strategically increase their safety. Unfortunately, these devices and the systems that control them also provide yet another, highly invasive way that technology can be misused to monitor, harass, threaten, or harm survivors.

For more information and general tips about the Internet of Things and smart devices, see our Overview Document.

Smart Toys

We can now buy toys that listen and speak to our children, read stories, ask questions, and search for information on the Internet. Some toys come equipped with cameras, microphones, and speakers so the toys can interact with the child.

There can be safety and privacy risks related to voice recognition, as it can be misused to impersonate a child. Voice recognition can be misused by an abuser to lock and control certain features on smart toys, including setting up location tracking abilities. It is important to understand the difference between "voice recognition" and "speech recognition." *Voice recognition* is the device's ability to determine who is speaking: an adult vs. a child, for example, or even specific people in the house. *Speech recognition* is the device's ability to understand spoken words. This may be familiar with smartphones or home automation personal assistants like Amazon's Alexa or Google Home.

The main risk associated with these toys is surveillance from a perpetrator, a neighbour, or another third party. Many devices are not built with strong security protections. For example, some devices can be connected through Bluetooth, allowing people in close proximity, such as neighbours, 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 survivors.

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 competitions are much more expensive and may include microphones or cameras. Some drones are controlled remotely, like 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 as a way to increase children's safety. These may not have adequate security features or could 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 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.

Because the new versions of these devices are Internet-connected, they open up new risks for monitoring by a domestic violence perpetrator or child sexual abuse offender, both within and outside the home.

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 and Smart Devices

Connection to children 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 women experiencing violence that their loved ones are safe and healthy. In the event of violence or harassment towards a woman, her 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:

- Does that particular device need to be "smart" or "connected"?
- Do the benefits outweigh the risks?
- How secure are 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 you suspect that a device is being misused, you can begin to document the incidents. Our Technology-Facilitated Violence Log is one way to document each occurrence. These logs can be helpful in revealing patterns and determining next steps, and may potentially be useful in building a case if you choose to involve the legal system.

You may also try to access evidence through the device, or the app or website that controls it. You can also try to reach out to the manufacturer 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 Wi-Fi security. For more information, see our handout on Wi-Fi security.

Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use sheltersafe.ca to find a shelter/transition house near you to discuss options and create a safety plan. You don't need to stay in a shelter to access free, confidential services and support.

Adapted for Canada with permission from NNEDV's Safety Net project, based on their resource Smart Toys and Location Trackers: Privacy and Safety Concerns with Children and Pets.

© Copyright 2024 Women's Shelters Canada | All Rights Reserved

This project is made possible through funding from the department of Women and Gender Equality (WAGE) Canada.

Women and Gender Equality Canada Femmes et Égalité des genres Canada Canada