Internet of Things and Connected Devices

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.

Overview of the Internet of Things and Connected Devices

What Is The Internet of Things?

The Internet of Things (IoT) refers to devices connected to each other and to a device or app that can control them. These devices may be connected through the Internet, Bluetooth, or other means. Unfortunately, these devices and systems can provide yet another, highly invasive way that technology can be misused to monitor, harass, threaten, or harm. At the same time, they are also potential tools people can use to strategically increase their safety.

Most Common Iot Devices

Home Automation and Personal Assistants

Our homes are rapidly being filled with “smart” and “connected” devices that promise to increase convenience, improve energy savings, and strengthen personal security, such as smart lights, thermostats, and security cameras. Home automation IoT allows remote control and surveillance through Internet-connected devices in the home.

Smart Toys and Location Trackers

“Smart” and “connected” toys promise to entertain, increase safety, and connect us to our kids and pets while we’re away from home.

Smart Cars and Driverless Vehicles

While driverless vehicles get all the headlines, many newer cars come off the lot already “connected,” allowing parents to monitor and control teen drivers and employers to monitor employee driving habits. In addition, small gadgets can be attached to a car to allow for remote monitoring and, in some cases, remote control of some features.

Connected Health and Medical Devices

Many health and medical devices are now connected to the Internet, offering to help you track information about your healt or even send that information to your doctor.

Steps to Increase Safety and Privacy

Be aware of the risks when you use a smart device and learn what you can do to increase privacy and security. Although each smart device will be different, here are some general tips.

1. Know How Your Smart Device Works

The first step to staying on top of your privacy, security, and safety when using a smart device is to understand how it works. When you set up a smart device, you will either create an account for that device, attach an email to that device, or connect that device to a network (usually your home Wi-Fi network) – or perhaps all of the above. Having a general idea of how your smart device works and what it’s connected to will help you determine what information is shared and how it is accessed, which will help you identify and minimize potential risks.

2. Limit Connections to Your Smart Device

Review how and what it is connected to. If it’s connected via Wi-Fi, turn it off when you’re not using it. If you can’t turn it off, disconnect it from the Internet. If it has other types of access, such as Bluetooth, turn off the connection access. If it’s turned off or not connected, it will not be possible for someone to access the device remotely.

3. Limit Personal Information Shared from Your Smart Device

Information about you is stored either on the device, in an account, or with the company. If you are worried about someone gaining access to your information, determine whether you can limit personal information stored or shared via the device. This can include turning off the device when not in use, turning off cameras or microphones, or reviewing the device’s settings and limiting how much information the company can gather about you. Read the company’s privacy policy to learn about how they share your personal data.

4. Secure the Account Associated with Your Device

Some devices require you to set it up with an account, prompting you to create a username and password. Create a username and password that someone else (including the perpetrator) can't guess. Some accounts may offer 2-step verification so that if someone tried to access your account from a different device or location, they will require an additional verification code (generally in the form of an SMS code).

If the device doesn't require a username/password to access, know how it connects and whether someone else could connect to it.

5. Increase the Security of Your Home Network Router

Because smart devices are mostly connected to a home Wi-Fi network, make sure that your home router is secure. There are many things you can do to increase your home router's security, including the following:

- Put a passcode on your home Wi-Fi network
- Change the router's username/password from the default
- Use WPA2 encryption
- Turn off remote management on the router

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 WESNET's Tech Safety project, based on their resource Smart Devices and Internet of Things.

Home Automation: Privacy Risks and Strategies

Our homes, workplaces, and vehicles are rapidly being filled with "smart" and "connected" devices that promise to increase convenience, improve energy savings, and strengthen personal security. 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.

What Are Some Examples of Home Automation?

Home Automation includes devices, systems, or apps that allow remote control of Internet-connected devices in the home. Some examples include:

- Personal Assistants (e.g. Google Home, Amazon Echo/Alexa). These devices are voice-activated and often include features that adjust lights, play music, place phone calls, read text messages, search for information, and other functions.
- Home Automation Systems (e.g. Nest, Arduino.). These systems often begin with a thermostat or lights and can be expanded to include additional connected devices. Some brands will only allow for connection with devices of the same brand, while others may allow for more universal control across brands.
- Apps pair with IoT devices to allow web-based control through mobile devices. Many of these apps come with the IoT devices, and some work across brands. The apps might notify a user of a smoke alarm, a person at the door, or if an appliance was left on.
- Settings or pre-programmed routines may be built into a device or service and left to run, with or without current remote access. For example, when a user's phone nears the house, the front door might unlock, the lights might go on, music may begin, and the thermostat may adjust to preferred settings.

Connected Devices

These common devices might also be part of the network:

- Thermostat
- Smart light bulbs
- Smart electrical outlets (with lights or other devices plugged into them)
- Entertainment systems (e.g. stereo, TV, speakers)
- Hubs that are located on a bedside table, in a closet, or other locations throughout the house that connect to the home personal assistant
- Security cameras and motion detectors
- Smoke detectors
- Video doorbells
- Smart locks
- Appliances (e.g. refrigerator, vacuum)
- Pet feeders, nanny or pet cams, toys, and trackers
- Children's toys and trackers

Home Automation Misuse as a Tactic of Abuse

Home automation devices and systems can be misused to monitor, harass, isolate, and otherwise harm survivors. The technology can track who is in the home and what they are doing. Such surveillance might be done secretly, or overtly, as a way to control behaviour – by capturing images, keeping activity logs, eavesdropping, and gaining access to email or other accounts linked to the connected devices.

Home automation technology can also be misused to cause distress and harm by turning lights and appliances on or off, adjusting the temperature to uncomfortable levels, playing unwanted music or adjusting the volume, triggering home invasion and smoke alarms, and locking or unlocking doors. This kind of harassment can cause significant sleep disruption and trigger traumatic reactions.

Home automation may also be misused to isolate a survivor by threatening visitors, posting private videos or images without consent, and blocking physical access. For example, smart locks could be remotely controlled, limiting a survivor's ability to leave the house or return to it. A video doorbell could be used not only to monitor who comes to the door, but also to harass them remotely or, in combination with a smart lock, prevent them from entering the house.

People with disabilities may experience additional harm when a caregiver, family member, or roommate takes control, limits access, or damages the system or home automation devices, as might happen with other assistive technology.

Safety Planning and Home Automation Misuse

As with all safety planning, each survivor's experience and priorities should determine the course of action. Identifying the technology being misused and taking steps to decrease related risks will take time, energy, and access to information.

If you suspect that a device is being misused, you 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 and determining next steps, and may be useful in building a case if you choose to involve the legal system.

Ask questions that can help identify what the person could be doing, such as:

- Are there any patterns in terms of when devices are misused (e.g. the time of day, related events like contact, visitation, or court proceedings)?
- Does the person misusing the technology have access to the home or accounts for utilities, security services, or devices? Did they in the past?
- What devices do you know are in the home?
- What else might be hidden?

Once the devices and services that might be involved have been identified, particularly what sort of system could be controlling the devices, the next step is to identify options for regaining control of the system. For instance, if a personal assistant device is being misused, can the account be accessed by you and the password changed to lock out unauthorized access? If it is an app, can the system, network, or devices be reconfigured to block access?

Potential approaches include:

- Contacting the company that made the device or maintains the software to change account ownership and access.
- Changing router or network settings. For more information, see our document on Wi-Fi security.
- Replacing the devices (lightbulbs, the thermostat, electrical outlets, or other connected devices) to either remove those devices from the system or regain control of the system.

NOTE: It is important to safety plan around the possibility that cutting off remote control may escalate harmful behaviour.

Using Home Automation to Increase Safety

These same systems and devices that may be misused to harm survivors can also be used to protect privacy and enhance safety. Here are some examples:

- Security cameras, video doorbells, and other security devices can notify a woman when someone approaches or enters the house. These devices might also gather evidence to document violations of a protection order or other criminal behaviour.
- Smart lightbulbs might provide peace of mind to a woman by illuminating the house or a room before she enters it.
- Pet cams and feeders might provide needed support or comfort to a woman when she is away from home, or help reassure her of a pet's health or safety.
- Energy-saving devices might help to reduce the financial burden of living independently from a perpetrator.
- Home automation can assist women with disabilities, potentially decreasing the level of support needed from caregivers and increasing independence.

Considerations with New Devices

When considering buying new home automation devices, 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?
- Can that security be strengthened?

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 Internet of Things Home Automation: Survivor Privacy Risks and Strategies.

Smart Toys and Location Tracking: 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 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.

Connected Cars and Driverless Vehicles: Safety and Privacy Concerns

While driverless vehicles are yet to appear on Canadian roads, more and more passenger cars come off the lot already "connected," allowing parents to monitor and control teen drivers and employers to monitor employee driving habits. In addition, small gadgets can be attached to a car to allow for remote monitoring and, in some cases, remote control.

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

Driverless Cars

Some car manufacturers, rideshare services, and cargo delivery businesses are touting the future of self-driving cars. These cars combine a wide variety of sensors and systems that navigate a vehicle through city traffic and on long stretches of highway. In almost all cases, the cars still require a person to be present in the driver's seat to take over if there is a problem. Many cars on the road today already include basic computer-assisted features where a computer assists the driver with a function, such as automatically engaging the brakes.

Connected Cars

Several services on the market today are designed to monitor and control the driving decisions of employees and teen drivers. These services are used to track driving habits and location and then deliver the information via an electronic report or with real-time updates. Options to control a car remotely or through pre-set limits include limiting car speed and audio volume or blocking texts or app alerts from reaching a teen's phone while driving. These could also be misused by a perpetrator to control a woman's vehicle.

A limited number of vehicles come with these services built-in, while many others work by plugging in a small device to the onboard diagnostics (OBD) port. The OBD system is a part of the car that many drivers aren't aware of – it's a computer that can monitor emissions, mileage, speed, and other data. Some available apps also bypass the need for a plug-in device by using the driver's smartphone to gather and send information and block incoming messages.

Safety and Privacy Risks

The primary safety risk with connected cars is the possibility of remote control of the car. The most extreme risk would be crashing a car by taking over control of steering, braking, or acceleration. Other serious risks include taking control of the stereo volume, lights, horn, windshield wipers, and other features that could distract or disturb a driver and lead to accidents. Hackers have demonstrated that it is possible to hijack control of all of those features in cars currently on the streets.

Privacy risks stem from tracking and sharing information about driving habits and location. Built-in, plug-in, and smartphone apps can all share information with someone remotely, providing the opportunity for monitoring and control. Manufacturers also store information collected from vehicles, which can pose a privacy risk related to unauthorized access.

Benefits of Connected and Smart Devices

While the risks of connected cars are deeply troubling, there are ways that the technology can be used strategically to increase safety. A woman who is concerned about the location of a car or its passengers could use these features for reassurance or direct emergency services in case of theft or abduction. A woman could also choose to share her location with trusted friends or family. Finally, a perpetrator's movements or driving habits could be used as evidence.

Questions about IoT Devices

When considering purchasing connected cars, devices to plug into cars, or apps, 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 privacy and safety include learning about the built-in security options, turning off features 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 Connected Cars and Driverless Vehicles Safety and Privacy Concerns.

Connected Health and Medical Devices: Survivor Privacy, Risks, and Strategies

Many health and medical devices are now connected to the Internet, offering to help track information for the user or even send that information to a doctor. Unfortunately, these devices and systems can provide yet another, highly invasive way that technology can be misused to monitor, harass, threaten, or harm survivors. At the same time, they can also offer potential tools to strategically increase safety. There have already been examples where data from these devices was used successfully as evidence in criminal cases.

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

Below are some examples of connected health and medical devices.

Consumer Electronics

An increasing number of devices are marketed to help people get active, lose weight, and support a healthy lifestyle. The most common devices are step trackers and smartwatches. Exercise machines now offer to connect to a mobile device to track and share information about the duration and intensity of a workout, as well as vital signs like heart rate. Athletic shoes can be connected as well, sharing information including location.

Medical Devices

Newer devices for tracking vital signs collect, analyze, and share information, including blood pressure monitors and thermometers for tracking fertility. Medical equipment such as wheelchairs, pacemakers, and pill bottles can include the capability of tracking location or frequency of use and reporting that back to a doctor or medical facility.

Privacy and Safety Risks

While everyone may face privacy risks from unauthorized access to data from health and medical devices, women experiencing violence face specific risks to privacy and safety. Information about location, physical activity, vital signs, or habits could be misused to threaten or harm her. Sensitive personal information could be shared publicly in an attempt to ruin a woman's reputation. For example, usage data from connected sex toys used by a woman as part of healing from abuse could be shared with an employer or others. Inadequate built-in security of devices, and the data they gather, raises concerns that the devices could be tracked or even disabled remotely. Additionally, information from connected devices is being fed into large sets of data held by companies and governments. These data sets may contain identifying, inaccurate, and potentially damaging information.

Potential Benefits to Survivors

Women with disabilities or those who face complex medical issues, have trouble remembering health-related tasks, or simply want to improve their health, may benefit from connected devices. The effects of trauma can hinder the ability to remember daily tasks, decrease motivation for physical activity, or impact heart rate and other vital signs. Connected devices could be part of a plan to improve well-being or track the impacts of trauma. The use of specific health and

medical devices may help to lessen symptoms and illnesses that result from trauma or physical injury. All of these benefits may be undermined by a lack of privacy and security, so women and any health professionals they are working with should take these factors into account when selecting devices.

Evidence

Recent news stories have covered cases in which data from health and medical devices have been used as evidence in criminal cases in the United States. Information about location, movement, and vital signs are likely to be used in future to support or counter a version of events surrounding crimes. This same evidence may also be used in civil legal settings to support protection orders or family law matters.

Evidence from connected health and medical devices may be stored on the device itself, on a mobile device, in a user's account, or on the server of a manufacturer or medical provider. In some cases, a woman may have access to the data, and in other cases, a subpoena or court order may be necessary to access the data.

Questions about Health and Medical Devices

When considering connected health and medical devices, there are a few questions to consider:

- Does that particular device truly 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 individualise and increase privacy and security?

Strategies to Increase Privacy and Safety

Steps to increase privacy and safety 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. Ask doctors about using a device that is not connected to the Internet, or alternatives like keeping a handwritten log of the information that would otherwise be shared or other ways of setting up reminders to take medication or exercise.

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 Connected Health and Medical Devices: Survivor Privacy Risks and Strategies.

This document is part of a series of resources provided through Women's Shelters Canada's Tech Safety Canada project. We encourage you to visit www.techsafety.ca to find additional information and resources about technology-facilitated violence, technology safety planning, and preserving digital evidence. This document, or any portion thereof, may be reproduced or used as long as acknowledgement is included. If you would like to adapt the content, please contact Women's Shelters Canada at info@endvaw.ca.

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