NNEDV

Privacy and Safety with IoT Devices

What is "IoT"?

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 a survivor. At the same time, they can also offer potential tools survivors can use to strategically increase their safety.

Safety Net has developed a series of handouts describing the risks and potential benefits of the new wave of IoT devices.

Home Automation & 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. Home automation IoT allows remote control and surveillance through Internet-connected devices in the home. Read more.

Connected Health & Medical Devices

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

Smart Toys & 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. Read more.

Smart Cars & Driverless Vehicles

While driverless vehicles get all the headlines, newer cars often 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. Read more.

Steps to Increase Safety & Privacy

Across the spectrum of new IoT 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 is the device and the app that runs it? Are there features that allow the user to individualize and increase privacy and security?

General steps to increase the privacy and safety of IoT devices 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.

We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.