Home Automation:
Survivor Privacy Risks & 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 a survivor.

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, the Internet and WiFi, Bluetooth, or other means.

These devices, systems, or apps allow remote control of Internet-connected devices in the home:

- **Personal Assistants** (Google Home, Amazon Echo/Alexa, etc.). 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** (Nest, Arduino, etc.). 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, and 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 lightbulbs
- Smart electrical outlets (with lights or other devices plugged into them)
- Entertainment systems (stereo, TV, etc.)
- 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 (refrigerator, vacuum, etc.)
- Pet feeders, nanny or pet cams, toys and trackers
- Children’s toys and trackers

IoT 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 behavior - 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 video 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 to return to it. A video doorbell could be used not only to monitor who comes to the door, but to harass them remotely or, in combination with a smart lock, prevent them from entering the house.

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

Safety Planning & 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 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.

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, the time of day, related events like contact, visitation, or court proceedings?
- Does the person misusing the technology have access to the home or to 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, a next step would be 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 the victim 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 in order to change account ownership and access.
- Changing router or network settings. For more information, see our handout on WiFi security.
- Replacing the devices (lightbulbs, the thermostat, electrical outlets or other connected devices) to either remove those devices from the system, or to regain control over the system.

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

The Digital Divide & Home Automation

As is the case with many kinds of emerging technology, high costs currently make some of these devices more prevalent in wealthier homes and businesses. That said, when working with survivors, we shouldn’t make assumptions about the use of IoT devices based on economic status. And as costs come down, the devices will also become more widespread. Bear in mind that these devices may also be used by other parties in ways that can compound trauma. For example, a survivor in low-income housing might find that a landlord is misusing a video doorbell to restrict access or inappropriately monitor activity.

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 could be used to notify a survivor when someone approaches or enters the house. These devices might also gather evidence to document violations of a protection order or other criminal behavior.
- Smart lightbulbs might provide peace of mind to a survivor by illuminating the house or a room before a survivor enters it.
- Pet cams and feeders might provide needed support or comfort to a survivor when they are away from home, or help reassure the survivor of a pet's health or safety.
- Energy saving devices might help to reduce the financial burden of living independently from an abuser.
- Home automation can provide assistance to survivors 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 is the device and the app that runs it? Can that security be strengthened?

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.