Evidence Collection Series:
Internet of Things (IoT)

Where to begin?

This technology-specific guide is a part of a series that details how to collect evidence related to the misuse of technology in domestic violence, sexual assault, and stalking cases. Before proceeding, we recommend that you read A Primer for Using the Legal Systems Toolkit: Understanding & Investigating Tech Misuse, Approaches to Evidence Collection: Survivor Considerations, and Approaches to Evidence Collection: Criminal vs. Civil Systems.

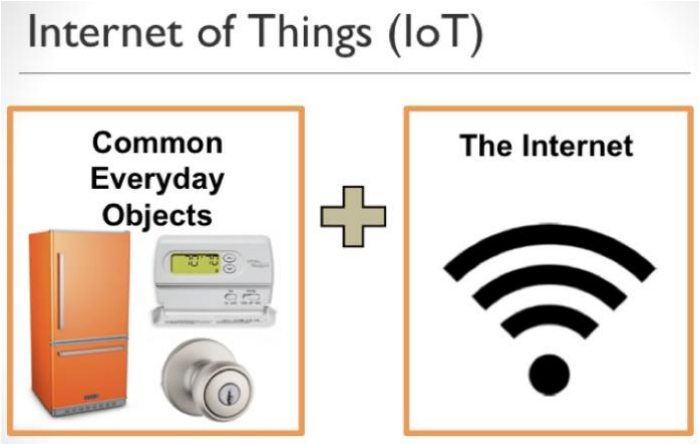
Who should use this resource?

The series is part of a Legal Systems Toolkit that includes guides to assist prosecutors, law enforcement, and civil attorneys.

IMPORTANT TIP/NOTICE FOR ADVOCATES: If you are a non-attorney survivor advocate, we strongly recommend that you do NOT gather or store evidence for survivors. You can greatly assist survivors by giving them information to gather evidence themselves. Your participation in the process of gathering or storing evidence can lead to you being forced to testify in court, which can undermine confidentiality protections and negatively impact both the survivor and the integrity of your program. If you have questions, please contact Safety Net.

IoT: An Introduction

The term or phrase Internet of Things (IoT) refers to a wide variety of devices with different purposes, functions, and capabilities. IoT devices may be connected and controlled through the Internet, Bluetooth, or other means, which makes them practical and efficient tools that can be used to improve quality of life. Survivors can also use IoT to increase their safety. However, these devices or systems can also be misused to monitor, harass, threaten, and isolate. More information about the risks and benefits of IoT devices can be found at TechSafety.org.



IoT devices themselves are not the problem, but rather the misuse of them. For domestic violence, sexual assault, and stalking survivors, the intimate role IoT devices play in people's lives can pose an especially dangerous risk.[1] Investigating IoT abuse can be challenging since the devices can be used to *remotely* harass or threaten victims.

As with most technologies, there are many ways that IoT can be misused. While the possibilities of misuse are evolving with the devices, we will discuss some of the more common types of IoT misuse currently known.

IoT: The Technology

To assist in investigating and uncovering IoT misuse, this section provides examples of different kinds of IoT devices, possible misuses, and security suggestions.

IoT devices are commonly in the home or worn as an accessory, and may be misused to harass or track a victim's movement. The following chart provides examples of common IoT items that can be misused or that may contain useful evidence.

[1] https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

Smart Appliances: Speakers, home assistants (e.g. Amazon Alexa, Google Home), kitchen appliances, TVs, etc.
Smart Home Systems: Doorbells, thermostats, lighting, security cameras, baby monitors, etc.
Wearable Items: Health trackers (e.g. FitBit), medical devices (e.g. pacemakers), sleep trackers, eye glasses, watches, panic buttons, mood sensors, clothing, etc.

Ways to Connect and Access IoT Devices

- ***Apps and Websites:*** Many IoT devices communicate with other devices, like a smartphone, through the use of apps or websites. These apps or websites enable a user to manage the IoT device settings and to track activity. There are also apps, like Wink Hub[2], that allow users to connect all their IoT devices on a single app for convenience.
- ***Networks:*** A network is what connects different IoT devices and allows them to "speak to each other". This is typically a WiFi network in someone's home. IoT devices can also connect to each other via Bluetooth. For example, a survivor's Alexa home assistant can communicate to their smart speaker system, so that when a song is requested to Alexa it automatically plays on the home speakers.[3] Because many IoT devices share a network, each individual device is only as secure as the most vulnerable device connected to that network. Any insecure device on the network can potentially serve as a doorway into all the other devices. Therefore, it is essential to examine whether the network itself has been breached and whether there are ways to increase the security for all connected devices, and their systems.
- ***Multiple Device Access:*** Most IoT devices are designed to connect to multiple mobile devices (e.g. smartphones) at the same time. It is not uncommon for individuals in intimate relationships to share access to their IoT devices, which

[2] https://www.wink.com/products/wink-hub/

[3] WiFi networks function using the internet while Bluetooth is a separate technology that connects devices that are near one another. https://www.techopedia.com/2/27881/networks/wireless/what-is-the-difference-between-bluetooth-and-wi-fi

means that those devices may have multiple mobile devices that are connected to their network, with or without the knowledge of the survivor.

IoT and the Law

Unlike many other consumer products, there are no federal regulations specifically for IoT products and few if any laws that specifically regulate IoT activity. Some devices, like those used in medical institutions, are regulated because of the laws already covering those industries. The National Institute of Standards and Technology (NIST), has studied IoT devices and created a list of general IoT safety standards, including security risks like hacking and data breaches.[4]

Currently, laws that specifically make abuse through IoT devices a crime are lacking, although many other existing laws may apply. Laws that focus on abusive behavior, such as harassment, spying or surveillance, intercepting communication or eavesdropping, or stalking may be able to be applied in some IoT abuse situations. It may require creatively using available laws. For example, inappropriate access to a victim's IoT device or network without permission, could result in a computer-related crime or a civil lawsuit for invasion of privacy (or similar laws). A victim may also be able to request a protection order if they believe they have experienced abuse and are at risk of IoT abuse. A protection order can include provisions that require the abusive person to not interfere with IoT devices or related accounts, and to remove themselves from those accounts. Proactive protective order provisions may help prevent future incidents.

While the law catches up to the technology, IoT evidence is already making its way into the court system. In a recent case, evidence from a murdered victim's FitBit was used to help prosecute her husband.[5] The increased use of IoT technology is leading to an explosion of new information that may prove indispensable in proving future cases.

[4] https://www.nist.gov/topics/internet-things-iot
[5] https://www.nytimes.com/2017/04/27/nyregion/in-connecticut-murder-case-a-fitbit-is-a-silent-witness.html

Investigating IoT Devices

The first step when investigating IoT abuse is to help survivors identify internet connected devices in their homes, work, transportation, including things they use or wear to determine whether those devices, are being misused, or have been breached. If so, they may contain valuable evidence.

Sometimes it can be difficult to know which devices are Internet-connected. Smart speakers, TVs, or home assistant devices are more commonly understood to connect through WiFi. However, victims don't always know that many common items (like refrigerators, thermostats, and toys) can be connected to the Internet or shared networks. Survivors may have difficulty identifying all of the places to look for Internet-connected devices, systems, and products. It can be helpful to provide a list of common IoT devices, such as the chart on page 3. Knowing which items are at risk can help guide safety planning strategies and evidence collection.

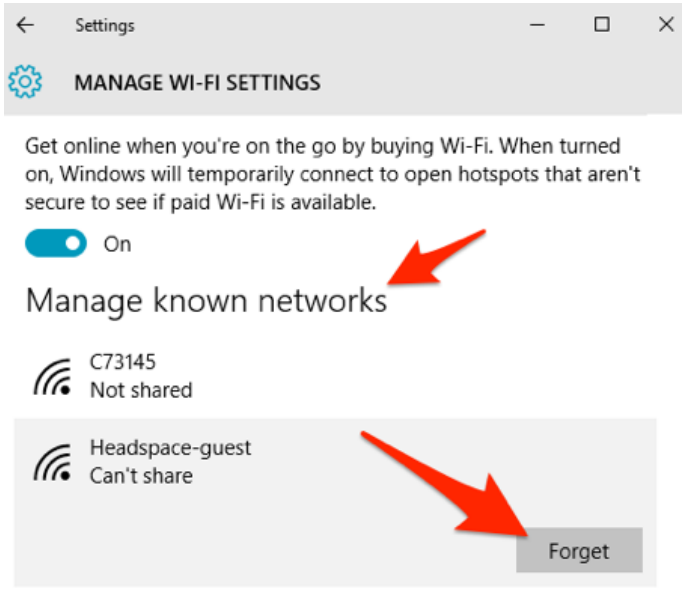
One strategy for identifying what is connected to their network is to access their WiFi router. The router keeps a list of all connected devices, as well as what IP address they have been assigned and other network related information. This will show what is connected, both wirelessly or by a cable, but it will NOT tell you what is connected to another device via Bluetooth.

Tips for Getting Survivors Involved in Evidence Collection

Help the survivor understand how to protect, collect, and preserve evidence. Read more about the importance of involving survivors in the process of collecting evidence in Approaches to Evidence Collection: Survivor Considerations. Survivors' active participation can lead to information that may strengthen the case, and can give survivors essential tools for safety and healing regardless of the outcome of the case.

Look for Shared Devices and Networks

- If the abusive person shares or has shared a home or any device with the survivor, then they could have direct access to those devices or to the accounts that control them. For example, an abusive person who knows the password to a thermostat system could control the thermostat remotely, anywhere the abuser has internet access.
- An abusive person can also misuse an IoT device by downloading spyware or hacking into the actual device, network, or account linked to the device. Certain apps can scan devices to see who is connected to a network or router if the user is near the victim's network, but they do not always work in locating abusive persons operating from a greater distance. An important first step is to identify which devices are connected to the IoT network. Generally, that information is found by locating "settings,"
  exact steps may differ depending upon the device and network. An online search for "how to find out what devices are connected to [name of IoT]" will provide further information in most cases.



Document Changes or Suspicious Activity on Account

There may be vital information available in the survivor's apps, websites visited, account information, passwords, and device settings. Sometimes a simple password change, being locked out of an account, or an unusual change in a

survivor's app settings can show that an abusive person has accessed or tried to access the device. However, it is not always easy to identify some of these clues. A more in-depth search of the information or account by a forensic investigator may be required.

Changes in settings or account information should be documented by videos, photos, or screenshots, if possible. Many IoT devices also have online or in-app activity logs, which can be useful in identifying misuse. Some additional options to explore for evidence are:

- A message or notification that a password has been changed without the survivor's knowledge
- Any change in identifying information (name, address, phone number, etc.)
- Any change in functional settings (e.g. temperature selected, doorbell ring option, any automatic feature by the user)

Track Usage and Timing

Any changes or suspicious activity in the real-time use of the IoT devices should also be documented. Are lights turning on without the survivor initiating it? Are devices making unusual noises? Does the abusive person have knowledge of any incidents involving the survivor or their private information that could have been learned through an IoT device?

Physical observations should be logged and whenever possible, a safe device should be use to take videos, photos, or recordings as proof. A log of strange activity can be important to understanding the full scope of the misuse. The timing of misuse can be compared to the normal activity of the survivor.

Accounts linked to the IoT devices can also provide information about unusual activity. Screenshots or printed copies of this logged information can then be compared to any unusual activity captured live by videos, photos, or audio recordings. Whenever possible, screenshots or videos should include date and

time. Proof of digitally logged activity combined with physical evidence of the activity can strengthen a case.

Law Enforcement May Need to Investigate

Law enforcement are usually the first to interact with survivors once a crime has been reported, which means they play a significant role in the early stages of collecting evidence. Law enforcement generally have the tools to do a more advanced search of devices and networks. If the survivor makes an informed decision to involve law enforcement, it may strengthen the ability to search the actual hardware of the devices, as well as their linked accounts and networks. Some examples of evidence that may be more accessible in criminal investigations include (but are not limited to):

1. Records on the abusive party's device that show it was used to remotely control IoT.
2. IoT company records including the IP addresses of remote sign-ons, which can be compared with the abusive person's IP addresses.
3. The abusive person's online activity via WiFi network or ISP, that shows evidence of IoT abuse against the survivor.

Get a Court Order to Collect Records

If the information is not available through the account or the survivor does not have access to the information, a court order for the records might be necessary to collect evidence of IoT activity. Gaining access to account records for IoT apps and websites, WiFi networks, or the abusive person's own devices, networks, smartphones, or computer activity can help prove misuse. At the very least, it can help strengthen a survivor's case.

Differences Between Civil and Criminal Investigation

The process of evidence collection may look different depending on whether the investigation is for a criminal or civil case. While survivors will be important resources in all case types, the evidence available may differ. Approaches to Evidence Collection: Criminal vs. Civil Systems discusses important differences in the two systems and offers tips for professionals in each system.

IoT Safety Tips

If a survivor thinks they are at risk or has already experienced IoT abuse, the following general security tips may be useful.

Create Separate Networks

IoT devices are convenient in part because they rely on shared networks. This same network can then also be linked to a user's email, mobile, and other online accounts. Networks can be private and require a password or they can be public, meaning anyone who is physically close enough to the WiFi can connect and use it. Read more information about WiFi network security.

Create Strong Passwords

Make sure all WiFi network, accounts, and websites linked to the IoT devices have strong passwords. Discuss with survivors the importance of protecting passwords, especially if there is a higher risk of IoT abuse. Read more about strong passwords.

Regularly Update IoT Devices

Software updates include security improvements. IoT users should regularly check for available updates, so their devices have increased protection against hacking or spyware. Updating devices does not eliminate all risk, but it can significantly strengthen device and network security.

Hit Mute and Block Camera

With IoT devices that record audio or images, it is generally a good idea to block the lens of cameras when not in use and to mute sound recording options. If they are hacked into or accessed by an abusive person, this can prevent the abusive person from being able to see or listen to the survivor.

Seek Support from IoT Manufacturers

Survivors may want to communicate with the companies that build or run their IoT devices, to let them know about the abuse. The company may be able to provide suggestions and to help institute protections. For example, it may be

possible to add security or block the abusive person's devices or locations, preventing them from accessing to a device or account. This may not always be possible and may not be the best option for preparing evidence for court, but survivors should decide what would be the best solution for their own situation.

IMPORTANT: Be sure to help the survivor to make a safety plan, in case removing access escalates an abusive person's behavior. Refer victims to a local advocate who understands tech safety, or let them know about the resources in our Survivor Toolkit at TechSafety.org.

Carefully Consider Use of IoT Devices

Because IoT devices can give a large amount of access to private spaces, people should carefully consider their own needs and weigh the potential risks and benefits of using IoT devices. A survivor may decide that the practical benefit of using an IoT device outweighs the possible threat of abuse. Some survivors may decide to temporarily take a break or entirely give up IoT devices until they feel safe to use them. We do not recommend telling survivors to get rid of IoT, but instead believe that a thoughtful conversation about the pros and cons can help survivors to weigh their needs and risks.

Provide Support

If a survivor feels that IoT devices are being misused, they should be supported in trusting their instincts. Many survivors have people telling them that their experiences are not real or that their instincts are wrong. Sometimes it can be useful to let them know that IoT devices can be used to cause harm and that they should document what is happening to them.

Next Steps in your Investigation

Proving technology abuse can be challenging, however it *is* possible to successfully prove tech abuse cases through effective investigation and creative advocacy. For more information, see the resources in our Evidence Collection Series.

If you have further questions about investigating tech abuse cases, please contact Safety Net, and visit TechSafety.org for more information.

Special thank you to Bryan Franke of 2CSolutions for providing expertise and guidance on the creation of this series.

Supported by US DOJ-OVW Grant No. 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.