Where to begin?

This 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 the survivor the skills to gather the 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.

**Spyware: An Introduction**

Mobile devices hold intimate details of our lives and this single access point for information is usually a convenience. But for survivors of domestic violence, sexual violence, or stalking, an abusive person can misuse spyware to access a terrifying amount of information.

This document includes information about how to identify a spyware case, how and where to look for evidence of spyware, and tips for gathering evidence.

**Spyware: The Technology**
“Spyware” refers to software applications that give a person remote access to a device, allowing them to monitor and collect information and device activity. To install spyware on a mobile device, a person generally must have physical access to the device, or convince the user to install the software, often through deception. For Apple products, devices will generally need to be jailbroken before these applications can be installed. While the Play Store for Androids does not allow applications to run covertly, the Android operating system does not enforce this requirement and spyware can be installed.

**Dual-Use Applications and Tools That Can be Misused**

In addition to spyware applications that have a main purpose of remotely spying on someone, there are also applications that have legitimate purposes, but can be misused to access a device remotely or receive data from it. Dual-use applications may be purposefully downloaded by the user and they may not even be aware the abusive person has remote access to their device data through it. For example, the Find My Friends or Find My iPhone applications on iPhones can be used to surreptitiously track a user.

There are also many applications with secondary *features* that share location data. For example, if certain settings are used, Snapchat or Google Maps may be misused to access the location information of someone’s device. Depending on what information the abusive person knows, it may be helpful to assess for the misuse of these types of apps as well.

**Analyzing Spyware Cases**

Though the use of spyware in domestic violence, sexual violence, and stalking cases has been well-documented for almost two-decades—first with computers and now with mobile devices—the methods used to monitor and collect information about survivors are often complex and may or may not include spyware. It can be useful to start an investigation by considering all possible sources—including non-spyware options—for how an abusive person could be inappropriately obtaining information.
Step 1 – Give the survivor the benefit of the doubt.
When a survivor is concerned that an abusive person knows too much information about them, tell them to trust their instincts. Ask about what information the abusive person seems to know and help them document behaviors and events to see if there is a pattern. For example, the abusive person might show up at places the same time as the survivor or may drop hints that they are collecting information about the survivor. In one case, a survivor was looking at a particular pair of shoes online and shortly after the abusive person sent the survivor the exact URL and said they would look great on her. Hints, however, are not always so blatant. It is important to walk through experiences that have caused the survivor concern.

Step 2 – Identify what information the abusive person is accessing.
Identify each piece of information that the abusive person appears to have access to. For instance, if the abusive person consistently shows up at the survivor’s work, despite varying shift times, there may be a leak in the survivor’s workplace (i.e. a coworker) or the online scheduling software, or maybe the schedule is emailed to an account that is being monitored. If the survivor has gone to three different grocery stores and the abusive person has shown up each time, the abusive person may be accessing their real-time location through GPS.

Step 3 – Consider social explanations.
The most common, non-technological explanation for an abusive person having too much information about a survivor is a friend or relative leaking the information. Friends or relatives might not understand the entire situation, and may unwittingly provide information. Alternatively, someone may be spying on the survivor and purposefully reporting to the abusive person.

Ask the survivor if any friends or relatives were privy to the information in question. Then, from that list of people, ask if any of them are or could be in contact with the abusive person. If so, the survivor may need to tell them to stop
sharing information, or the survivor may need to stop sharing information with them.

Step 4 – Consider everyday features and apps that contain the information. An abusive person may inappropriately access information by misusing everyday features and apps used by the survivor. For example, they may know or have guessed a password or be physically looking through phone activity while the survivor’s phone is unattended.

Ask the survivor where each piece of information may be stored. Is the work schedule in their email? Does the abusive person have access to the Find My iPhone feature? Knowing where the information is located will help narrow the focus in determining how the abusive person is getting the information.

Step 5 – Consider information the survivor shares publicly. Some survivors may unwittingly share private information through publicly accessible accounts, including social media. For example, they may have posted about their work shifts and not realized the privacy setting was set to public.

It is important to understand what the survivor chooses to share about themselves and how. An online search for the survivor can be helpful. Identify what social media platforms are used and then identify what information is accessible or visible to the general public. They may be posting publicly, rather than privately or the abusive person may be connected to a third-party who can see that activity. Help survivors review privacy settings so they can make informed choices about who has access to their information.

Step 6 – Look for evidence of spyware. If no other leaks of information can be identified or if the abusive person knows too much without explanations, look for evidence of spyware.
**IMPORTANT:** If you believe the survivor is being targeted by spyware, **one of the safest things the survivor can do is use the phone as though nothing is wrong.** Normal use will avoid tipping off the abusive person of suspicions, allowing more time to collect evidence before it is destroyed. It is important to speak with survivors about the pros and cons of this strategy, as well as strategies to use their devices in more secure ways. Some people may feel safest getting rid of the device or doing a factory reset to try to rid of the spyware.

**Preparing to Gather Spyware Evidence**

Often, domestic violence, sexual assault, and stalking cases lack documentary evidence or witnesses, and cases are determined by which person’s testimony is believed by the courts. Evidence of spyware misuse can clearly demonstrate how the abusive person created an environment of fear and control.

Unfortunately, useful evidence is not always properly sought out, is accidentally deleted, or is not collected properly. Below, we will describe how to collect and maintain evidence to increase its usefulness in court. You can also read about the differences in technology evidence collection between criminal and civil cases.

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

**Identify Types of Evidence**

The existence of spyware can be difficult to uncover as the application may be hidden or may not clearly disrupt the regular use of the device. It can be especially difficult to prove the misuse of dual-use applications because it must be shown that the application is present and that it is being manipulated to obtain remote access to device data without the survivor’s knowledge or permission, or with coerced permission.
Protect all of the mobile device’s data.
In some cases, direct evidence of spyware on a mobile device can only be obtained with the help of a forensic professional. It is important to protect all data since you may not know immediately what to look for and it may be needed later by a forensic professional.

Throughout your investigation and evidence collection process, help the survivor build a picture of what leads them to believe spyware is being used. They may have seen a receipt for a spyware company on the abusive person’s computer or the survivor may have information that the abusive person used this type of software against another person. Even without this information, asking open ended questions may encourage a survivor to share information that may help the investigation.

**NOTE ABOUT PASSWORDS:** Usually when technology is used to facilitate abuse, it is a good idea to help the survivor to change their passwords and to disconnect other devices from accounts. However, if spyware is on the device, it is not safe to change passwords on that device. Create a plan on how to change passwords without alerting the abusive person, such as using a separate, safer device. Once a plan is created, you can help the survivor create strong passwords.

Create a list of information that will help the case.
You may not know all the experiences that have led the survivor to believe the abusive person has access to information, which limits your knowledge of what experiences are relevant. The survivor may not be familiar with the justice system and may be unaware of what is most important for court. Have a detailed conversation with the survivor, and encourage them to share as much detail about the situation as they can remember. It is also important to be very clear about what kind of information you are seeking.

Help the survivor understand how to protect, collect, and preserve digital evidence. Read more about the importance of involving survivors in the process.
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.

Next Steps in your Investigation

Spyware misuse is one of the most invasive forms of tech abuse, and investigations can be extremely complicated. However, it is possible to successfully prove spyware cases through effective investigation and creative advocacy. For more information, see the resources in our Collecting Evidence Series. If you have further questions about investigating tech abuse cases, please contact Safety Net, and visit TechSafety.org for more information.

Additional Resources

- Spyware, Surveillance, and Safety for Survivors
- 12 Tips on Cell Phone Safety and Privacy
- Technology Safety Quick Tips
- Admissibility of Forensic Cell Phone Evidence
- How to Gather Technology Evidence for Court from the National Center for Juvenile and Family Court Judges
- Avoiding Cell Phone Spyware Infestation
- Vice, Motherboard: When Spies Come Home Series
- How to Protect Yourself from Creepy, Phone Snooping Spyware
- How To Bust Your Boss Or Loved One For Installing Spyware On Your Phone

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

© 2018 National Network to End Domestic Violence, Safety Net Project. Supported by US DOJ-OVW 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.