Stalkerware and Location Tracking

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.

Phone Stalkerware and Safety Guide

What Is Stalkerware?

Stalkerware refers to tools – apps, software programs, and devices – that enable another person to secretly monitor your phone activity.

Stalkerware can monitor almost everything you do on your phone, including photos and videos you take, websites you visit, messages you send and receive, your call history, and your location. Stalkerware can allow someone to turn on the webcam or microphone, take screenshots, see activity on third-party apps (such as Snapchat or WhatsApp), and intercept, forward, or record phone calls.

Almost all phone stalkerware requires physical access to the device to install. Once installed, it runs in stealth mode without any notification or identifying activity and is difficult to detect or remove. To access your phone activity, the person monitoring you signs in to a website or app on a different device. They may also receive notifications of certain activities, such as copies of text messages or an alert that you are on a call so they can secretly join and listen in.

How Do I Find Out if Stalkerware Is on My Phone?

Detecting stalkerware can be difficult. Some signs could include your battery draining rapidly, your device turning off and on, or spikes in your data usage. The most common sign that your activity is being monitored will be the other person's suspicious behaviour. They may know too much about your phone activities, for example. Trust your instincts and look for patterns. A trained professional may have to check the device to know for sure.

Responding to Stalkerware

Safety first. Before looking for or trying to remove stalkerware, think about your safety. Some people may escalate their abusive behaviour when stalkerware is removed. You can speak with an anti-violence worker about safety planning.

If you suspect stalkerware, what you do on your phone could be seen by the other person. For calls or online activity where you want more privacy, use a phone or other device that isn't being monitored. This could be a friend's phone or a computer at a library, school, or work.

Documenting the Stalkerware

You can make notes about what you're experiencing. Our Documenting Digital Abuse info sheet and sample Technology-Facilitated Violence Log will provide you with some helpful information.

Alternatively, when you're ready, some police or forensics experts can look for evidence on your device. It may also be worth reading WSC's Preserving Digital Evidence Toolkit on a device that is not being monitored for more helpful documentation tips.

Removing Stalkerware

In most cases, a full factory reset can remove the stalkerware. However, reinstalling apps or files from a backup can re-load it onto the device. In addition to doing the factory reset, you could also create a new iCloud or Google account for your device so you're starting the device with a blank slate without any option for the stalkerware to be reinstalled.

Preventing Stalkerware

- **Consider access.** Be cautious if someone wants to update or use your phone. Stalkerware is easy and quick to install. Trust your instincts. Beware of gifts of a new phone or tablet from the perpetrator to you or your children.
- **Update accounts.** Change passwords and set up two-factor authentication. Read more about Password Safety.
- **Lock your phone.** Because most stalkerware requires physical access to the phone to install, place a passcode lock on your phone (and don't share it) to minimize risk. Many devices allow you to choose between a number, pattern, thumbprint, or other security features. Read more Phone Security Tips.
- **Use anti-virus and anti-stalkerware protection.** Download security apps to your phone; these apps can help prevent stalkerware from being installed and can scan your phone for malware or stalkerware apps.
- **Use security features.** Review the security features under your settings to learn what is available on your devices. Android phones allow installations from "unknown sources"; make sure this is turned off. Always install the latest updates for your phone and apps. Not doing so can make them more vulnerable to security and privacy issues.
- **Do not "root" (Android) or "jailbreak" (iPhones) your phone.** "Rooting" or "jailbreaking" a device means removing the operating system limitations to allow for third-party installations (ones not in the app stores). Doing this impacts the built-in security features designed to protect the device and makes the device vulnerable. Many of the more invasive stalkerware features don't work unless the protections put in place by the manufacturer are bypassed. On

iPhones, most stalkerware cannot be installed unless the device is jailbroken. A rooted or jailbroken phone will be more vulnerable to viruses and malware, making it easier for stalkerware to be installed.

[KG1]Link to 1.24

link 1.08 [RW2]

When It's Not Stalkerware

There are many other methods someone can use to access information on your phone or know your activities without installing stalkerware. If the perpetrator has physical access to the phone or your cloud accounts, they may not need to install stalkerware to monitor you. Sometimes, the perpetrator uses friends and family members to gather information. Look for patterns in what the person knows and where that information might have come from to help you to narrow down the possibilities. An anti-violence worker can help you figure out what may be happening and plan next steps.

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 Stalkerware: Phone Surveillance & Safety for Survivors.

Spyware and Stalkerware: Computer Surveillance and Safety

What Are Spyware and Stalkerware?

Spyware and stalkerware refer to tools – apps, software programs, and devices – that let an unauthorized person (such as a perpetrator) secretly monitor and record information about your computer. The term "stalkerware" is a more recent term that draws attention to the invasive, intrusive, and dangerous misuse of these tools.

Spyware can keep track of almost everything you do on your computer, including every keystroke typed, website visited, online chat or instant message sent or received, and documents opened. Some spyware can also allow the person who installed it to turn on the webcam or microphone, take screenshots, make the computer talk or make other noises, or shut down or restart the computer. The abusive person can view your computer activities or control your computer remotely, generally via a website dashboard or accompanying app.

Most computer spyware can be installed remotely, usually by sending an email or message with an attached file or link. The spyware automatically installs when you click on the link or open the attachment. Some spyware products can be sent through an instant message, computer game, or other ploys to entice you or your children to open the attachment or click on a link. Once installed, it runs in stealth mode without any notification or identifying activity and is difficult to detect or remove.

While most spyware is installed as software, there are also hardware-based spyware devices called keystroke loggers. These keylogging devices may appear to be normal computer parts; for example, it can be a special keyboard with keystroke logging capabilities or a small device that connects the keyboard to the computer. Once the keylogger is plugged into the computer, it records every key typed, which can include passwords, personal identification numbers (pins), and websites visited. Some hardware devices allow for remote spying while others require the abuser to have access to the hardware to access information about the computer activity.

How Do I Find Out If Spyware Is on My Computer?

Detecting spyware on your computer can be very difficult. In most cases, a computer with spyware installed will not have noticeable changes in the way it operates (e.g. your computer won't necessarily slow down or freeze up). Even without these things happening, however, you might suspect that your activity is being monitored because of the abuser's suspicious behaviour. Trust your instincts and look for patterns. If the abusive person knows too much about your computer activity or knows things that you've only done on your computer or phone, spyware may be on your device.

If a hardware device has been installed, you might see an additional component between the computer and the keyboard cord, or you might suddenly have a new keyboard or mouse. On laptops, a hardware device may not be as noticeable since it would be installed inside the laptop, through the access panel.

Responding to Spyware

Safety first. Before acting to find or remove spyware, it is important to consider safety and the possibility of collecting evidence. Since many perpetrators use spyware as a way to monitor and control women, they may escalate their harassing and abusive behaviour if they suspect that she is removing the spyware and cutting off their access. Before removing the spyware, think through your safety as you consider ways to protect yourself, and talk with an advocate about safety planning. If you need an anti-violence worker, please go to www.sheltersafe.ca.

Gather Evidence

Law enforcement or a computer forensics expert may be able to assist you if you want to preserve evidence needed for a criminal investigation or civil legal action. Forensic tools may be the only way to determine for sure if spyware is on a computer. Read more about spyware evidence in WSC's Preserving Digital Evidence Toolkit.

Use devices that aren't being monitored. If you suspect that spyware is on your device, remember that all activity including online chat, emails, and web searches, can be revealed to the perpetrator. If you can, use a safer computer or device – one the person does not have physical or remote access to – when you look for help or information. This may be a computer at a public library or community center or a friend's device.

Remove Spyware

Spyware on a computer can be very difficult to remove once it's installed. You can consider wiping the computer and rebuilding the computer starting with reinstalling the operating system, although this will not guarantee complete removal. Another option is to replace the hard drive of the computer or get a new computer. Be careful not to copy files or documents from the infected computer onto the new computer, which could reinstall spyware hidden in the files. Use online cloud services to store documents from the infected computer.

Update Accounts

Since spyware would have given the perpetrator access to your login information, consider resetting your passwords on a different device and no longer accessing certain accounts from the computer you are concerned is being monitored. Also consider changing passwords to sensitive accounts such as online banking and social media accounts. Read more about password safety.

Preventing Spyware

Consider access. Be suspicious if someone abusive wants to install a new keyboard, cord, or software, or updates or "fixes" the computer or phone – particularly if this coincides with increased monitoring or stalking. Beware of gifts from the perpetrator to you or your children, such as new phones, computers, keyboards, or games.

Create separate user or guest accounts. You can create guest accounts or a user account that has settings that do not allow software or apps to be installed without the administrator's login. This can prevent accidentally installing spyware or other malware if you or someone else using your computer clicks a link or opens a file.

Use anti-virus and anti-spyware protection. Install anti-virus and anti-spyware programs, make sure they are up-to-date, and set them to scan your computer regularly. These programs can help prevent spyware from being installed, and they work best before your computer has been compromised. In addition, before browsing online or clicking on links, run your anti-virus/anti-spyware software for further protection. Note that these programs will only protect you from spyware software or programs, not hardware devices such as a keystroke logging keyboard or device.

Not Spyware?

There are many other methods for someone to access information on your computer without installing spyware. If the perpetrator has physical access to the computer, they may not need to install spyware, which is mostly for remote monitoring.

Perpetrators may also be logging into accounts such as email or social media to learn about what you are doing. These accounts can be accessed from another device if the abusive person knows the username or email and password.

Sometimes, the explanation for the perpetrator knowing too much about what you're doing could be as simple as friends or family members sharing information about you. Looking for patterns of what the person knows and where that information might have come from can help you to narrow down the possibilities. An anti-violence worker can help you figure out what may be happening and plan next steps.

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 Spyware and Stalkerware: Computer Surveillance & Safety for Survivors.

A Survivor's Guide to Location Tracking

Location privacy is critical to safety. Phones and apps can share location with other people, sometimes without our knowledge. In addition, location tracking devices and built-in GPS in cars can all be misused to monitor location. Location tools can also be used to increase safety (to know where your children or pets are), for convenience (to find lost phones or keys), or to know if an abusive person is nearby.

There are times when you may want more location privacy, particularly if you're worried that someone is tracking you. This guide offers information and strategies to help you figure out if you're being tracked and, if so, decide what to do.

Step 1: Prioritize Your Safety

Get more information. Navigating violence, abuse, and stalking can be difficult and dangerous. Anti-violence workers can help you figure out options and local resources and help you create a plan for your safety. You can use www.sheltersafe.ca to find local resources.

Trust your instincts. Perpetrators are often very determined to maintain control over their victims, and technology is one of many tools they use to do this. If it seems like the person knows too much about you, they might be monitoring your devices, accessing your online accounts, tracking your location, or gathering information about you online.

Step 2: Narrow Down How Your Location Is Being Tracked

- Is there a pattern to what the other person knows? Do they know where you are in real-time or do they only know where you've been afterwards?
- Do you share your phone account with others? Does anyone else have access to your phone or know how to log on to your account?
- Are you using apps that share your location? If so, who can see that information?
- Could your friends or family be sharing your location, for example through social media?

Step 3: Learn More About How that Technology Works

Phones and Mobile Devices

- Phones track your location through GPS built into your phone, Wi-Fi connections that may reveal location, and cell phone towers that connect your phone to the network. You can turn off some location sharing, but emergency services and phone companies will be able to access your location whenever the phone is on.
- Phones connected to your Apple or Google account have features designed to help find lost phones. Anyone who has access to your account can see the location of your phone.
- Your phone, tablet, or laptop will also make a record of all the Wi-Fi networks you've connected to. You may be able to delete all or part of that history.

Apps and Social Media

- You might be sharing your location through social media and other apps. Check the location and privacy settings in each app.

- Camera and photo apps often store the location where a photo was taken, and include that information when you share a photo. You can usually turn off location in the settings of the camera and photo apps. Remember that location could also be revealed by what's in the photos, such as landmarks.

- Friends might share your location through social media by checking you into a certain location, or mentioning you by name in a post that includes a specific location. If you use that app, you may be able to set up notifications so that you know if others share your location, or you might be able to change your privacy settings to not allow others to share your location or tag your name in a post.

- Some apps request your location. Examples include shopping apps, ride-share services, or food delivery services. Someone with access to those accounts could see your location.

- Spyware (also called stalkerware) installed on your phone, tablet, or laptop can track your location. This type of app could be installed without your knowledge and may not be visible on the phone. Read more about mobile spyware.

Global Positioning System (GPS) devices

- Many cars have built-in navigational systems that could reveal a history of where you've been to anyone with access to the system.

- GPS devices can also be placed in a vehicle or personal belongings to track someone. These devices can be inexpensive, small, and easily hidden. GPS devices usually need to be connected to a power source.

- GPS tracking information can be real-time (i.e. sharing the data directly to the person who installed the GPS via a website or their phone) or it can record location history to be reviewed later.

Location Trackers

- Newer location tracking devices are small and can be hidden in a bag, backpack, or gifts.

- Unlike GPS devices, these location trackers don't have to be connected to a power source and can last for months without being recharged.

- These location devices are connected to an app or online account.

- Location trackers use some combination of GPS, active RFID (radio frequency identification), Bluetooth le (low energy), and Wi-Fi networks.

Step 4: Safety and Privacy Strategies

There are steps you can take to secure your location. There isn't one "right" way to respond. What works for some may not work or be safe for you.

Caution: making changes will often alert the other person, and they might become more abusive. They might try to track you another way or force you to share your location again. It might also erase evidence. Consider speaking with an advocate about safety planning. If you need an anti-violence worker, please go to www.sheltersafe.ca.

Documenting What's Happening

You can document what is happening if it feels safe before you make any changes. You have the option to share this with law enforcement or an attorney, or save it for later. Documenting the abuse can also help you make or update a safety plan.

- Even without knowing how your location is being tracked, you can document what's happening. What has the abusive person said that indicates they know your location? When and where have they shown up when you didn't expect them? What else do you know or suspect that makes you think you're being tracked? Be as specific as possible.

- If you know how you're being tracked, take pictures or screenshots if possible. Some technology will have traces or records of someone else's access to your location information.

- If you show someone else what's happening, make a note of who it was and when you told them.

Finding the Device or Service

- Check for hidden GPS devices or other location-tracking services in your belongings or vehicle.

- In your car, check in the trunk, under the hood, inside the bumper, and under and between the seats. You could ask a trusted mechanic or law enforcement to see if they can find the device.

- In your belongings, look for any items that don't belong to you; remember that a device can be as small as a quarter. For gifts that are non-electronic (such as a toy), look for any electronic parts that shouldn't be part of the toy.

Reporting the Abuse

- Victim service providers can help you explore options for reporting to law enforcement or discuss civil remedies.

- Consider notifying law enforcement, if it feels safe to do so. Their capacity to investigate your complaint may vary depending on resources and knowledge.

- Get help from a civil attorney or legal aid organization. You may also consider seeking a civil order of protection on your own or with the support of an advocate or attorney.

- You could also contact the company to request that the abusive person's access to your location is removed or get more information on how to gain more control over your location sharing.

Removing, Blocking, or Jamming

- If it's safe, you can remove the tracking device or turn off location sharing.

- You can decide when to keep the location tracking working and when to turn it off as part of your safety plan.

- Some counter-surveillance equipment will "jam," or stop, the communication of a location tracking device, but this may also stop other signals, such as phone communication.

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 Survivor's Guide to Location Tracking.

Mobile Spyware: Identification, Removal and Prevention

The content of this information sheet does not constitute legal advice. The information contained below is current as of February 2023 and discusses what can be done in Canada if you believe that mobile spyware has been placed on your phone or device.

If you suspect that your phone or device is being monitored, use a phone/device you believe is safe when searching for information or calling for support. This could be a computer at a public library or an anti-violence organization or a trusted family member or friend's phone or computer.

If you suspect someone is monitoring you using technology, the perpetrator may also be making you feel unsafe in other ways. If you would like to explore support options available, you can contact an anti-violence program in your area from a safe phone or device. If you are receiving support from an anti-violence worker, it may be helpful to discuss the monitoring and technology-facilitated violence with them and incorporate a response into your safety plan.

Safety Planning

Before taking action, please consider how the perpetrator may react if you stop or limit their ability to monitor you. When discussing a safety plan, you may wish to discuss with an anti-violence worker the possible repercussions of removing access to the perpetrator and build specific safety measures into your safety plan. For information about strategies for enhancing safety plans for technology-facilitated violence see WSC's Technology Safety Planning Toolkit.

I Am Concerned that Spyware Is on My Phone. Is this Possible?

For spyware to be placed on your phone, someone would need to have physical access to the phone or know your cloud ID and password.

If someone had physical access to your phone, and they knew your password, it is conceivable that spyware was placed on your phone. This information sheet will help you identify whether that is likely, and what steps can be taken to help identify and potentially remedy the spyware monitoring.

What Is Spyware and What Can It Do?

“Mobile spyware” refers to an app or program that is deliberately placed on someone's mobile device to monitor that person. Mobile spyware is a category of stalkerware. Stalkerware is defined as “all spyware that is explicitly sold or licensed to facilitate intimate partner violence, abuse, or harassment, inclusive of deleteriously intruding into the abused partner’s private life by way of physical or digital actions.”

Depending on the type of spyware installed, mobile spyware will most likely monitor:

- Call history, including phone number, date, and length of call
- Text messages, including phone number and content
- Keystrokes that have been typed
- Contacts
- Internet browsing, including history and bookmarks
- Location of the phone
- Photos taken on the phone
- Emails downloaded onto the phone

If the phone has been “jailbroken” (i.e. hardware restrictions by Apple and the wireless carrier have been on an iPhone) or “rooted” (i.e. the Android operating software code was modified and other software blocked by the manufacturer was installed), spyware software can monitor more including:

· Certain messaging apps, such as WhatsApp, Viber, and Skype

· Phone conversations

· Using the phone’s microphone to record the phone’s surroundings

It can be difficult to identify whether spyware is installed. Since most spyware products operate in “stealth” or hidden mode, the products cannot be easily detected on the phone.

Once the software is installed, the perpetrator can monitor all the above activity via an online website or an App.

If It’s Not Spyware, What Else Can It Be?

There are other ways that a person can track or monitor the activities of another person using different technology such as:

- Monitoring information on Facebook
- Logging into the iCloud or Google account associated with the phone, which accesses sensitive information including location
- Using phone functions such as Find My Phone to locate the owner of the phone. These built-in capabilities advertised as helpful tools can also provide location tracking in the context of criminal harassment (stalking), for example.

I Own an iPhone. What Are the Risks of Spyware on iPhones?

If you have an iPhone 6 or higher and have been regularly updating the iOS (operating system), the likelihood of spyware being on your phone without your knowledge is unlikely.

If you have an older iPhone model, or have not been updating your iOS regularly, the risk of spyware being on your iPhone without your knowledge is possible if: (a) someone had physical access to your device; (b) that person was aware of your device password, as well as your Apple ID login and password; and (c) your iOS is not able to be updated to the latest version.

If another person does have access to your physical device, your device password, as well as Apple ID login details, and you think spyware is on your device, please contact your local anti-violence organization to develop a safety plan.

I Own an Android. What Are the Risks of Spyware on Phones that Use the Android Operating System?

This includes phones by Samsung, Sony, Google Pixel, Huawei, LG, HTC, and Nokia.

The Android operating system is more vulnerable to spyware being placed on someone's device without their knowledge. It is also easy for a user to conceal traces of spyware on Android devices. If you think another person has access to your physical device or your device password, and you believe spyware is on your device, please contact your local anti-violence organization from a safe device for further information on spyware and safety planning.

Can I Take My Phone to the Shop Where It Was Purchased or to a Local "Tech Expert" to Check for Spyware?

Certain forms of spyware can be easily identified by an in-store, consumer retail outlet "tech expert." But there are also forms of spyware that would require a more forensic examination that is not readily available to individuals who work in computer or smartphone stores.

Depending on your situation, if the stalking/surveillance through spyware is just one part of the abuse you are experiencing, you may wish to seek support from a family violence service to put a safety plan in place**.**

I Think that Spyware Is Being Used on My Phone or Devices Right Now. What Can I Do to Protect Myself?

If you do not have the opportunity to contact an anti-violence organization, but have reason to believe that spyware is tracking you, here are some temporary, emergency steps you can take to protect yourself:

- Consider using another phone or safe device for private communications or other activities such as searching for support services. Continue to use the suspected monitored phone for "public" activities until it is safe to check the

device for spyware. This combination can be helpful if you do not want the perpetrator to know that you suspect spyware is on the phone.

- As a precaution, have private conversations on another device or in person out of earshot of the suspected device, as some spyware is able to record the sound in the area surrounding a phone/device.
- Keep in mind that spyware can monitor location, so be careful about where you go with your phone. For example, if you take the phone to the police, the perpetrator may then know that the phone is at the police station. Think through any potential risks and how to plan for safety.
- Spyware will only communicate information while the phone is turned on and is connected to the internet. Turning off the phone or turning on Airplane Mode will allow temporary relief from GPS tracking or any danger of the camera capturing pictures, audio, or video.

However, turning on Airplane Mode or turning off the phone is only a temporary measure to prevent spyware from tracking your phone. Once Airplane Mode is disconnected and the phone is turned back on, the spyware will access the activities (for example, a photo taken) and location that occurred while it was in Airplane Mode and/or disconnected. Consideration should be given as to when you can safely turn your device back on.

- If it is safe to do so, performing a factory reset on your device, ensuring the operating system is up to date, and changing your Apple ID/iCloud or Google login passwords might rid the device of spyware. This will work for many types of spyware but not all. Seeking further information from your anti-violence organization is advisable. An anti-violence organization will be able to assist you with: 1) how to preserve evidence if necessary; 2) how the perpetrator might react if you remove their ability to monitor you; and 3) developing a safety plan.
- Consider using a reputable anti-virus or anti-malware program to detect and remove spyware. Some spyware programs can be detected and removed using these programs.

- As a last resort, purchasing a brand-new phone should remove the threat of spyware. However, if purchasing a new Android device, avoid using the full backup from the old device when setting up the new one and change your Google login passwords on a safe device. If you have an iPhone, changing your iCloud password should be sufficient unless there are additional ways (desktop computer and key logger) in which the perpetrator is monitoring you.
    - Note: On Android phones, check the security settings and disable “allow installation from unknown sources” and select “verify apps” to assist in preventing spyware from being installed.

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.

Special thanks to Christopher Parsons, Citizen Lab, Munk School of Global Affairs & Public Policy; Dr. Diarmaid Harkin, Deakin University; and Dr. Adam Molnar and Ms. Erica Vowles, Deakin University.

Adapted for Canada with permission from WESNET’s Tech Safety project, based on their resource Mobile Spyware: Identification, Removal and Prevention.

This project is made possible through funding from the department of Women and Gender Equality (WAGE) Canada.