



## Cell Phone & Location Safety Strategies

Cell phones and smartphones are integrated into our lives in a way that allows us, and potentially others, access to a lot of personal information, including our activities, social circles, and even location. The following information will help you assess whether you think your activities and location are being monitored through your cell phone and offer strategies to consider that can help maximize your safety needs. If you believe someone is abusing, stalking or harassing you, we recommend that you work with a domestic or sexual violence victim advocate to ensure that you get all the information and resources you need.

### **Is there a pattern?**

Cell phones can be monitored in many ways. If you think that someone is monitoring your cell phone activity, try to narrow down what that person is doing by looking for patterns in the person's behavior.

#### *What does the person seem to know?*

Does the person seem to know everything—who you've spoken to, the content of conversations you've had either on your cell phone or near your cell phone, texts you've written and received, where you go—or just pieces of that information? Narrowing the possibilities of how your activities are being tracked will help you determine the device, program, or means by which you are being monitored, and safety strategies you may want to consider.

#### *Has the person monitoring you, or someone they know, had access to your cell phone?*

Most monitoring of cell phones requires physical access to the phone. The person might regularly scroll through the phone to see who called and texted you or may have installed monitoring software on the phone allowing them to view your activity from another phone or computer. With physical access to your phone, they could download apps or change account and security features to make your phone more vulnerable.

*Does the person have access to your wireless carrier's account?*

Another way that perpetrators can monitor your cell phone use is if they have access to your wireless carrier's account. If their name is on the account, they may have the ability to turn on features, such as family locator services, or they may be able to access your billing records online and see your call logs and other information.

### **Do they seem to know your location?**

*Are you using location-based apps on your phone?*

With many location-based social media platforms, you could inadvertently be sharing your location. Check to make sure that you don't have apps running that are pulling your location and publishing it online. Although many of these apps require you to "turn on" your location, you'll want to look into the location and privacy settings on your phone and within these apps to ensure that you are in control of that information. Additionally, there are "locate my phone" features in apps or built-in settings in some phones to locate your phone when lost or stolen. The person monitoring you may access that account or install an app with that feature without your knowledge to determine your location.

*Are your friends or family using social media and sharing your location?*

Some applications allow friends to check you into a certain location, showing exactly where you are. Other times, someone may mention you by name in an online message while also referring to being at a specific location. If you are using these social media applications you may be able to set up notifications so that you know if others share your location. Depending on the application, you might be able to change your privacy setting to not allow others to share your location information.

*Does the person monitoring you seem to know where you go, even when you don't have your cell phone?*

Although cell phones can be misused to track someone's location, many other technologies can be misused to track location as well. They can use an actual GPS device that could be in placed your car or your belonging. Or they could misuse

the navigational system in the car to see where the car is in real-time or they could download the data from the navigational system to see where the car has gone.

### **Do you notice unusual activity on your phone?**

*Excessive battery drain on your phone or a spike in data usage can be an indicator that additional software or spyware is running on your phone.*

If the perpetrator has installed spyware on your phone in order to monitor your usage, you may see a surge in battery and data usage, double text messages, and sometimes shutdown problems. If you are concerned about spyware, work with your carrier and find out what your options are.

### **Safety Strategies:**

*Trust your instincts.* If you suspect that someone is monitoring your location or conversations, they might be doing so. Narrowing down how they are monitoring your activities will help you determine your next steps.

*Pay attention to patterns and behaviors.* In many intimate partner stalking instances, the victim knows that the abusive person is monitoring his/her activity based on things the abusive person says or does. This information might help you figure out how they are monitoring your activities.

*Document what you can.* If you can, document what is happening so you can establish a pattern of monitoring and stalking behavior. This can be helpful if you want to pursue stalking or harassment charges and can help you visualize the monitoring so you can adjust your safety strategies accordingly.

*Talk to friends and family.* For many survivors who are trying to relocate or hide, it is family and friends that inadvertently share their location. If you have children, talk to them about their technology use and limit how much they share about their own location. Even innocent comments or posts about where they are going or what they are doing might tip off stalkers about their location.

### **General cell phone safety strategies:**

- Lock your cell phone with a pass code and don't share the passcode with anyone.
- Turn off the GPS on your phone and leave it on E-911 only. Be aware that some phones may limit this capability and some apps will not work with the GPS turned off.
- Some apps will allow you to opt out of it gathering location information; if an app will not give you that option, consider not downloading the app. For apps that do allow you to opt out, turn off the location feature and check regularly to ensure that your preference doesn't get changed during an update.
- If you have apps connected to online accounts on your cell phone, do not stay logged in. Log off after each use.
- Turn off the Bluetooth on your cell phone when it is not in use.
- Check your cell phone account every now and then through your wireless carrier's website to ensure that you know all the features that are running on your phone.
- Run anti-virus and security software on your phone. Some software will even list all the programs that are running on your phone.
- Avoid purchasing a "jail-broken" iPhone or "jail-breaking" your iPhone (removing the manufacturer and carrier's restrictions) since these phones are much more vulnerable to spyware and malware.

### **Strategies if you feel you are being monitored:**

- If you can, and you feel it's safe, replace your current phone.
  - Some carriers offer free or low-cost phones and service to people who qualify as low-income. You can also contact your local domestic violence program to see if they can help.
  - You can purchase a pay-as-you-go phone, one that isn't connected to any accounts that the perpetrator might have access to. Make the purchase with cash to avoid the phone being connected with your personal information.

- If you purchase a new phone with a traditional carrier, considering switching carriers and phone number. Ask that you are the only authorized account holder and check to see what type of notifications you will receive if any features get added or removed.
- Think about your safety when getting rid of the monitored cell phone. Some perpetrators may escalate their abusive behavior if they think that the survivor is removing their control and access.
- Depending on what is being used to track your location, some location applications will allow the user to set a location that could be different from where the user actually is.
- Take caution before moving data (porting contacts through the carrier or using the same memory card) or SIM cards from the cell phone that is monitored onto the new phone. The safest method is to manually enter the new data onto the new phone.
- If you cannot leave the cell phone but don't want the person monitoring you to know where you are going, you can turn off the phone and take out the battery. For additional security, you can wrap your phone in aluminum foil to ensure that no signal is being received or sent. Keep in mind, however, that once you turn the phone back on, all data waiting to be sent and to be received will occur, and if someone is monitoring your whereabouts, when you turn the phone back on, they will know.

**Safety strategies for location tracking devices:**

- Narrow down what might be used. If it is a location tracking device that is in the car, you could ask a trusted mechanic or law enforcement to go through the car to see if they can find the device.
- Be thoughtful about identifying and removing the device. Keep in mind that the person monitoring you might also know that you visited a mechanic or law enforcement and may escalate his/her abusive behavior if he/she suspects that you may be removing his/her access and control.
- Location tracking devices can also be hidden in gifts either to you or to family members. Look through anything that is new or was given as a gift.

- Location tracking devices can be passive or active; if it is passive, the person monitoring will need to extract the data from the device to see where it traveled. If it is active, then the device is sending out a signal that is communicating where it is traveling.
- Some counter-surveillance equipment will “jam” a location tracking device frequency but keep in mind that this will also jam other signals, such as cell phone signals.

© 2017, *updated 2018*, National Network to End Domestic Violence, Safety Net Project. For more information visit [TechSafety.org](https://www.techsafety.org). Supported by US DOJ-OVC Grant# 2011-VF-GX-K016. 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](https://www.techsafety.org) for the latest version of this and other materials.