# SMARTPHONE AND LOCATION SAFETY STRATEGIES

Smartphones are integrated into our lives in a way that allows us, and potentially others, to access a lot of personal information, including our activities, social circles, and even our location. The following information will help you assess whether you think your activities and location are being monitored through your smartphone and offer strategies that can help maximise your safety.

*If you believe someone is abusing, stalking or harassing you, we recommend that you work with a family and domestic violence service to ensure that you get all the information and resources you need.*

## Is there a pattern?

Smartphones can be monitored in many ways. If you think that someone is monitoring your smartphone activity, try to narrow down what that person is doing by looking for patterns in the person's behaviour.

### 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 smartphone or near your smartphone, 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 (or someone they know) who is monitoring you, had access to your smartphone?

Most monitoring of smartphones requires physical access to the phone. The person might regularly scroll through the phone to see who called and texted you or they 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 phone account?

Another way that perpetrators can monitor your smartphone use is if they have access to your smartphone 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 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 also notice double text messages, and sometimes shutdown problems. If you are concerned about spyware, work with your phone company and find out what your options are.

## 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 have access to that account or may have installed an app with that feature without your knowledge in order 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 post/update/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 smartphone?

Although smartphones can be misused to track someone's location, many other technologies can be misused to track location as well. An actual GPS device could be placed in your car or your belongings, or the navigational system in the car could be misused to see where the car is in real-time, or data from the navigational system could be downloaded to see where the car has gone.

## Safety Strategies

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

*Pay attention to patterns and behaviours.*
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 behaviour. This can be helpful if you want to pursue stalking or harassment charges or need evidence to obtain a protection order. It can also help you to visualise the monitoring so you can adjust your safety strategies accordingly.

*Talk to friends and family.*
For many women 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 smartphone safety strategies

- Lock your smartphone with a passcode and don't share the passcode with anyone.
- Turn off the location settings on your phone. Be aware that some phones may limit this capability and some apps will not work with the location is 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.
- Consider what apps you are logged into on your smartphone (for example, Facebook, Instagram or Twitter) and consider logging out after each use.
- Turn off the Bluetooth on your smartphone when it is not in use.
- 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, replace your current phone, or use a safer phone.
- If you are accessing a front line service, you may be able to get a donated phone through the Telstra *Safe Connections* program (which partners with WESNET).
- You can purchase a pay-as-you-go phone (AKA prepaid account), one that isn’t connected to any accounts that the perpetrator might have access to.
- If you purchase a new phone, ask that you are the only authorised 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 smartphone. Some perpetrators may escalate their abusive behaviour if they think that they are losing control and access (plus you might need it for evidence).
- 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 (Instagram, for example).
- Take caution before moving data (porting contacts through the carrier or using the same memory card) or SIM cards from the smartphone 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 smartphone 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. If you cannot take the battery out you can turn on flight mode and wrap your phone in aluminium 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 GPS or location-tracking devices.

- Narrow down what might be used. If it is a GPS device that is in the car, you could ask a trusted mechanic or police to go through the car to see if they can find the device.
- Be mindful when identifying or removing the device. Keep in mind that the person monitoring you might also know that you visited a mechanic or the police and may escalate his/her abusive behaviour if he/she suspects that you may be removing his/her access and control.
- GPS 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.
- GPS monitoring can be passive or active; if it is passive, the person monitoring will need to extract the data from the GPS device to see where the GPS device travelled. If it is active, then the device is sending out a signal that is communicating where the GPS device is traveling.