



## Technology facilitated violence: Mobile phones

### What is your Phone capable of?

Smart phone devices are essentially small computers, with abilities far beyond simply calling and messaging people. Many people use their phones as diaries, recording their appointments and setting reminders. GPS functions on phones can be used not only to find places but to track the phone if lost.

However, for all the conveniences and legitimate uses of these functions, phones can be used as stalking and tracking devices. This guide outlines some of the dangers and how you might protect yourself against them.

### Password/PIN/Passkey

It is important to lock your phone to help prevent unwanted access. Choosing to not lock your phone or to not set a password could enable anyone to access and make changes to your phone and its data. Some phones enable you to choose your level of security and the 'lock-out' time (how long your phone is inactive before requiring the passcode).

When choosing a password or PIN it's important to:

- Avoid the simplistic or common e.g. 1234, 0000, 5683, 2580, password
- Avoid birthdays or easily known dates
- Avoid repeating passwords/PINs for multiple devices/accounts

If you suspect your device or account has been accessed, change your password.

### Location/Tracking

Mobile phones have the ability to transmit information about location and users can be traced using this facility, additionally many apps have geo-tagging abilities that may post on your behalf. It is possible to turn this function off (change privacy setting in settings  location), alternatively you may be able to go through each app individually and choose the settings to allow it to access your location or not.

### Spyware

Certain apps can be installed upon phones, often hidden or disguised, that can allow others to access your information such as contacts, messages, phone logs and internet use. These apps are known as spyware. These apps may also transmit information such as your location or remotely turn on your phone's camera or microphone allowing others to see and/or hear your phone's surroundings. Some spyware apps are even able to send messages from your phone.

It is against the law to install and use a device to track, listen or watch a person or persons without their consent.

Detection and removal of these applications can be difficult. If you suspect there is a spyware app on your phone there are some anti-virus apps available however they are not fool proof. Setting your phone to a factory reset (after backing up your data) or changing phones entirely may be the best way to remove spyware.

### Signs someone is accessing your phone

If someone is accessing your phone either remotely or in person there are some signs that may indicate that this is happening.

- There are messages that you haven't sent on your phone
- Messages marked 'read' have not been read by you
- Your phone's battery drains unexpectedly or quickly
- Your data usage/phone bill is inexplicably high
- There are apps of unknown origin or purpose on your phone
- Contacts have been deleted or added
- Appointments or memos have been altered

### References

[http://www.staysmartonline.gov.au/home\\_users/Secure\\_your\\_mobile\\_phone\\_and\\_devices](http://www.staysmartonline.gov.au/home_users/Secure_your_mobile_phone_and_devices)

<http://nakedsecurity.sophos.com/2011/06/14/the-top-10-passcodes-you-should-never-use-on-your-iphone/>

<http://www.cnet.com.au/smartphone-spy-apps-the-facts-339301799.htm>