MOBILE APPS
Privacy Factsheet

MOBILE APPS are programmes which can be downloaded for free or for a small fee onto a mobile device like a smartphone or tablet. They are hugely popular. Games, information, maps, news, entertainment, health, fitness, shopping, banking, whatever you can imagine there is likely to be a mobile app for it. Mobile apps are a critical element of the next stage of our online engagement. As the Internet of Things (IoT) – the idea of everything, everywhere connected to the internet, becomes more popular, our ability to control technology is likely to be mobile rather than from a computer in our home or place of work.

Be app savvy

Before downloading an app read the terms and conditions. It is important to do this as many apps require access to some parts of your phone to enable them to work. For example, a calorie counting app may require access to your camera to scan barcodes, or an app that looks for nearby restaurants will require access to your location.

By downloading the app you are agreeing and accepting that the app will access all the parts of your smartphone or tablet requested in the permissions. Many apps access information, not to make the app work but to target adverts at you or sell data onto other companies. Some apps and devices try and make it clear what data an app wants to access. For example Android displays the "permissions" requested by the app before you download it.

What data can apps access?

- Phone number
- Phone ID
- Geo-location
- Phone contacts
- Calendar
- Text messages
- Camera
- Photographs
- Information on other apps on your device

Why should you care?

A study in 2014 revealed that 95% of the top 200 free apps and 80% of the paid for apps on Apple and Android collected sensitive data or shared it with others. The data which apps gather can build a sophisticated profile of you. This is done by linking your phones unique ID with all the other data which is being gathered.

Most apps do not make much money. Gathering our data and selling it onto marketing companies can be a source of revenue for an app. By knowing what other apps you use or by looking at your photo or calendar, apps can build a picture of your likes and dislikes, interests, hobbies and shopping habits. This data is hugely valuable to advertisers.

BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

What should you do to protect your privacy?

The nature of using an app exposes you to potential privacy intrusions. It is your responsibility to determine the benefit from using the app against the privacy risks.

• Only download and use apps from reputable sources.

• Read the terms and conditions and privacy policy. If you aren't sure what permissions the app is asking for don't download it. Look for an alternative.

• Update the settings on your device so you can choose which apps can collect your data:

* *

Android: Open the App Drawer → **Settings** → **Applications** → **Manage Applications** and tap any app. At the bottom of the screen you will see the Permissions area, which tells you the permissions each app uses. Uninstall any app which concerns you.

To turn off location settings, open the App Drawer, go into **Settings** → **Location** → **Google Location Settings**. Turn off 'Location Reporting' and 'Location History'.

* *

Apple iPad or iPhone: Go to **Settings** → **Privacy**. You will see a list of the apps. Click on each app to see which other apps they want access to By moving the slider at the top you can then enable/disable access.

Go to: Settings → **Privacy** → **Location Services**. You will see a list of the apps which use location services on the device. You can choose to disable them all by moving the slider at the top, or disable location services only for specific apps.

* *

Windows: Open **Start** → **Setings** → **Privacy**. Select the app (for example, Calendar) and select which app permissions are on or off. Apps with permission to "Use all system resources" are not listed. You can't use Windows Privacy Settings to control which individual capabilities these apps can use.

For apps that don't have permission to "Use all system resources" you can use Windows Privacy Settings to control individual capabilities. To see the capabilities for an app, go to the app product page in Windows Store. If you don't want an app to use any of the features listed, you can choose not to install it.

* *

Don't Forget

• Apps on your smart device can collect your location, contacts, calendar, photos and text messages.

• Read the terms and conditions and privacy policy. If the app doesn't provide detail of the permissions think twice before downloading it.

• Only download and use apps from reputable sources.

• Update the settings on your device to see which apps can collect your data.

• There is no guarantee that your data will not be gathered and shared with third parties.

BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY