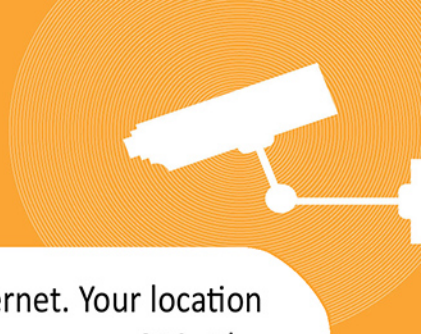
LOCATION DATA
Privacy Factsheet



LOCATION DATA is gathered on every device that connects to the internet. Your location is pinpointed using Global Positioning System technology – better known as GPS. The information from the GPS is known as geolocation data. Sometimes it is helpful to have someone know where you are, particularly if you are lost, but is your location something you always want to share? Particularly if it is with people and organisations you don't know? As technology continues to become "smart" – meaning always connected to the internet – the phone in your pocket or the technology at home and work will be pumping out information about you, including your location and what you are doing online. This will be available to technology companies, advertisers and potential malicious hackers.

How is location data gathered?

Smart phones have GPS capability, which uses satellite data to calculate your exact position. When a GPS signal is unavailable, the signal from nearby cell towers can be used to triangulate your approximate position.

This can be of use when using maps on your phone or other apps which rely on providing you with information based on your location.

Why does it matter if location data is gathered?

Whenever geolocation data is collected there are privacy concerns. By not protecting your personal information, you are sharing aspects of your private life with companies, advertisers, hackers, the police and government.

Apps and smartphone data

Apps are the technology that provide solutions for our every whim. Whether we want to find a nearby restaurant, pub, coffee shop, petrol station, toy shop, public toilet, whatever it may be, there are a multitude of apps which can give the answer. Many apps use geolocation data to provide a tailored service, for example Google Maps, FourSquare, Uber, and Yelp. Yet, there are many other apps, including games, dictionaries, health, fitness and fashion, which do not need to know your location.

Many apps hoover up our location because it provides a way to monitor how the product works. But it can also be sold onto third party advertisers who you may not be aware of. A study in 2015 by the prestigious Carnegie Mellon University looked at the App use of 23 Android Smartphone users for three weeks. It found that some of the apps were tracking location every three minutes. The apps they followed did not specifically need to collect geolocation data to provide the best service.

LOCATION DATA
Privacy Factsheet

What can you do to protect yourself?

Turning off geolocation settings means that many apps will still work, just not to the best of their ability. Geolocation does two things: a) it reports your location to other users; b) it associates real-world locations (like restaurants or bus stops) to your location.

Update the location settings on your mobile device to put you in control of who can access your location data.

Apple: Open → Settings → Privacy → Location Services. You'll see a list of the apps that 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.

Android: Open → App Drawer → Settings → Location → Google Location Settings. Turn off 'Location Reporting' and 'Location History'.

Who are those dreaded "third parties"?

It is important to recognise that taking these steps does not guarantee that your data will not be gathered and shared with third parties.

You may see the vague term "third parties" in terms and conditions and privacy policies, usually phrased as "We may share information with third parties" or in a similar way.

So who are these third parties? Unfortunately, it is all too rare for companies to explicitly say who these third parties are.

Further vague phrases which regularly feature in terms and conditions and privacy policies include "companies who help us provide and improve our Service or who use advertising or related products". Put simply, it is companies who buy the data usually for marketing purposes.

What does the law say?

The Europe Commission's Article 29 Working Party; the group of EU data regulators including the UK's Information Commissioner, released a statement saying that geolocation information is personal data. In Europe it should only be collected, shared, or stored with the individual's consent.

In practice it is less than straightforward. Because of the number of bodies involved – the wireless carrier, the operating system provider, application developer – all of which may have access to your personal information.

Don't Forget

- Every electronic device which connects with the internet has the ability to pinpoint your location using geolocation technology.
- Using geolocation means that companies, law enforcement and hackers could know where you are and where you have been.
- Turning off geolocation settings means that many apps will still work, just not to the best of their ability.
- Take control. Only give permission to apps you are happy to have access to your geolocation data.