Protecting your privacy if you use a route mapping app

May 16 2016, by Farhad Farokhi

Credit: AI-generated image (disclaimer)

There are plenty of smartphone apps that can help map your movements as you are driving, cycling, running or just out for a good walk. Many of these apps encourage you to share your route publicly on websites or with friends on social media.

Some people even go to extreme lengths to pre-plan their routes to produce maps with entertaining shapes.

What many people don't realise is that by using such apps, you could be giving away information that could be abused by others.

For example, in the UK last year, police in Hull revealed how a spate of bicycle thefts was linked to hi-tech thieves who used such app information to track expensive bikes online. Since many of the routes people recorded started and ended at home, the thieves were able to pinpoint the location and type of bicycle being used.

This is not an isolated case. There have been several other thefts prompting warnings from insurers that people should think more about their privacy when using such apps.

Privacy zones may not be that private

One approach is to mask the specifics of your "wearabouts". Strava, for example, is a fitness app that allows people to set up a privacy zone to hide the start and the end points of their trip.

Users can enter their home address (or any other place they don't want others to know they have visited) and create a radius of exclusion around that location.

The app hides the portion of a user's activity that starts or ends in their privacy zone. But this feature, like many others that rely on not sharing data in a structured manner, simply doesn't work, at least not against tech-savvy thieves.

Assume you have created a privacy zone around your house (or Brisbane GPO, as above) with a radius of 500 meters (noting that the issue will

arise with any given radius). When you leave home, the data as amended by the privacy zone feature shows your starting point as being 500 metres away from your actual home.

Each time you pass through a new point 500 metres away (assuming you don't always pass through the exact same point when leaving or returning home), you provide a new data point 500 metres from your home.

Over time these data points can be plotted on a circle, and some simple geometry can determine the radius of the circle and the centre of the privacy zone: your house.

You might be sharing more than you think

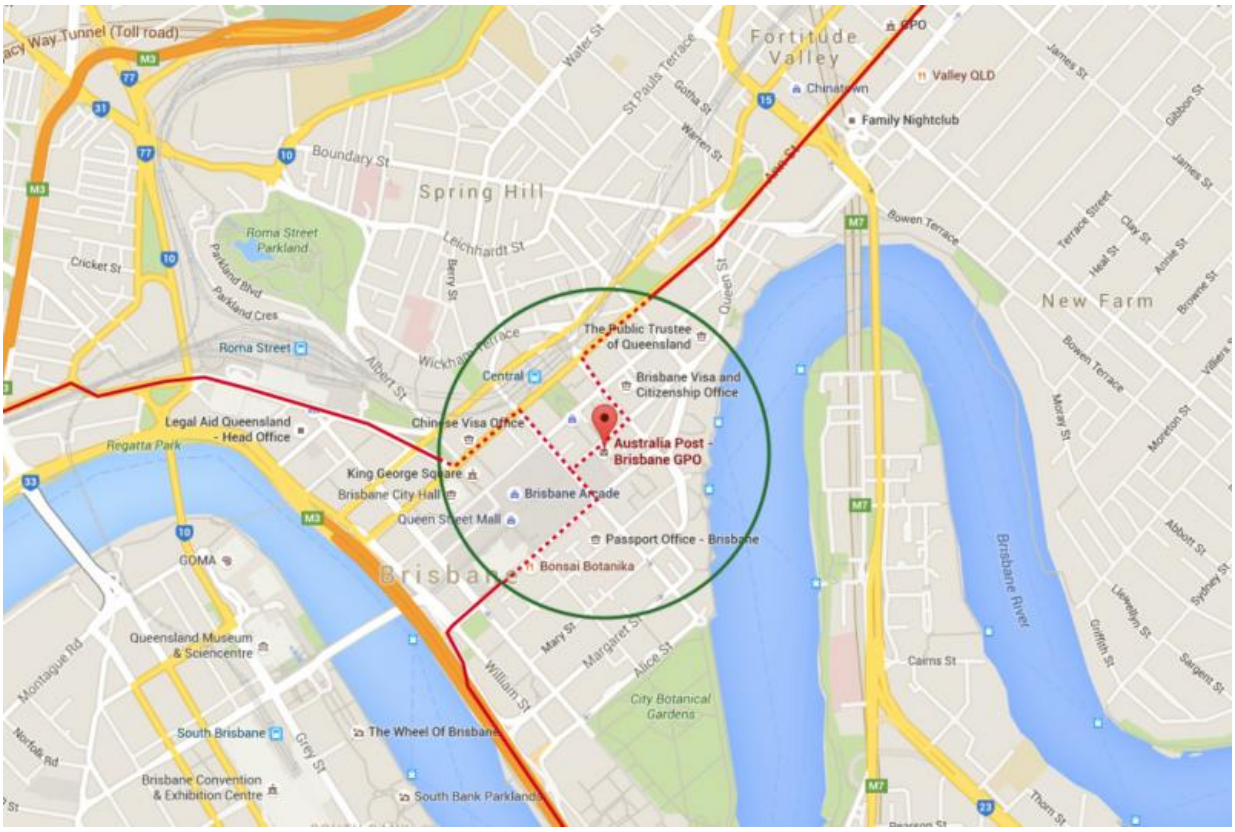
Even if you are a privacy-aware person and do not share your route data with strangers, there are chances that several apps and services are infringing on your privacy (sometimes unintentionally).

If you use sat-navs or mobile phones, then many of these devices share your movements with other apps, albeit in an anonymised way (your movements are shared without attaching your name to them), to improve traffic estimates and to identify the location of the traffic jams to reroute you through shorter paths.

In addition to these devices that share data behind our backs, we are used to sharing anonymised data. We provide anonymous feedback to our teachers or bosses. We submit anonymous feedback to app developers when they crash.

But anonymsing data most often doesn't work in preserving your privacy. It turns out that four anonymised spatio-temporal points (each spatio-temportal point is a measurement of your position at a different time of day) are enough to uniquely identify (figuring out the name of) 95% of

the individuals. These identifications mostly rely on us being creatures of habit.



A privacy zone created around Brisbane's central post office in this example (green circle). The portions of the routes that are inside the privacy zone (dashed red lines) are not shared with the public. Note how three different routes exiting the privacy zone would be enough to pinpoint the central 'home' location. Credit: Google Maps screenshot, modified

What can you do?

The good news is that sometimes there are convenient fixes for unintentional privacy leaks. For instance, if you want to use the privacy

zone idea, you should set the centre of the privacy zone at a random location in your neighbourhood, but within the radius of privacy zone around your home.

This way, the thieves cannot centre in on your home inside the privacy zone. Remember if you do this, you should not frequently change the centre point (since you provide more information to the thieves).

Another fix is something that apps such as Strava could develop in the future. It could allow the use of random shapes for the privacy zone.

The common theme between these two fixes is randomness, which takes away hidden structures that can be used to identify your private information (without your knowledge).

We need to remember that there is always a trade-off between privacy and utility. I can stop sharing everything by not using any online services and connected devices, but then I will be lost every time that I am driving to a new location.

Sometimes, it is perfectly fine to share a bit to receive great services. For instance, I personally would be happy to share my position in real-time on my way to work and back so long as no one can infer where my home is (everyone can figure out where I work by a simple Google search, so that's not an issue).

The first step in preserving our privacy is to understand how much of it we are losing, such as the extent to which privacy-preserving features actually work, and any unintended consequences of their design.

In this quest, an important thing that we need to remember is that common sense might not align with reality: privacy zone and anonymisation don't work, at least not without careful consideration.

This article was originally published on The Conversation. Read the original article.

Source: The Conversation

Citation: Protecting your privacy if you use a route mapping app (2016, May 16) retrieved 9 April 2024 from https://phys.org/news/2016-05-privacy-route-app.html