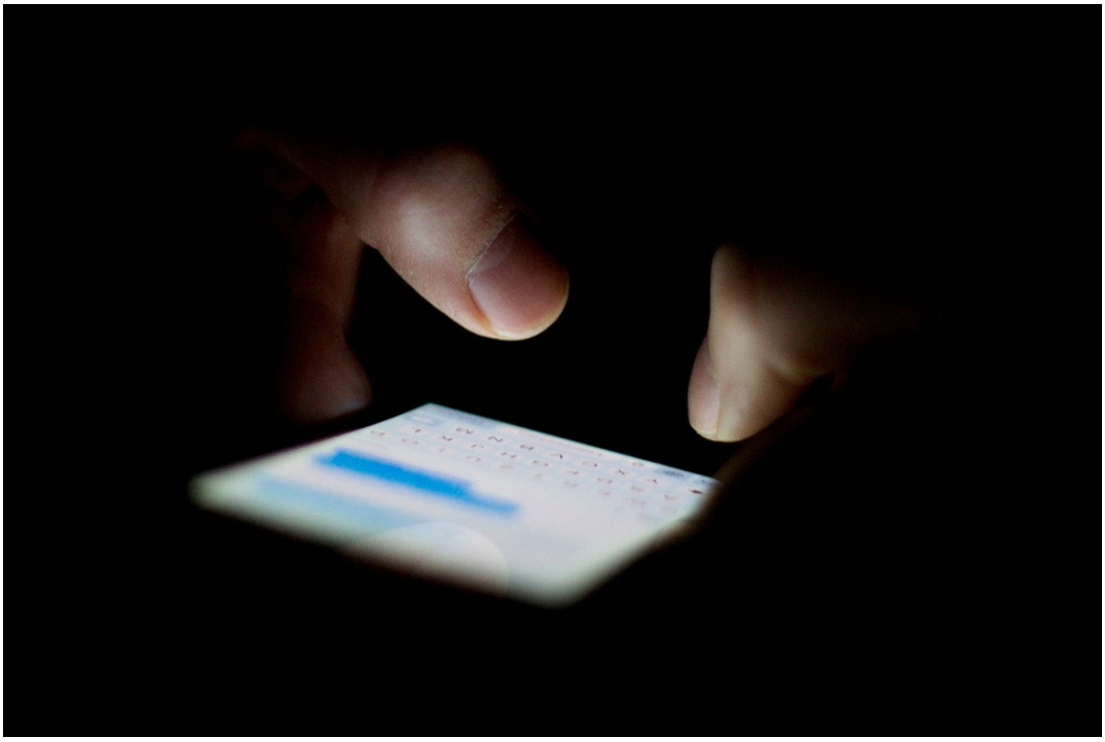
DAILY NEWS 21 June 2018

Just four tweets can reveal the identity of an anonymous troll



Just a few posts can give a troll's identity away
Janis Engel/EyeEm/Getty

By **Frank Swain**

Your scathing restaurant reviews on Trip Adviser might not be as anonymous as you think. Just four geotagged posts are enough to identify an anonymous account from a phone company's database of 10 million customers.

In order to effectively route calls to a phone, telecoms companies need to know which cell towers are nearby. In this way, they build up a crude map of each customer's movements. A team led by Apostolos Pyrgelis at University College London examined these "fingerprints" to see if there was a risk users could be identified from their movements.

They modelled how many "leaks" – tweets or Facebook posts that give away where a person was at a particular time, for example – would be necessary to match them to a unique fingerprint.

A single geolocated post from an anonymous account was enough to exclude 99.999 per cent of the database. But with 10 million records to begin with, this still leaves 100 people in the frame, so a few more posts are needed.

"In the paper we show that four location leaks are sufficient to uniquely identify 95 per cent of the users in our dataset," says Nicolas Kourtellis at Telefónica Research, part of Spain's largest telecoms company, who worked on the project.

Highly mobile users, both in terms of distance traveled and area covered, are 100 times more prone to identification, as are those who eschew popular destinations for more unique bars and restaurants.

Read more: Fed up with Facebook? Here's how to fix your online privacy

Kourtellis says this is something that can be used for good, such as anti-terrorism efforts or identifying trolls. "The police could say to a telco 'I have this set of geolocated posts, and I want you to tell me with some probability who this person is from your database'."

But there is also a risk to users if databases like this are accessed illegitimately. Hackers or authorities could use the databases to unmask anonymous critics, or learn where they live and work.

It's not only telecoms companies that build these databases. Companies like Apple and Google can infer a user's location based on nearby WiFi networks, even if the owner of the phone has not connected to them.

And your location data can be intentionally given out, for example when using exercise-mapping apps like Strava or using in-car GPS. With enough information, any of these companies could connect a user's identity to an anonymous account through coinciding location data.

"Mobile networks are effectively giant tracking systems – they have to be in order to work," says Sarah Jamie Lewis, executive director at the Open Privacy Research Society. "If you need to use a phone, that kind of trace is very difficult to scrub."

Tools like Tor will help anonymize your location if you are trying to post anonymously, says Lewis, but people and tools regularly leak identifying data. "We need to build better tools that are aware of and can identify these kinds of location leaks."

Journal Reference: arxiv.org/abs/1806.02701