Journalist wins metadata battle with defiant Telstra

After almost two years I finally get access to my information, writes *The Age's* **Ben Grubb**.

Yesterday marked 688 days since I first asked Telstra for the metadata generated by my mobile phone – the same information it routinely gives law-enforcement and intelligence agencies without a warrant when investigating crime.

Yesterday also marked the start of Privacy Awareness Week 2015, which usually goes by each year without too much fuss and is, to be frank, a little boring. Not this year.

You see, yesterday also marked the day the Office of the Australian Information Commissioner made public a landmark decision in relation to my battle with Telstra for access to my metadata.

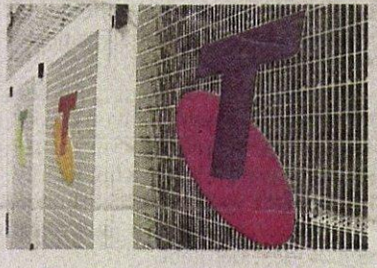
You might remember how I detailed my tussle with the telco last year, explaining how spies, councils, the RSPCA and others could gain access to my phone's metadata but I couldn't, as Telstra was refusing me access.

I wanted access to the data in light of the data retention laws, which recently passed Parliament, so I could show Australians exactly what metadata was – considering that not even George Brandis could explain it. I wanted to put my metadata on a map like German politician Malte Spitz did after he successfully sued his telco in 2011 to show just how invasive it was to have all your metadata stored, in the wake of mandatory data retention in his country.

It turns out that, by refusing me access to my metadata, Telstra breached the Privacy Act. So I won – at least in the eyes of the Privacy Commissioner.

"Telstra has breached [National Privacy Principle] 6.1 by failing to provide the complainant with access to his personal information in breach of [National Privacy Principle] 6.1 of the Privacy Act," Privacy Commissioner Timothy Pilgrim states in his 37-page decision, handed to Telstra and myself on Friday and now made public.

Mr Pilgrim goes on to state in his ruling that Telstra must, within 30 business days, provide me with access to my metadata, including Internet Protocol (IP) address information, Uniform Resource Locator (URL) information, and cell-tower location information beyond what is on my bills.



This is in addition to some of the information Telstra handed over to me while the complaint was ongoing, including outgoing call records and some cell-tower location information.

Telstra must also provide the data free of charge, Mr Pilgrim said, "because of the drawn-out and incremental approach that Telstra has taken to the provision of personal information to the complainant in relation to his access request".

As I didn't ask for damages, none will be awarded.

I won't be able to access incoming call data though (which law-enforcement agencies can), as Telstra successfully argued that this would breach the privacy of the person calling. So I won't be able to identify pesky telemarketers.

But it may be a short-lived win. Shortly after the decision was made public yesterday, Telstra said it would appeal the decision. It had 28 days to decide.

"We respect the role the Privacy Commissioner plays and we share his commitment to transparency, but we will be seeking a review of the determination," Telstra said on its blog.

So what does this all mean and will it have wider consequences for businesses? I asked former Deputy Privacy Commissioner for NSW, Anna Johnston, who is now director of Salinger Privacy.

"This is a ground-breaking decision," she says. "Telstra argued that geo-location data – the longitude and latitude of cell towers connected to the customer's phone at any given time – was not 'personal information' about a customer, because on its face the data was anonymous. They lost that argument, because the Privacy Commissioner found that a customer's identity could be linked back to the geo-location data by a process of cross-matching different datasets."

Ms Johnston said the implications of the case went well beyond the telcos and geo-location data..

"This case has far-reaching consequences for any organisation which deals in any form of 'big data'. No one should think that privacy can be protected simply by leaving out customer names or other identifiers from a database. Any data set which holds unit record-level data can potentially be linked to data from other sources, which can then lead to someone's identity being ascertainable."