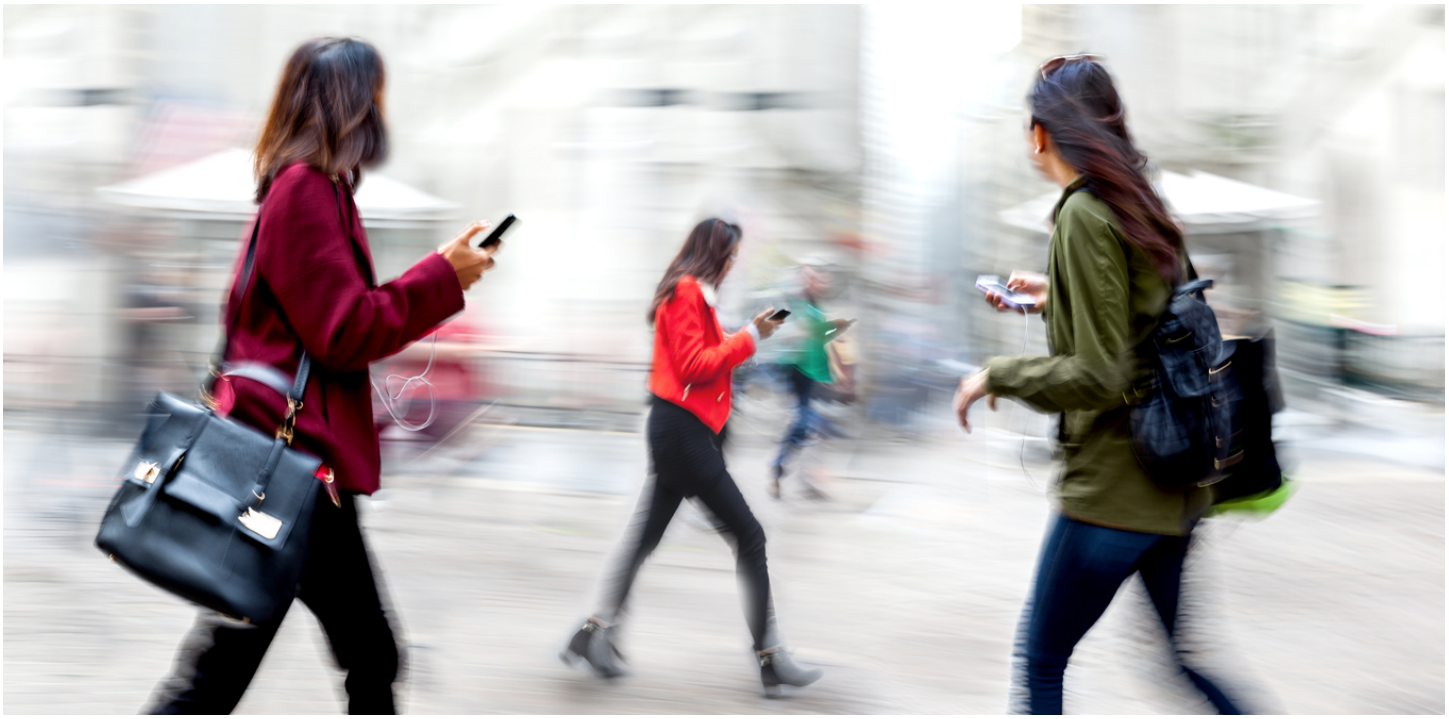
THE CONVERSATION
Academic rigour, journalistic flair



Australia’s privacy laws gutted in court ruling on what is ‘personal information’

January 19, 2017 4.17pm AEDT

Not all the data captured by Telstra on how you use its technology is considered ‘personal information’. Shutterstock/blurAZ

Author

Jake Goldenfein
Lecturer, Swinburne University of Technology

In possibly Australia’s most important privacy case to date, the Federal Court today dealt a severe blow to Australia’s information privacy laws by narrowing the definition of “personal information”.

Australia’s data privacy laws only protect “personal information”, which is defined by whether a person is identified or identifiable from data.

By reasoning that data is only “personal information” if a person is the actual subject matter of that information, the court’s decision means “personal information” may not include data that only reveals identity if linked with other data.

This means certain data held by Telstra, including IP addresses, URLs (websites) visited and geolocation data, are not protected by Australian privacy law. They are not subject to any restrictions on processing or disclosure to other entities.

By ignoring the possibilities of data linking, the court leaves us with one of the weakest data privacy regimes in the Western world. This may be appropriate for the age of print media, but it's hardly adapted for the thoroughly datafied world we live in today.

The background

If data is deemed "personal information" it is then subject to the Privacy Principles set out in the Australian data privacy acts.

One of these protections is the ability to access "personal information" held about you. This allows you to know what information is held and, for example, to correct inaccurate information.

This case began when former Fairfax journalist Ben Grubb asked Telstra to provide him with the information retained about him under Australia's mandatory data retention laws. He was investigating the significance of that regime for journalists.

Telstra acknowledged that the subscriber and billing information it held about Grubb had to be provided under privacy law.

But it refused Grubb access to his internet browsing histories (URL addresses visited), assigned IP addresses and geolocation (cell tower) data. It's argument was that this information did not reference his name or telephone number, and was thus not "personal information".

What is 'personal information'?

The definition of "personal information" (from the legislation applicable at the time) includes:

> *[…] information or an opinion (including information or an opinion forming part of a database), whether true or not, that is recorded in a material form or not, about an individual whose identity is apparent, or can be reasonably ascertained, from the information or opinion*

In Privacy Commissioner v Telstra, the question was whether anonymous mobile network data, such as geolocation data and URLs visited, might still be "personal information" because it could be linked to identified subscriber and billing information.

This question has become extremely relevant in the context of a rapidly evolving technological environment in which government and commercial entities increasingly use profiling, data linking and data matching.

Data matching, the technology that presently has Centrelink in hot water, is the process of comparing multiple systems of records to aggregate data about an already identified subject.

Data linking on the other hand, involves linking identified databases with anonymous databases to re-identify (or de-anonymise) the anonymous data by finding data fingerprints. These are often linked to

some third or associated data set.

The data fingerprint in the Privacy Commissioner v Telstra case was the IP address of the device visiting websites or creating the location data. This is because it was linked to identified information in other network assurance, subscriber and customer management databases held by Telstra.

But Telstra argued that, while it was possible to link URLs and geolocation data to an individual this way, it was extremely difficult because the data in those databases was only retained for between three to 30 days. Further, linking would require complex historical searches.

Telstra did acknowledge that law enforcement could possibly request data be linked in this way.

Data 'about' a person

While the court accepted Telstra's arguments, it did not actually base its decision on the difficulty or reasonableness of data linking the data in question. Rather, the court focused on a threshold question of whether that data was "about" a person in the first place.

The court did note that information might only become "about" a person if combined with other information. But in the judges' minds, that meant that a person had to be the actual subject matter of the information.

Because the court confined itself to this very basic question of statutory interpretation (the meaning of "about") and ignoring the broader issues, the Australian decision has produced a highly antiquated data privacy regime that ignores the working reality of contemporary information infrastructures and processing.

Failing to consider the relationship between data linkage and "personal information" puts Australia out of step with the global approach, where data linking is the focus of substantial discussion and several European privacy cases.

The European example

The latest comparable international decision, Patrick Breyer v Germany, directly explored whether the definition of "personal information" in European law included dynamic IP addresses that could only be identified when linked with data held by a third party (in this case an ISP).

The dispute in that case concerned storage by the German government of the IP addresses of devices that visited government websites.

The court found that even though a dynamic IP address is not itself personal information, it can become personal information when linked with other data.

It reasoned that the inclusion of the word "indirectly" in the European definition of "personal information" included the possibility of linking data held by one party (the German government) with datasets held by third parties (the ISP).

That is, the term “indirectly” means that the question of whether an individual is identifiable from one particular data holding does not resolve the question of whether it is personal information. Rather the focus is on how reasonably likely such data linkage was to occur.

The Australian case

Unfortunately in Australia, the court has not taken into account the international discussion on how individuals need to be protected in the telecommunications technology of contemporary society.

This case began as an exploration of the reach and significance of Australia’s metadata retention laws. These laws are presently being reviewed to consider whether access to retained data should be allowed in certain civil affairs rather than exclusively criminal matters.

But the court left standing a Tribunal decision that not all metadata retained under the data retention laws are “about” a person, and thus are not “personal information”.

This is also very different to the situation in Europe where rights of data protection and privacy have profoundly circumscribed mandatory data protection laws.

European privacy standards have now clarified that no untargeted, indiscriminate collection of data is permissible, even if it is for the purposes of protecting national security or investigating serious crime.

On the other hand, here in Australia, the court has decided that the categories of data, namely data such as an IP address, that give potentially the most intimate information away about a person (but only when linked with other data held by ISPs, communications companies, or the government) receive the least protection, or none at all.