Metadata, Privacy and the Right to Personal Information

Tim Brookes, Sophie Dawson and Jessica Norgard explain the recent landmark privacy determination - Ben Grubb and Telstra Corporation Limited – and its impact on how metadata and personal information now can be construed.

BEN GRUBB AND TELSTRA CORPORATION LIMITED [2015] AICMR 35 (1 MAY 2015)

In the lead up to Privacy Awareness Week, the Privacy Commissioner made a landmark determination which helped clarify the Commissioner's view as to what amounts to "personal information". On 1 May 2015, the Privacy Commissioner made a determination that Telstra Corporation Limited (**Telstra**) had breached the *Privacy Act 1988* (Cth) (the **Act**) by failing to provide Mr Grubb with access to some of his personal information, described as "metadata", held by Telstra. The Commissioner found that, in Telstra's hands certain metadata including IP addresses was "personal information" because Telstra could identify individuals by matching the information with information separately held by it in other databases.

Telstra has indicated it will seek review of the decision.

If upheld, the decision will have consequences for the handling of anonymised information which can be matched with other information to identify particular individuals. The decision makes it clear that such information will be treated as Personal Information by the Commissioner even if significant work is required to match information so as to identify individuals.

BACKGROUND

The Act contains a rule which enables individuals to seek access to information about them held by organisations. Until 12 March 2014, that rule was contained in National Privacy Principle 6 (**NPP 6**). From 12 March 2014, NPP 6 has been replaced by Australian Privacy Principle 12 (**APP 12**) which is in similar terms. Relevant parts of NPP 6 and APP 12 are set out below.

On 15 June 2013, Mr Ben Grubb, journalist for Fairfax, sent Telstra a request for "all the metadata information Telstra has stored" about him in relation to his mobile phone service, including cell tower logs, inbound call and text details, duration of data sessions and telephone calls, and the Uniform Resource Locators (**URLs**) of websites visited.

Mr Grubb argued that if Australian law enforcement authorities could request (and gain access to) his personal information, then he should be afforded the same right. The existence of such requests is confirmed in Telstra's Transparency Report (available on Telstra's website) which was taken into account by the Privacy Commissioner, who, in his determination disclosed that Telstra "received and acted on around 85,000 requests for customer information from law enforcement agencies as well as other regulatory bodies and emergency service organisations between 1 July 2013 and 30 June 2014".

Telstra produced a substantial amount of information prior to the Privacy Commissioner's determination. The information produced included call records in relation to all outgoing calls, SMS and MMS messages from Mr Grubb's mobile service, itemised bills to Mr Grubb, subscriber information including name, address, date of birth, mobile number, email address, billing account number, customer ID, IMSI number, PUK, SIM and password information, Mr Grubbs' IMSE, the colour of his mobile phone, his Handset ID, his mobile device payment option, his network type, and 9 to 10 months of call data records in including Mr Grubbs' number, IMEI, IMSI, cell ID, location, original called number, call date, time and duration.

The decision will have consequences for the handling of anonymised information which can be matched with other information to identify particular individuals

Telstra declined to produce certain categories of network data and incoming call records. It submitted that it was not obliged to produce them because:

- In its submission the network data was not "personal information" for the purpose of the Act; and
- Incoming call data was, in its submission, properly characterised as third party personal information disclosure of which would have an unreasonable impact on the privacy of those third parties, and which could contravene relevant *Telecommunications Act 1997* (Cth) provisions.

On 8 August 2013, Mr Grubb lodged a complaint with the Office of the Australian Information Commissioner (the OAIC) under section 36 of the Act, seeking a declaration that Telstra meet its access obligations under the Act.

KEY PRINCIPLES

Under the pre-reform Privacy Act, personal information was defined under section 6 as "information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably

be ascertained, from the information or opinion" [emphasis added].

This definition was amended as part of the reforms, and is now as follows:

> **Section 6**: ***"personal information"*** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> (a) whether the information or opinion is true or not; and
>
> (b) whether the information or opinion is recorded in a material form or not.

Section 16 of the pre-reform Act states that an organisation must not do any act that breaches a NPP.

Mr Grubb's request was made under NPP 6, which relevantly provides that: `

> **NPP 6.1**: If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that (*relevantly here*):
>
> (c) providing access would have an unreasonable impact upon the privacy of other individuals…

Relevant parts of APP 12 are in almost identical terms. They are as follows:

> **APP 12.1**: If an APP entity holds personal information about an individual, that entity must, on request by the individual, give the individual access to the information…
>
> **APP 12.3**: If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:
>
> (b) giving access would have an unreasonable impact on the privacy of other individuals.

As will be apparent from the consideration below, the Privacy Commissioner's analysis is as relevant to the revised provisions as it is to pre-reform provisions. It is therefore likely that the Privacy Commissioner would reach the same views as those explained below under the amended Act.

DOES METADATA CONSTITUTE PERSONAL INFORMATION?

The question of what constitutes "personal information" is of critical importance to privacy law in Australia, as the Privacy Act only regulates information in this category. It has been the subject of much recent discussion and debate amongst NSW privacy practitioners since the District Court's recent controversial Ritson decision: *R v Ritson; R v Stacey* [2010] NSWDC 160.

Because of the terms in which Mr Grubb's request had been put, the meaning of the term "metadata" was the subject of submissions to the Privacy Commissioner by Telstra and Mr Grubb.

In the end, the Privacy Commissioner's determination was in relation to specific categories of data which Telstra did not provide access to. His decision in relation to each will be briefly summarised in turn.

NETWORK DATA

Telstra identified three sub-types of network data which Mr Grubb had not been provided access to:

- Internet Protocol (IP) address information;
- URL information; and
- Cell tower location information beyond the cell tower location information that Telstra retains for billing purposes (as this had already been provided).

As noted above, the question of whether information is "personal information" under section 6 depends on whether a person's identity is "apparent" or "can reasonably be ascertained" from the information.

APPARENT

Mr Grubb's submissions focussed on his contention that his identity could reasonably be ascertained. He did not argue that it was "apparent" from the data. However, the Commissioner considered this aspect of the test.

The Commissioner accepted the test for "apparent" in *WL v La Trobe University (General)* [2005] VCAT 2592 (**WL**) which was made in relation to a provision in the *Victorian Information Privacy Act* (2000) in identical terms to section 6. That finding was to the effect that a person's identity is only apparent if a person can "look at the information collected and know or perceive plainly and clearly that it was information about the applicant". In WL, Coghlan DP accepted that in some cases a person can be identified by reference to information which is specific to that person other than his or her name or photograph.

The Privacy Commissioner reviewed the metadata in question and considered (in effect by way of obiter) that "the complainant's identity would not necessarily be apparent from some of the metadata he is seeking".

REASONABLY ASCERTAINED

Mr Grubb argued that law enforcement agencies must be able to reasonably ascertain his identity from the metadata to which they obtain access.

The Commissioner accepted Telstra's evidence that network data may, by cross-matching it with other data held on Telstra's various networks and records management systems, link that data to a particular individual.

The Commissioner found on this basis that Mr Grubb's identity could be ascertained. In reaching this conclusion, he had regard to the decision of DP Coghlan in WL that reasonably ascertained "must allow for some

resort to extraneous material" and that "the legislation requires an element of reasonableness about whether a person's identity can be ascertained from material and this will be determined by the circumstances in each case".

Telstra submitted that the metadata retrieval and matching process would be too burdensome in terms of complexity time and cost for the reasonableness criterion to be met. Telstra estimated that the data retrieval and analysis process would take a minimum four days full time engagement for one week's data retrieval or a minimum 12 days full time engagement for four (or more) week's data retrieval. In addition to this Telstra noted that there was a segregation between systems which contain customer records and network data, and that any need to cross-match would have an adverse impact on Telstra's business. While the Commissioner accepted that the process of extracting some of the metadata may be lengthy and require interrogation of databases by specially qualified personnel, when considered in the light of Telstra's resources and operational capacities (and the fact that it already supports this process for information requests from law enforcement bodies), the Commissioner considered that this exercise (and its scope) was reasonable in the circumstances.

Accordingly, the Commissioner determined that the metadata held by Telstra in respect of "network data" constituted Mr Grubb's personal information under the Act, was able to be reasonably ascertained and that this was reasonable under the circumstances, and should be disclosed to Mr Grubb.

INCOMING CALL RECORDS

Telstra identified that incoming call records contain inbound call numbers, location-based information, details of the communication such as time and date and the billing information and subscriber data of incoming callers. Mr Grubb said that his request was limited to the numbers of incoming callers.

As noted above, Telstra argued that this information was not required to be produced for two reasons.

First, Telstra submitted that the information was third party personal information, and not personal information of Mr Grubb.

The Commissioner rejected this argument, and found that an inbound call number, in the context of Mr Grubb's mobile phone activity, comprises shared personal information about Mr Grubb and the incoming caller. The Commissioner also held that while the identity of Mr Grubb would not readily be apparent from the phone number alone, it would be reasonably ascertainable.

Secondly, Telstra argued that it was not obliged to provide access under NPP 6 because providing access would have an unreasonable impact on the privacy of others.

NPP 6.1(a)-(k) provide exceptions to the obligation that an organisation has under the Act to provide an individual with access to their personal information.

As noted above, NPP 6.1(c) provides that an organisation may refuse an individual access to their personal information where the provision of that information would have an "unreasonable impact on the privacy of other individuals".

Referring to the authority of *Smallbone v New South Wales Bar Association* [2011] FCA 1145 [47] the Commissioner noted that whether a disclosure would have unreasonable impact "is a matter of practical judgment having regard of all the circumstances of the case".

The Commissioner considered the different circumstances of incoming calls. For example, if callers take active steps to make their phone numbers silent or blocked, then the Commissioner held that any subsequent disclosure of that information would have an unreasonable impact on the privacy of those callers. Where a caller may have dialled Mr Grubb's number unintentionally, the Commissioner stated that granting subsequent access to the phone numbers of the unintentionally callers would prejudice the privacy of those callers. The Commissioner considered that the position is less certain where a caller intentionally dials Mr Grubb but that it might reasonably be expected that these callers would consent. However, the Commissioner did not draw a firm conclusion on the latter circumstance. The Commissioner also took into consideration Telstra's Privacy Statement and its assurances of confidentiality.

This decision is particularly significant in respect of "anonymised" data, which may constitute personal information, if, when combined with other information, can identify a person.

Telstra indicated that it is possible for specialised staff to interrogate the data for no more than 30 days to identify callers with silent numbers or blocked IDs, however, it is not possible to identify records of persons that unintentionally contacted Mr Grubb.

As it is not possible to edit the records so that only intentional calls are provided, the Commissioner found that Telstra could rely on NPP 6.1(c) to refuse Mr Grubb access.

OUTCOME

The Commissioner determined that Telstra was in breach of NPP 6.1 by failing to provide Mr Grubb with access to the network data above.

The Commissioner held that Telstra must, within 30 business days, provide Mr Grubb with access to his personal information concerning "network data" including IP address

information, URL information and cell tower location information beyond the data already provided. The Commissioner stated that the information should be provided free of charge.

The Commissioner held that Telstra was not required to give access to the phone numbers of incoming callers, and was not in breach of the Act in its refusal to provide this information.

Mr Grubb did not seek an apology or compensation.

LOOKING FORWARD

This decision is particularly significant in respect of "anonymised" data, which may constitute personal information, if, when combined with other information, can identify a person.

This decision also highlighted what the Privacy Commissioner considers to be "reasonable under the circumstances".

Telstra has already indicated that it will be seeking a review of the determination.

The outcome of this review will provide further certainty in this area. This decision and the review hearing will be particularly significant for Carriers and Internet Service Providers affected by the amendments to the *Telecommunications (Interception and Access) Act 1979* (Cth), which requires the retention of metadata for a two-year period.

TIM BROOKES and SOPHIE DAWSON are partners at Ashurst. JESSICA NORGARD is a lawyer at Ashurst.