Australian Government Solicitor

Express law
fast track information for clients

AGS

25 May 2015

Metadata is 'personal information' under the *Privacy Act 1988* (Cth)

In *Ben Grubb and Telstra Corporation Limited* [2015] AICmr 35 (1 May 2015), the Privacy Commissioner determined that the complainant's metadata held by Telstra constituted 'personal information'. In failing to provide the applicant with access to his network data information, Telstra breached the *Privacy Act 1988* (Cth).

Although this determination was made under the National Privacy Principles, the discussion about metadata as personal information is relevant to entities covered by the Australian Privacy Principles.

Is metadata personal information?

The complainant claimed a right of access under the *Privacy Act 1988* (Cth) to 'all the metadata information' that Telstra had stored concerning his mobile phone service.

The complainant argued that he should be entitled to the same information that is made available to law enforcement agencies. The complainant was given access to information about his outbound call details and the length of data usage sessions. However, the complainant was refused access to Internet Protocol (IP) address information, Uniform Resource Locator (URL) information, cell tower location information and incoming call records. The complaint alleged that Telstra had interfered with his privacy by refusing access to all of the requested information.

While the complaint was being determined, Telstra modified its access policy to allow its customers to 'access the same metadata about them (save for shared information) that Telstra would provide to law enforcement agencies, on request without a warrant'.

Telstra continued to refuse access to network data and incoming call records on the basis that the data was not 'personal information' as defined by the Privacy Act.

The case turned on whether the complainant's metadata constituted 'personal information' for the purpose of the Act. Under the definition of 'personal information' at the relevant time, the identity of an individual must be 'apparent' or 'can reasonably be ascertained'.

Identity of complainant can 'reasonably be ascertained'

The complainant did not contend that his identity is apparent on the face of the metadata he sought. He claimed that his identity must reasonably be able to be ascertained from that metadata if law enforcement and national security bodies can seek and obtain metadata connected with an individual's phone service.

The Commissioner heard evidence from Telstra that it is possible to extract the data that is held on various network elements and management systems spread access Telstra's mobile

network and ascertain a customer's identity by cross-referencing the metadata with other data held in Telstra's customer management and subscriber record systems. This type of date is extracted and provided to law enforcement agencies on request and is used for network assurance purposes.

The Commissioner found that the fact that data extraction and matching is a process already in practice is indicative of Telstra's ability to ascertain an individual's identity.

The Commissioner accepted that extracting some of the metadata that the complainant requested may require interrogation of several of Telstra's information systems by specifically qualified personnel. However, taking into account Telstra's resources and operational capacities, the Commissioner found that the process was not beyond what is reasonable relative to the resources at its disposal and its existing operational capacities. In coming to this conclusion, the Commissioner noted that Telstra responds to tens of thousands of similar requests from law enforcement bodies every year.

Accordingly, the Commissioner found that the network data constitutes 'personal information' under the Act. The Commissioner also found that inbound call numbers were personal information about the complainant.

No requirement to give access to information about third parties

It was practically not possible for Telstra to edit incoming call numbers only to include those individuals who intentionally contacted the complainant and exclude those with a silent line or line blocking or who had unintentionally contacted the complainant. Consequently, the Commissioner decided that access to inbound call numbers could be refused on the basis that access would have an unreasonable impact on the privacy of other individuals.

Implications for clients

Although this determination was made under the former National Privacy Principles, it is relevant to all entities covered by the current Australian Privacy Principles. The discussion about metadata as personal information, and whether an individual's identity can reasonably be ascertained, equally applies to the current definition of 'personal information' in the Act. The current Act also includes a similar exception to refuse access on the basis that it would have an unreasonable impact on the privacy of other individuals.

The decision highlights the potential application of the Privacy Act to metadata held by an entity. The extent to which an entity is required to give access will depend on the type of metadata stored, whether the entity has the capacity and resources to ascertain the identity of an individual and whether the process is 'reasonable' in the facts and circumstances of the particular matter.

The determination also has implications for applications for access made under the *Freedom of Information Act 1982* (Cth), because that Act adopts the Privacy Act's definition of 'personal information'.

Telstra has lodged an application in the AAT seeking review of the decision.

For further information on the issues above please contact:

Elena Arduca
Senior Executive Lawyer
T 03 9242 1473
elena.arduca@ags.gov.au

Jane Lye
Senior Executive Lawyer
T 07 3360 5736
jane.lye@ags.gov.au

Justin Davidson
Senior Executive Lawyer
T 02 6253 7240
justin.davidson@ags.gov.au

Tara McNeilly
Senior General Counsel
T 02 6253 7374
tara.mcneilly@ags.gov.au
