Ben Grubb and Telstra Corporation Limited [2015] AICmr 35 (1 May 2015)

Determination and reasons for determination of Privacy Commissioner, Timothy Pilgrim

Complainant:	**Ben Grubb**
Respondent:	**Telstra Corporation Limited**
Determination date:	**1 May 2015**
Application number:	**CP13/01119**
Catchwords:	**Privacy — Privacy Act — National Privacy Principles — (CTH) *Privacy Act 1988* — s 52 — NPP6.1 — Access**

Contents

Summary

1. Telstra Corporation Limited (Telstra) interfered with the complainant's privacy by failing to provide the complainant with access to his personal information held by Telstra in breach of National Privacy Principle (NPP) 6.1 of the *Privacy Act 1988* (Cth) (the Privacy Act).
2. To redress this matter, Telstra shall:
   - within 30 business days after the making of this declaration, provide the complainant with access to his personal information held by Telstra in accordance with his request dated 15 June 2013, save that Telstra is not obliged to provide access to inbound call numbers;
   - provide the complainant with access to the above information free of charge.

Background

3. On 15 June 2013 the complainant claimed a right of access under the Privacy Act to 'all the metadata information Telstra has stored' about him in relation to his mobile phone service, including (but not limited to) cell tower logs, inbound call and text details, duration of data sessions and telephone calls and the URLs of websites visited.
4. His request was expressed as follows:

> ...I'd like to request all of the metadata information Telstra has stored about my mobile phone service (XXX XXX XXX).
>
> The metadata would likely include which cell tower I'm connected to at any given time, the mobile phone number of a text I have received and the time it was received, who is calling and who I've called and so on. I assume estimated longitude and latitude positions would be stored too. This is the type of data I would like to receive.
>
> Handing over RAW data would probably be easiest but if it's in a CSV format that'd be great.
>
> If there is a cost associated with getting the data please advise what it may be...

5. On 16 July 2013 Telstra notified the complainant that he could access outbound mobile call details and the length of his data usage sessions via online billing. Telstra advised the complainant that due to privacy laws it was unable to provide the complainant with information regarding location and details of the numbers that called and sent SMS to his mobile phone service. Telstra advised that the complainant would need a subpoena for any of the other information he had requested.

Privacy complaint and remedy sought

6. On 8 August 2013, the complainant lodged a complaint with the Office of the Australian Information Commissioner (OAIC) against Telstra under s 36 of the Privacy Act.
7. The complainant claimed that Telstra had breached his privacy by refusing him access to the personal information it holds about him.
8. The complainant seeks a declaration by me that Telstra meet its access obligation under the Privacy Act and provide the complainant with access to all the information he has requested.
9. The complainant has not sought an apology or compensation.
10. Telstra has not accepted that it has breached the complainant's privacy.
11. Notwithstanding this, I acknowledge that Telstra's approach to customer access to metadata has shifted significantly since this complaint was lodged. It is particularly pleasing to note Telstra's recent online announcement to its customers regarding its policy on customer access to metadata, which states that Telstra customers will now be able to access the same metadata about them (save for shared information) that Telstra would provide to law enforcement agencies, on request without a warrant.[1]
12. What this has meant for the complainant is that some information initially withheld has subsequently been provided to him over an 18 month period. Nonetheless, the complainant has still not been provided with all of the personal information that falls within his request and to which I have decided he is entitled. The reasons for my decision are as follows.

The law

13. I note from the outset that because this matter relates to events that occurred prior to reforms to the Privacy Act which commenced on 12 March 2014, the complaint has been dealt with under the legislative regime as it applied when the events occurred. The National Privacy Principles (NPPs) not the Australian Privacy

[1] Kate Hughes, 'A principle of privacy' on *Telstra News* (6 March 2015) <http://exchange.telstra.com.au/2015/03/06/a-principle-of-privacy>.

Principles[2] therefore apply in this instance to the question of whether or not Telstra has breached the Act. The NPPs outline the standards for handling personal information that legally bind organisations.

14. The question in this complaint is whether the complainant's metadata held by Telstra constitutes personal information, and if so, whether it has been improperly withheld from the complainant in breach of NPP 6.1.

15. The definition of 'personal information' is at s 6 of the Privacy Act, and under the pre-reform privacy regime is defined 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.[3]

16. Section 16A(2) of the Privacy Act provides that:

> To the extent (if any) that an organisation is not bound by an approved privacy code, the organisation must not do an act, or engage in a practice, that breaches a National Privacy Principle.

17. The parties do not dispute that Telstra is an organisation within the meaning of s 6C(1)[4] of the Privacy Act and is bound by the NPPs.

18. NPP 6.1 provides that:

> 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*[5]:
>
> …
>
> (c) providing access would have an unreasonable impact upon the privacy of other individuals; or
>
> …
>
> (g) providing access would be unlawful
>
> (h) denying access is required or authorised by or under law …

---

[2] From 12 March 2014, the Australian Privacy Principles replaced the National Privacy Principles (NPPs) and the Information Privacy Principles (IPPs). These new APPs apply to both Australian Government agencies and private-sector organisations covered by the Privacy Act.

[3] 'Personal information' under the post-12 March 2014 regime is defined to mean:
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.

[4] *Privacy Act 1988* (Cth) s 6C.

[5] Italics added.

19. It is common ground that if Telstra holds personal information about an individual, it must, as an organisation to which NPP 6.1 applies, provide the individual with access to the information on request by the individual unless the information is the subject of an exception under NPP 6.1 (a)-(k).

20. Section 52 of the Privacy Act provides that, after investigating a complaint, I may make a determination:

- dismissing the complaint (s 52(1(a)); or
- finding the complaint substantiated and declaring:
  - that the respondent has engaged in conduct constituting an interference with the privacy of an individual and should not repeat or continue such conduct (s 52(1)(b)(A)); and/or
  - the respondent should perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant (s 52(1)(b)(ii)); and/or
  - the complainant is entitled to compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint (s 52(1)(b)(iii)); and/or
  - it would be inappropriate for any further action to be taken in the matter (s 52(1)(b)(iv)).

Scope of access request

21. The complainant has requested 'all the metadata information Telstra has stored' about his mobile phone service.

22. The term metadata has been used interchangeably with 'communications data'[6] and 'telecommunications data'.[7]

23. During a hearing into this matter on 2 October 2014 (Determination Hearing) Telstra stated that it had relied on a number of documents in its consideration of the meaning and scope of the complainant's request including the Background Note, *Telecommunications data retention – an overview* (the Background Note).[8] The Background Note was also referred to in Telstra's final submission to the OAIC dated 18 November 2014.

24. The Background Note refers to 'communications data', which it states:

[6] Nigel Brew, *Telecommunications data retention – an overview,* Background note, Parliamentary Library, Canberra, 24 October 2012.
[7] Commonwealth, *Parliamentary Debates,* House of Representatives, 30 October 2014, 44 (Malcolm Turnbull).
[8] Nigel Brew, *Telecommunications data retention – an overview,* Background note, Parliamentary Library, Canberra, 24 October 2012.

> …is information about an electronic communication – a footprint left after accessing the internet, sending an email, or making a phone call. It might, for example, include customer registration details, the date, time and duration of a communication, the phone number or email address of the sender and recipient, the amount of data up/downloaded, or the location of a mobile device from which a communication was made.
>
> …. The Attorney-General's Department Discussion Paper notes that communications data:
>
> …is not defined in the TIA [*Telecommunications (Interception and Access) Act 1979* (Cth)] but is generally understood to refer to information about a communication that is not the content or substance of a communication. Data is increasingly understood as falling into two categories: subscriber data, which provides information about a party to a communication such as name or billing address; and traffic data, which relates to how a communication passes across a network, such as the location from which the communication was made.

25. The Background Note also makes note of 'telecommunications' data:

> According to the *Telecommunications (Interception and Access) Act 1979 report for the year ending 30 June 2011*:
>
> > While telecommunications data is not defined in the TIA Act, it is taken to mean anything that is not the content or substance of a communication. It can include:
> >
> > - subscriber information
> > - telephone numbers of the parties involved in the communication
> > - the date and time of a communication
> > - the duration of a communication
> > - Internet Protocol (IP) addresses and Uniform Resource Locators (URLs) to the extent that they do not identify the content of a communication, and
> > - location-based information.[9]

26. In his submission to the OAIC dated 21 July 2014, the complainant provided his understanding of metadata information:

> My interpretation of metadata is that it is data that isn't the contents of a communication.
>
> If it's a text message (SMS) that's the time, date and location the text was sent or received; if it's a call it's the time, date and location the call was sent or received; if it's internet access, it's the time, date and location the URL or IP address was

[9] Nigel Brew, *Telecommunications data retention – an overview,* Background note, Parliamentary Library, Canberra, 24 October 2012, 1-2 (citations omitted).

accessed, or the port used; if it's an email it's the time, date, location and subject line.[10]

27. Since the time of the Determination Hearing Telstra has provided the complainant with the following information[11] falling within the scope of his request:

- call data records in relation to all outgoing calls, short message service (SMS) messages and multimedia messaging service (MMS) messages from the complainant's mobile telephone service since 2011 . Outgoing call records include the following information:
    - the originating number (A-party number, i.e. the complainant's mobile number)
    - A-party location information including the cell tower involved in the communication (may not be the one physically closest to the caller)
    - the numbers the complainant called from his mobile phone (B-party numbers)
    - the date, time and duration of the communication (in relation to SMS or MMS messages, duration of the communication is not recorded)
- itemised bills issued to the complainant, including the numbers he called from his mobile service, the time and duration of those calls
- subscriber information including name, address, date of birth, mobile number, email address, billing account number, customer ID, IMSI (International Mobile Subscriber Identity) number, PUK (Personal Unlock Key) number, SIM (Subscriber Identity Module) category and requested password for account
- the complainant's International Mobile Station Equipment Identity (IMEI)[12]
- the colour of his mobile device
- his Handset ID
- his Mobile Device Payment Option (that is, the payment method for the mobile device) and
- his Network type (the mobile network utilised by his mobile phone service).

[10] Complainant's submission to the OAIC, 21 July 2014, 1.
[11] Information falling within the scope of his request was provided to the complainant at the Determination Hearing (2 October 2014), on 18 November 2014, on 29 January 2014 and on 5 February 2015.
[12] The IMEI is an identifier allocated to a mobile device.

28. The complainant was also provided with approximately 9-10 months of call and data records (19 February 2014 to 3 December 2014), which includes:

    - A-party (the complainant's) number, IMEI, IMSI, cell ID, location, original called number, call date, time and duration.

29. There is now no dispute in respect of access to the above listed information.

30. Telstra has categorised the remaining data which has not been provided to the complainant into two broad information sets:

    - network data[13]
    - incoming call records.

Network data

31. Telstra's General Manager, Network Infrastructure Operations (the NIO General Manager) delivered an oral submission before me on 2 October 2014 explaining what Telstra means by network data:

    - a reference to network data is a reference to the connectivity or signalling information that allows a communication to occur, which is distinct from the information contained in Telstra's billing systems.[14] This signalling data does not include the content or substance of a communication
    - signalling data, which Telstra collects and uses for network assurance purposes (that is, to investigate why something isn't working), is captured by Telstra's 13 different network management systems.

32. Telstra has identified three sub-types of network data which the complainant has not been provided access to:

    - Internet Protocol (IP) address information
    - Uniform Resource Locator (URL) information
    - Cell tower location information beyond the cell tower location information that Telstra retains for billing purposes (to which the complainant has been given access).[15]

[13] Determination Hearing, 2 October 2014. See also Telstra's closing submission to the OAIC, 19 November 2014, 10.

[14] Determination Hearing, 2 October 2014. Telstra's General Manager explained that, 'Telstra has dedicated systems which store details in order to charge customers what they charge and confirm the record is correct. These details are passed through an interface into Telstra's billing systems which capture this data'.

[15] E.g., Telstra's closing submission to the OAIC, 19 November 2014, 12.

Incoming call records

33. Incoming call records hold the same type of information as outgoing call records and include:

- inbound call numbers and location information including the cell tower involved in the communication (which may not be the one closest to the caller)
- details such as the date, time and duration of the communication. If SMS or MMS messaging, duration is not provided
- billing information of incoming callers
- subscriber data in relation to the incoming callers.

Contentions

34. Telstra contends that it is not in breach of its access obligation under NPP 6.1 because:
    - the metadata in dispute, which sits on its network management systems, is not personal information as defined under the Privacy Act as the complainant's identity is not apparent nor can it reasonably be ascertained from that data
    - incoming call records are not the personal information of the complainant but rather constitute the personal information of third parties and if disclosed would:
        - have an unreasonable impact on the privacy of other individuals, i.e., those incoming callers, and/or
        - potentially place Telstra in breach of the provisions of the *Telecommunications Act 1997 (Cth)* (the Telecommunications Act), which regulates the use and disclosure of telecommunications data.
35. The complainant's position is that the metadata stored about him:
    - is his personal information
    - in relation to inbound call numbers, would not have an unreasonable impact on the privacy of other individuals in cases where the calling number display has not been blocked or the option of a silent line not taken.
36. The complainant has made it clear that he is not seeking access to third party data such as subscriber data or billing information.[16] His complaint in relation to incoming call records centres around Telstra's refusal to provide him with access to inbound call numbers.

[16] Ben Grubb, Determination Hearing, 2 October 2014.

Other information - content

37. In his submission to the OAIC the complainant requested that I make a decision regarding his access to the content or substance of his communications to and from his mobile phone service:

> I also make the point that I should be able to access other information Telstra stores on me, such as any case notes and the contents of my mobile phone's text messages (if they are stored).[17]

38. The content or substance of a communication lies outside of the scope of metadata information and consequently outside the complainant's original access request.[18] Telstra has not had an opportunity to deal with the issue of access in relation to it, and I am not required to consider it.

39. Nonetheless I am of the view that if the content of a mobile phone communication or any other record that Telstra holds in relation to the complainant meets the definition of personal information under the Privacy Act, then Telstra is obliged to provide access to that information on request except to the extent that one of the exceptions under the Privacy Act apply. At paragraphs [122] to [155] I discuss some of the exceptions to an organisation's access obligations, chiefly NPP 6.1(c) which is particularly relevant to this matter.

Investigation process

40. The OAIC's investigation of this complaint involved the following:

Date	Action
23 December 2013	An investigation was opened under s 40(1) of the Privacy Act
24 January 2014	Telstra responded to the OAIC's investigation notice contending that it had met its obligations under the Privacy Act and was amenable to providing the complainant with his customer account record. It argued that the information the complainant requested and which it refused to give access to was not personal information for the purposes of the Privacy Act
7 February 2014	The OAIC requested further information from Telstra
14 February 2014	A second response from Telstra was received by the OAIC, with Telstra maintaining that the information requested by the complainant was not personal information and was therefore not subject to the access obligation under the Privacy Act

[17] Complainant's submission to the OAIC, 21 July 2014, 1.
[18] See excerpts from the Background Note at paragraphs [24]-[25] of this determination, which provide various descriptions of what is generally understood by 'metadata'.

Date	Action
12 March 2014	The complainant submitted that if law enforcement authorities could access the information about him, the complainant should also be able to gain access to that information
20 March 2014	A conciliation meeting occurred with no resolution being reached and the decision was made to determine the matter under s 52 of the Privacy Act
25 June 2014	Notice of the s 52 determination was provided to both the complainant and Telstra
21 July 2014	The complainant provided a written submission in support of his request for access to the disputed information, which was received and provided to Telstra with the complainant's consent, for its consideration and response
25 July 2014	Telstra responded to notice of the determination with a written submission which was provided in redacted form to the complainant for his consideration
15 August 2014	A further submission was received from Telstra in response to the complainant's 21 July 2014 submission
2 October 2014	A hearing was held affording the parties the opportunity to appear before me, with both parties accepting the invitation to appear. An audio record of the hearing was made available to both parties
7 November 2014	A Notice to Attend was issued under s 44 of the Privacy Act requiring a Telstra representative to attend before me and give further information
18 November 2014	A Telstra representative attended before me and provided further information. A summary of notes taken during the attendance was made available to both parties (to the complainant on 29 January 2015)
19 November 2014	Telstra provided a closing submission summarising its position, with a copy also provided to the complainant
27 November 2014	A Notice to Produce was issued under s 44 of the Privacy Act requiring Telstra to produce all of the complainant's metadata information associated with his mobile phone service which would be provided to law enforcement agencies on request
11 December 2014	Further to the Notice to Produce, Telstra arranged to have a sample of files (on a USB device) delivered to the OAIC in response to the Notice to Produce.

Date	Action
19 December 2014	Some further questions were identified, the answers to which would assist in finalising the decision in this matter, and further information was requested from Telstra
19 January 2015	Further to the request for more information, Telstra provided responses to the 19 December 2014 queries
5 February 2015	A redacted copy of the information produced in response to the 27 November 2014 Notice to Produce was provided to the complainant.

Personal Information

41. The general rule under NPP 6.1 is that if an organisation (such as Telstra) holds personal information about an individual (such as the complainant), access must be provided to the individual upon that individual's request.

42. As defined in s 6 of the Privacy Act and in the context of this matter, personal information must be information that is:

    - about the complainant, and
    - information from which the complainant's identity is apparent, or can reasonably be ascertained.

43. I will begin my consideration of whether the metadata that Telstra has refused the complainant access to constitutes his personal information by reference to the subject headings of 'network data' and 'incoming call records', in keeping with Telstra's earlier classification of that metadata into these broad information sets.

Findings in relation to network data

44. In its submissions to the OAIC, Telstra contends that metadata generated from the complainant's phone activity on Telstra's mobile network (that is, network data), is not personal information about the complainant. It contends that a customer's identity is not apparent from Telstra's network data nor can it reasonably be ascertained from that metadata.

45. Telstra argues that none of the network data is linked in such a way as to identify an individual customer. Telstra explains that:

> …it would be very difficult and require a great deal of forensic effort for Telstra to identify and gather the network data that relates to [the complainant]. There is no likely scenario in which Telstra would do this in the ordinary course of its business,

> and so the network data should not be treated as personal information about [the complainant].[19]

46. Telstra goes on to say that because network data is spread across Telstra's various network management systems and each system has a different function and stores information in different ways[20], retrieving this type of data would be impractical, tie up its resources and would have an adverse impact on Telstra's business:

> There is a 'segregation between the systems which contain our customer records and our network data (…the data relating to the traffic network is several steps removed from being able to identify an individual customer)'…[21]
>
> …There is no ordinary business process at Telstra that would involve the identification and retrieval of this type of information for any particular individual. Network data generated through the use of [the Telstra] mobile telephone network is not kept in a single repository. The network data is spread out across many different network elements and systems where it is mixed with information generated from the use of those networks by other users…[22]
>
> Identifying and retrieving any network data relating specifically to the complainant would be difficult, time consuming and costly. Only a very limited number of [Telstra] personnel who are technical experts on network design and configuration, and have access rights to the multiple systems, would have the knowledge and expertise required to access all the relevant systems and retrieve this information.[23]

47. The complainant submits that the information he has requested from Telstra in relation to his mobile phone service is his personal information to which he is entitled access. He contends that:

> If an Australian law enforcement authority (RSPCA, ATO, local council, etc.) can request access to certain aspects of my metadata that is personal to me then I too should also be able to access that information. This information is able to be mined out of Telstra's systems and given to agencies and is identifiable. I should be able to access that data because it is mine.[24]

Information about the complainant

48. For the network data requested by the complainant to be the complainant's personal information as defined in the Privacy Act, the data must be 'about the individual' (that is, in some way concerning or connected with the individual)

---

[19] Letter from Telstra to the OAIC, 15 August 2014, 1.

[20] Determination Hearing, 2 October 2014. Telstra's NIO General Manager explained that, 'connectivity data is captured across the 13 systems, allowing Telstra to collect and use this information for network assurance purposes, though one central repository system provides most of the signalling capture'.

[21] Letter from Telstra to the OAIC, 15 August, 1.

[22] Letter from Telstra to the OAIC, 25 July 2104, 2.

[23] Letter from Telstra to the OAIC, 25 July 2014, 3.

[24] Complainant's submission to the OAIC, 21 July 2014, 1.

whose identity is apparent or can reasonably be ascertained from the information.

49. I have heard from Telstra's NIO General Manager who stated that metadata created on the various components or 'elements' of the Telstra communications network, including individual customer transactions, are captured on one or more of 13 network management systems, with one management system capturing much of the signalling. A network-based identifier, such as an IMSI or temporary IMSI, is assigned to each of these transactions, which allows a customer to be identified, primarily for the purpose of dealing with issues relating to service connectivity or performance.[25]

50. Telstra's NIO General Manager stated that in order to identify a customer associated with an IMSI, a Telstra employee with appropriate access and training would need to access subscriber information from a subscriber database to look up the phone number of the SIM card to which the IMSI was allocated. That person would then need to access a separate customer relationship management system to look up the name of the customer using the telephone number. There would consequently be at least three databases involved in obtaining this information.[26]

51. Telstra's NIO General Manager also provided information about the way in which a customer's identity could be ascertained from network data using a network identifier other than an IMSI.[27] Telstra's counsel summarised this in Telstra's closing submission:

> …The only way in which this identification could occur would be for someone recursively to review historical network data around a particular time in relation to a particular network element. …. If the network data recording the allocation of the protocol [identifier] was identified, it would then be possible to ascertain the IMSI relevant to that particular network data…[28]

52. I accept that network data like an IMSI (or other network identifier) may, by cross matching it with other data held on Telstra's various network and records management systems, link that data to a particular individual.

53. I am therefore satisfied that network data in the context of customer transactions captured on Telstra's network management systems is 'information … about an individual'.

---

[25] Telstra General Manager, Network Infrastructure Operations, Determination Hearing, 2 October 2014.

[26] Telstra General Manager, Network Infrastructure Operations, Determination Hearing, 2 October 2014.

[27] Telstra General Manager, Network Infrastructure Operations, Determination Hearing, 2 October 2014.

[28] Telstra's closing submission to the OAIC, 19 November 2014, 13 [38].

54. Whether or not that information satisfies the definition of personal information under the Privacy Act will also depend on whether or not the identity of the individual:

- is apparent, or
- could reasonably be ascertained from the information.

55. I will consider each of these issues in turn.

Is the identity of the complainant apparent?

56. In reaching its conclusion that the network data sought by the complainant is not personal information within the meaning of the Privacy Act, Telstra has relied in part on the decision in *WL v La Trobe University (General).*[29].

57. In that case Coghlan DP considered the term 'personal information' within the meaning of s 3 of the *Information Privacy Act 2000* (Vic)[30], which is in identical terms to the definition provided in s 6 of the Privacy Act. The Deputy President observed that in order for the complainant's identity to be 'apparent':

> 17 … one would need to be able to look at the information collected and know or perceive plainly and clearly that it was information about the applicant. Thus for example, one's identity would be "apparent" if the information mentioned one's name or was a photograph of a person.
>
> 18 One could also conceive of situations where information which did not include one's name or photograph would, because of the singular nature of the information, mean that it could be no one else but a particular person, and in that way reveal one's identity. In that case the identity would be capable of being clearly perceived by looking just at the information…[31]

58. The definition of the word "apparent" in *The Macquarie Dictionary Online* (2013) means '"capable of being clearly perceived or understood; plain or clear".[32]

59. In response to my issuing of a notice to produce information under s 44 of the Privacy Act, Telstra provided me with a sample of the same metadata associated with the complainant's mobile phone service that would be provided to law enforcement agencies on request. This sample was constituted by the following information:

- the complainant's subscriber details

---

[29] [2005] VCAT 2592 (8 December 2005).

[30] The *Privacy and Data Protection Act 2014* (Vic) replaced the *Information Privacy Act 2000* (and the *Commissioner for Law Enforcement Security Act 2005*) from 9 December 2014 (most provisions of the Act came into operation on that date).

[31] *WL v La Trobe University (General)* [2005] VCAT 2592, [17]-[18] (footnote omitted).

[32] "apparent." *The Macquarie Dictionary Online* 2013. <https://www.macquariedictionary.com.au> (viewed 8 December 2014).

- approximately 9 months of call and data records (from 19 February 2014 to 27 November 2014)[33]
- 12 months of call records (28 November 2013 to 27 November 2014)[34]
- sample longitude and latitude positions of specific cell towers.

60. Telstra confirmed that of the metadata provided in response to the notice to produce the following information had not (at that time)[35] been provided to the complainant:

    - sample longitude and latitude data
    - incoming call information/records
    - detailed outgoing data records for approximately 9 months showing the time and date, and cell tower location information in relation to, the commencement of data sessions.[36]

61. Telstra explained that, despite it being metadata associated with the complainant's mobile phone service, it did not consider longitude and latitude data to be personal information. Telstra also reiterated its view that providing the complainant with call and data records containing personal information relating to the B-party (such as IMEI, IMSI and B-party location) would have an unreasonable impact on the privacy of those third parties.

62. I do not have access to all of the metadata that falls within the scope of this complaint. Telstra explained on 19 January 2015 that other metadata such as IP addresses and URL information was not provided in response to the notice to produce because Telstra does not provide this type of metadata to law enforcement agencies.[37]

63. I have considered the nature of the metadata to which the complainant has not been provided access. Taking the sample of cell tower location information (latitude and longitude positions) as an example, this is not metadata that one would know plainly from the information was related to the complainant. The complainant's identity is not apparent from this information alone.

64. Other network data such as IP addresses and URLs, is also unlikely to be information, on the face of the information itself, from which the complainant's identity is clearly perceived.

---

[33] Data records are only available for approximately 9 months.
[34] Some of the call record information duplicates the call records contained in the call and data records in the above file for the same period of time.
[35] Telstra subsequently provided a redacted version of the outgoing data records with B-party information redacted.
[36] Telstra response to the OAIC, 19 January 2015.
[37] Telstra response to the OAIC, 19 January 2015.

65. I am therefore of the view that the complainant's identity would not necessarily be apparent from some of the metadata he is seeking.

Can the complainant's identity 'reasonably be ascertained' from the information?

66. In any case, the complainant is not contending that his identity is apparent on the face of the metadata sought. Rather he is claiming that if law enforcement agencies and national security bodies can on request access metadata connected with his phone service, his identity must reasonably be able to be ascertained from that metadata, and on that view, is personal information for the purposes of the Privacy Act and therefore information to which he is entitled access:

> …law enforcement can access my records but I am being prevent (sic) from doing so. I just want the same access that they have to my records. There are more than 300,000 requests from law enforcement agencies to telcos for metadata every year, which doesn't include ASIO requests (they aren't required to report figures). That's a lot of requests and citizens deserve the same access as them.[38]

67. Telstra submits that the information I have before me does not support such a view.

68. The Privacy Act does not define the meaning of the expression 'reasonably be ascertained'. According to *The Macquarie Dictionary Online* (2013), 'ascertainable' means "able to be found out by trial, examination or experiment, so as to know as certain; determine".[39]

69. 'Reasonably' qualifies 'ascertainable' and relevant to the circumstances of this matter means, "not exceeding the limit prescribed by reason; not excessive".[40]

70. I have had regard to Deputy President Coghlan's consideration in *La Trobe University (General)* of whether or not an individual's identity could reasonably be ascertained from health survey information that had to be extracted from different databases and then cross-matched twice:

> 44 Just what is meant by "reasonably ascertained from the information" is not so clear. Does it mean ascertained solely from the information without reference to anything else? One would think it might not…
>
> …45 ….The use of the word "ascertained" must allow for some resort to extraneous material unless it is to be regarded as mere surplusage.
>
> … 52 Even allowing for the use of external information, the legislation requires an element of reasonableness about whether a person's identity can be ascertained

[38] Complainant's submission to the OAIC, 21 July 2014.
[39] "ascertainable". *The Macquarie Dictionary Online* 2013. <https://www.macquariedictionary.com.au> (viewed 8 December 2014).
[40] "reasonably". *The Macquarie Dictionary Online* 2013. <https://www.macquariedictionary.com.au> (viewed 11 March 2014).

> from the information and this will depend upon all the circumstances in each particular case…[41]

71. When considering the issue of reasonableness about whether an individual's identity could be ascertained from the information, Coghlan DP examined both:

    (a) the complexity of the inquiries that would need to be made to ascertain the information and

    (b) the degree of certainty with which possible connections between that information and the individual's identity could be made.[42]

72. Examining firstly the issue of whether the identity of an individual can be ascertained from the metadata held by Telstra to which the complainant has been refused access, I accept the statements made by Telstra's NIO General Manager during his oral submission[43], including those noted at paragraphs [49] to [51] of this determination and those that follow.

73. Telstra's NIO General Manager explained that it is possible to extract the data that is held on various network elements and network management systems spread across Telstra's mobile network, and ascertain a customer's identity with a good degree of certainty by cross-referencing this metadata with other data held in Telstra's customer management and subscriber record systems. The NIO General Manager has also stated that this type of metadata retrieval is currently undertaken to resolve complaints about connectivity service and performance.[44]

74. During his oral submission Telstra's NIO General Manager noted the transient nature of the metadata held on Telstra's network elements and network management systems:[45]

> The amount of metadata stored and subsequently retrieved is subject to the storage capacity of Telstra's network at any given time. This means that:
>
> - it is possible to extract customer data for a specific network element at a specific time to give certain customer information, but not possible to give a complete overview of customer information

---

[41] *WL v La Trobe University (General)*[2005] VCAT 2592, [44]-[45], [52].
[42] *WL v La Trobe University (General)* [2005]VCAT 2592, [52].
[43] Telstra General Manager, Network Infrastructure Operations, Determination Hearing, 2 October 2014.
[44] See paragraph [49]. The statement made by the Telstra NIO General Manager referenced at paragraph [49] is notably at odds with statements made by Telstra in its earlier written submissions and referenced at paragraphs [45] and [46] of this determination about there being no likely scenario in which Telstra would undertake this type of data retrieval exercise. However in light of Telstra's General Manager's working knowledge and experience with Telstra's Network Infrastructure Operations, I give his oral statement more weight than the more generalised statements outlined in Telstra's earlier written submissions.
[45] Telstra General Manager, Network Infrastructure Operations, Determination Hearing, 2 October 2014.

- the network systems operate on a 'best-effort' basis; that is, they are (with the exception of Telstra's billing system) not guaranteed to capture everything, but everything that is captured is accurate.[46]

75. He confirmed that the type of metadata that could be retrieved included that which Telstra has, to date, refused the complainant access to. That is:

- cell tower information (by initially checking billing records to ascertain where a mobile has initiated a data session and then focussing on the network elements associated with that location)
- destination and source IP addresses.

76. I have also heard from Telstra's Operations Manager, Law Enforcement Liaison (LEL Operations Manager), who confirmed that additional to extracting metadata for network assurance purposes, Telstra extracts metadata to provide to law enforcement agencies and national security bodies on request.[47]

77. Subsequent to me issuing a notice under s 44(3) of the Privacy Act, Telstra's LEL Operations Manager attended before me on 18 November 2014 and provided the following information, which I accept:

- the metadata provided to law enforcement bodies is generally extracted from call charge record systems which are distinctly separate systems to the network management systems used by Telstra's Network Infrastructure Operations to extract customer information for network assurance purposes
- the information provided to law enforcement bodies includes:
  - call charge record requests (which may include A-party phone number and cell tower location, the suburb from where the call was connected, time/date/duration of call, B-party number and if party B is a Telstra subscriber, the suburb where call was received, IMEI and IMSI)
  - personal details of the person who is subscribed to the phone number (subscriber information)
  - subscriber record requests (where the agency has a phone number and requests that Telstra give them information about that number, e.g., the name of the account holder, billing information associated with that number, the date the account was created, etc.)
  - general packet radio service (GPRS) data requests.[48]

[46] See also paragraphs [49]-[51].

[47] Telstra Operations Manager, Law Enforcement Liaison, Meeting before the Commissioner, 18 November 2014.

[48] Meeting before the Commissioner, 18 November 2014. Telstra's LEL Operations Manager explained 'GPRS data provides information about when radio packets were travelling on the network, including the date and time this data exchange commenced and the duration of the exchange. The GPRS data does not include the content of what was exchanged'.

- Telstra's Law Enforcement Liaison takes a staged approach to providing information to law enforcement bodies, disclosing information relating to a specific request (for example, 'subscriber data', or 'call charge record request'). Enforcement bodies may then come back with further requests for additional information. A staggered response allows Telstra to better time manage and prioritise requests.

78. I have also considered Telstra's Transparency Report[49] which confirms the provision of metadata to law enforcement bodies in response to requests made by them. The Transparency Report highlights 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 ("agencies") between 1 July 2013 and 30 June 2014. It is notable that this figure does not include the number of requests for information made by national security agencies such as ASIO, public disclosure of which is prohibited under the *Telecommunications (Interception and Access) Act 1979* (Cth).

79. Requests from law enforcement agencies, according to the Transparency Report, includes requests for the following types of information:

- customer information such as customer's name, address, service number and connection dates
- carriage service records including call records, SMS records, and internet records (including details of a called party and the date, time and duration of a call)
- internet session information including the date, time and duration of internet sessions as well as email logs from Telstra Bigpond email addresses. This does not include URLs of Internet browsing activity.

80. Similarly I have taken into account the *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (the Inquiry Report), tabled by the Parliamentary Joint Committee on Intelligence and Security on 24 June 2013, which details the type of metadata that may be disclosed by Telstra to law enforcement and national security agencies.[50] According to the Inquiry Report this includes:

- subscriber information
- telephone numbers of the parties involved in the communication
- the date and time of a communication

[49] Telstra.com, *Transparency at Telstra* (1 July 2013 – 30 June 2014) (Transparency Report) <https://www.telstra.com.au/privacy/transparency>.

[50] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (2013) Appendix H <http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm>.

- Internet Protocol (IP) addresses and Uniform Resource Locators (URLs) (to the extent that they do not identify the content of a communication) and
- location-based information.[51]

81. Telstra confirmed in its closing submission that it has provided URL information to a law enforcement agency though notes that it was 'an almost unique instance.'[52]

82. I am of the view that the process of ascertainment of an individual's identity involving inquiries from and cross-matching against different network management and records management systems is not only possible, but is in fact, a process that Telstra already puts into practice, not only for network assurance purposes but also in responding to large numbers of requests for metadata by law enforcement agencies and other regulatory bodies.

83. I am satisfied that Telstra's response to law enforcement agency requests in addition to its regular practice of extracting metadata for network assurance purposes is indicative of its ability to ascertain with accuracy an individual's identity from metadata linked to that individual which exists on its mobile network and to which an individual might seek access.

84. Having come to this conclusion, the question is then whether the process of ascertaining an individual's identity from the metadata should be considered reasonable in the circumstances. That is, does the process of ascertainment exceed reasonable limits or is it excessive in the context of the present circumstances?

85. The definition of personal information under the Privacy Act requires an element of reasonableness about whether a person's identity can be ascertained from the information and this will depend on the circumstances of each particular case.[53]

86. Telstra contends that the identity of a customer cannot *reasonably* be ascertained from Telstra's network data. It has argued that the metadata retrieval process would be burdensome in terms of complexity, time and cost:

> Network data generated through the use of [the Telstra] mobile telephone network is not kept in a single repository. The network data is spread out across

[51] According to Telstra, the information in Appendix H of the Inquiry Report (which was provided by Telstra in response to additional questions on notice from the Parliamentary Joint Committee) is a reference to metadata generally, and not specifically to mobile metadata: see Telstra's closing submission to the OAIC, 19 November 2014, 15, n 18. See also paragraphs [97] – [98].

[52] Evidence to Legal and Constitutional Affairs References Committee, Comprehensive revision of the *Telecommunications (Interception and Access) Act 1979*, Parliament of Australia, Canberra, 26 September 2014, 38 (James Shaw, Director Government Relations, Telstra), cited in Telstra's closing submission to the OAIC, 19 November 2014, 15, n 17.

[53] *WL v La Trobe University (General)*[2005] VCAT 2592, [52].

> many different network elements and systems where it is mixed with information generated from the use of those networks by other users…[54]
>
> Identifying and retrieving any network data relating specifically to the complainant would be difficult, time consuming and costly. Only a very limited number of [Telstra] personnel who are technical experts on network design and configuration, and have access rights to the multiple systems, would have the knowledge and expertise required to access all the relevant systems and retrieve this information.[55]

87. The quantity of data that can be retrieved at any one time may contribute to the complexity of the data retrieval process. According to the oral submissions of both Telstra's LEL Operations Manager and NIO General Manager, metadata such as IP address information is transient and in some cases may only be retained for a matter of 3-5 days. Other information, such as cell tower information, is reportedly retained for periods of up to only 30 days:

    - there is generally a 30 day metadata retention period but the storage capacity of the network systems is volumetric, which means that increased customers with increased calls will result in some data being retained for lesser periods. For example, system A might have a 30-day retention period but system B only has 5 or 10 days (because of the volume going through the system), so it will not be possible to capture data after this time period.[56]

88. This means that because only a certain amount of metadata can be stored at any one time, no more than that amount can be retrieved at any particular point in time to provide information about an individual.

89. Telstra in its written submissions has suggested that in relation to interrogation of Telstra's network management systems, despite the limited storage capacity of some of those systems, it would still require 'significant manual effort … to identify and extract all relevant data':

> …. Our mobile telephone networks have not been designed with this type of data retrieval in mind and, as such, do not have any in-built functionality to easily enable identification and on-mass retrieval of data relating to individual customers.[57]
>
> In order to identify and retrieve relevant network data, an experienced network engineer would need to first obtain relevant network identifiers…. and then interrogate each network element using these identifiers in order to confirm whether or not they hold any relevant data.
>
> … Even if an appropriate engineer with the right access privileges can be identified, completing the data retrieval exercise would be extremely time

[54] Letter from Telstra to the OAIC, 25 July 2104, 2.
[55] Letter from Telstra to the OAIC, 25 July 2014, 3.
[56] Telstra General Manager, Network Infrastructure Operations, Determinations Hearing, 2 October 2014.
[57] Letter from Telstra to the OAIC, 25 July 2014, Attachment B, 2.

> consuming. To give an indication, we estimate that data retrieval and analysis … would take:
>
> - a minimum four days full time engagement for one week's data retrieval; or
> - a minimum twelve days full time engagement for four (or more) week's data retrieval …
>
> In addition, the direct costs (e.g. salary) and indirect costs (e.g. lost productivity) to us of losing the contribution of a skilled employee for a long period would be very significant. While [the complainant] has offered to pay the cost of Telstra complying with his access request, we consider it unlikely that he would be prepared to cover the true cost of this.[58]

90. Telstra's NIO General Manager during his oral submission confirmed that the process of retrieving metadata like IP addresses and cell tower location information from Telstra's network management systems may be lengthy:

> …data such as destination and source IP addresses, as well as cell tower information is recorded, but could take up to 3 weeks to retrieve due to the complexities involved in interrogating the network systems.[59]

91. In comparison pulling metadata from other records management systems seems much faster. Subscriber record requests for example can be provided 'in a matter of minutes', while extracting metadata from a call charge record system[60] may by contrast take a day or more for expert staff to extract the requested information from the relevant system.[61]

92. From its submissions, Telstra seems to be saying that the metadata captured on its systems at any one time may only constitute days of data, but depending on which system the information is pulled from and the type of metadata being retrieved, the retrieval process could take from a matter of minutes to a number of weeks.

93. I accept that the process of extracting some of the metadata falling within the scope of the complainant's request may require interrogation of several of Telstra's information systems by a group of specifically qualified personnel. I also accept that the process of ascertaining this information may take some time to obtain. However this process of ascertainment needs to be considered in a practical context, in this case, relative to Telstra's resources and operational capacities.

---

[58] Letter from Telstra to the OAIC, 25 July 2014, Attachment B, 2.

[59] Telstra General Manager, Network Infrastructure Operations, Determinations Hearing, 2 October 2014.

[60] I note that according to Telstra's LEL Operations Manager, metadata such as IP address information is not captured on call charge record systems and is therefore not able to be retrieved from those system types. Telstra Operations Manager, Law Enforcement Liaison group, Meeting before the Commissioner, 18 November 2014.

[61] Telstra Operations Manager, Law Enforcement Liaison group, Meeting before the Commissioner, 18 November 2014.

94. Telstra is a large organisation with many resources at its disposal. On review of the oral testimony of Telstra's NIO General Manager and LEL Operations Manager[62] it is apparent that Telstra has a pool of over 120 staff with expertise in data retrieval of this kind and who are already specifically engaged in the retrieval and cross-matching of metadata in response to requests from law enforcement bodies or to problem-solve customer connectivity service or performance issues.

95. I also cannot discount the fact that according to its own Transparency Report Telstra received and responded to around 85,000 requests for customer information within a 12 month period (this number excluding requests made by national security bodies).[63]

96. Furthermore the Inquiry Report tabled by the Parliamentary Joint Committee on Intelligence and Security on 24 June 2013, confirms that the type of metadata that may be disclosed by Telstra to law enforcement and national security agencies includes the type of metadata sought after by the complainant.[64]

97. In its closing submission to the OAIC Telstra contends that the information provided in the Inquiry Report is a reference to metadata generally, and not specifically to mobile metadata which is the nature of the complainant's access request.[65] In my issuing of a notice to produce in November 2014 I gave Telstra an opportunity to provide further information in relation to any distinction it might hold between generalised and mobile telecommunications activity. Telstra did not submit any further information on this point.

98. As a result, in the absence of further information from Telstra going to this issue, I cannot be satisfied that any such distinction exists, or indeed is relevant to the present matter.

99. I consider that Telstra bears the evidentiary burden in respect of its assertion that the metadata the complainant is seeking is not his personal information. The onus is on Telstra to demonstrate that it is outside of the limits of reason for Telstra to provide the complainant with information that it provides or may provide to law enforcement agencies and other regulatory bodies.

100. Telstra has indicated the process of metadata retrieval may be lengthy and/or complex, but it has not demonstrated that the process is beyond what is reasonable relative to the resources it has at its disposal and its existing

---

[62] Telstra Operations Manager, Law Enforcement Liaison, Meeting before the Commissioner, 18 November 2014. Also Telstra's General Manager, Network Infrastructure Operations, Determination Hearing, 2 October 2104.

[63] Telstra.com, *Transparency at Telstra* (1 July 2013 – 30 June 2014) (Transparency Report) <https://www.telstra.com.au/privacy/transparency>.

[64] Parliamentary Joint Committee, Parliament of Australia, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (2013) Appendix H <http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm>.

[65] Telstra's closing submission to the OAIC, 19 November 2014, 15, n 18.

operational capacities. I also take into consideration that under NPP 6.4 an organisation can charge for access provided the charge is not excessive. I have dealt with this issue in more detail at paragraphs [158] to [168].

101. Telstra's handling of tens of thousands of requests made by law enforcement bodies, together with its recent public statement affirming that customers may access their metadata on request, suggests instead that Telstra has the capacity through the use of its network and records management systems to ascertain the identity of an individual and this process of ascertaining an individual's identity does not exceed the bounds of what is reasonable.

102. I am consequently of the view that the metadata Telstra holds in connection with an individual which permits that individual's identity to reasonably be ascertained from that metadata constitutes the personal information of that individual under the Privacy Act.

103. I therefore find that in the present set of circumstances, the metadata held by Telstra to which it refuses to give the complainant access (the so named 'network data') constitutes the complainant's personal information under the Privacy Act.

National Privacy Principle (NPP) 6.1

104. If an organisation holds personal information about an individual, it must provide the individual with access to the information unless an exception applies to the information in question.

105. The complexity of a request for personal information, in and of itself, does not constitute one of the exceptions provided at NPP 6.1(a)-(k). The complexity, as well as the scope of an individual's access request goes to the estimates of time (and cost) in which an organisation might give access.[66].

106. There are no exceptions to the obligation to provide access that are relevant to the metadata sought after by the complainant which Telstra has labelled 'network data'. Accordingly I find that Telstra's refusal to provide that information in breach of NPP 6.1 of the Privacy Act.

107. My consideration of the NPP 6.1 exceptions relevant to this matter centres on Telstra's obligation to provide the complainant with access to inbound call numbers. I deal with the relevant exceptions at paragraphs [124] to [154].

Incoming call records

108. Telstra has identified that incoming call records contain, as well as 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.

[66] See Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (September 2001), 49.

109. As I have said, the complainant has made it clear that he is only concerned with Telstra's refusal to give him access to the numbers of incoming callers. He does not want other third party data found in incoming call records. The complainant asserts that inbound call numbers constitute information about him and information from which his identity can reasonably be ascertained:

> [An incoming call number] is personal to me because that other person called me. They didn't call someone else.[67]

110. Telstra, on the other hand, initially contended that, along with other third party data, inbound call numbers to the complainant's mobile service are not personal information for the purposes of s 6 of the Privacy Act because they are not information about the complainant:

> While a call made or an SMS sent to [the complainant] could be considered information about [the complainant], we do not think that the number which made the call or sent the SMS is personal information about [the complainant]. [The complainant's] identity is not apparent or ascertainable from the calling number or sending SMS number. This is not information about an action that [the complainant] has taken, but is rather information about an action taken by the person making the call or sending the SMS. If anything, it is personal information about that person, rather than about [the complainant].[68]

111. Telstra appears not to have maintained this position.[69] Its current contention is that even if inbound call numbers fall within the scope of the complainant's personal information, the exception to disclosure at NPP 6.1(c) of the Privacy Act permits Telstra to refuse to provide that information to the complainant.

112. In some of its earlier submissions[70], Telstra also appears to have relied on arguments relating to exception provisions NPP 6.1(g) and/or (h) dealing with unlawful access and/or the requirement to deny access by or under law.

Information about the complainant

113. The concept 'about an individual' may apply not only to an item of information that identifies the individual, but to other information about that individual.[71] In the matter before me I must also consider whether or not this includes information about who has called the complainant.

---

[67] Complainant's submission to the OAIC, 21 July 2014, 1.

[68] Letter from Telstra to the OAIC, 14 February 2014, 5.

[69] This argument was not put forward during the Determination Hearing dated 2 October 2014; nor was it outlined in Telstra's closing submission to the OAIC dated 19 November 2014.

[70] Letter from Telstra to the OAIC, 24 January 2014. See also letter from Telstra to the OAIC, 14 February 2014.

[71] See *'BA' and Merit Protection Commissioner* [2014] AICmr 9 (30 January 2914), [56]. The same definition of 'personal information' is found in both the Privacy Act and the *Freedom of Information Act 1982* (Cth).

114. According to *The Macquarie Dictionary Online* (2013) the word "about" means "in regard to, concerning or connected with".[72]

115. In the present case, inbound call numbers have been recorded in circumstances which associate those numbers and the callers of those numbers with the complainant.

116. In *WL v Randwick City Council (GD)* the Appeal Panel explored the meaning of an identical definition of personal information in s 4 of the *Privacy and Personal Information Protection Act 1998* (NSW), observing that:

> Documents which themselves do not contain any obvious features identifying an individual may take on the quality by virtue of the context to which they belong. [73]

117. It appears to me that an inbound call number, in the context of the complainant's mobile phone activity, comprises shared information about both the incoming caller and the complainant. Calls being made to the complainant's mobile service reveal information about the complainant as well as the incoming caller. I am of the view that information about who is calling the complainant is consequently personal information about the complainant, notwithstanding that it may also be the personal information of other individuals.

Can the complainant's identity 'reasonably be ascertained' from the information?

118. In his oral submission Telstra's Operations Manager said that Telstra receives regular requests for, and provides to agencies, subscriber records as well as call charge records (inbound and outbound) which include the phone numbers of persons who initiated calls to the complainant.[74]

119. Though I am of view that the identity of the complainant would not be apparent from the phone numbers alone, it is clear that the complainant can be identified from the inbound call numbers to his mobile service in the context of those subscriber and call charge records.

120. Requests for call charges records are regularly made by law enforcement agencies[75] and the sought-after information is provided without excessive inquiry or delay. I also note that the association between inbound call numbers to an individual's phone service and that individual's identity can be made with certainty.

121. I am therefore satisfied that the process of ascertaining the complainant's identity is reasonable in these circumstances. Accordingly I find that the inbound

---

[72] "about." *The Macquarie Dictionary Online* 2013. <https://www.macquariedictionary.com.au> (viewed 11 March 2015).

[73] [2007] NSWADTAP 58, [15].

[74] Telstra Operations Manager, Law Enforcement Liaison, Meeting before the Commissioner, 18 November 2014.

[75] Requests for call charges records constitute the majority of requests made by law enforcement agencies: Telstra Operations Manager, Law Enforcement Liaison, Meeting before the Commissioner, 18 November 2014.

call numbers constitute personal information about the complainant under the Privacy Act.

Exceptions to obligation of access

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

123. Relevantly here, NPP 6.1(c) provides that an organisation may refuse an individual access to their personal information in instances where providing access would have an unreasonable impact on the privacy of other individuals.

124. Telstra contends that it was not obliged to provide access to inbound call numbers because providing access would have an unreasonable impact on the privacy of others, namely the incoming callers:

> Callers may have silent numbers, block their numbers when calling or may have simply dialled the wrong number. Telstra's network records of these calls are not able to identify these different scenarios and therefore, any release of such information would potentially be against the caller's wishes and a breach of the Telecommunications Act 1997.[76]

125. Telstra has also, throughout its submissions, referred to its obligations under the Calling Number Display Industry Code (the Code) 'which places obligations on carriage service providers to protect the Calling Line Identification (CLI) they receive when facilitating the delivery of a call'[77]:

- [The complainant] contends that if Telstra has access to details of the number of a person who has called [the complainant] then [the complainant] should be able to access that information even if the person in question has actively blocked their phone number in order that it not be disclosed to him. This is in direct conflict with the obligations imposed on carriage service providers like Telstra under the Calling Number Display Code to allow callers to block calling number display (either on a permanent or a per call basis) to the called party in order to protect their privacy. If accepted, [the complainant's] position would fundamentally undermine this important privacy protection.[78]

- Significantly, Telstra is required to ensure that its customers have the choice of blocking their calling number display, *however it generally has no way of determining whether an originating party has chosen to do so*. That is, it would generally not be possible for Telstra to ascertain those incoming calls to the Complainant's service where the originating party had chosen to block his or her calling number display. This underscores the general point that the provision of

[76] Letter from Telstra to the OAIC, 24 January 2014, 2.
[77] E.g. Letter from Telstra to the OAIC, 14 February 2014, 5, citing Australian Communications Industry Forum, *Calling Number Display Industry Code*, ACIF C522:2007, February 2007.
[78] Letter from Telstra to the OAIC, 15 August 2014, 2.

> incoming call records would have an unreasonable impact upon the privacy of the originating parties of the communications.[79]

126. The complainant's position is that providing access to the phone numbers of incoming callers would not have an unreasonable impact on the privacy of other individuals, being those individuals who called the complainant. The complainant states that:

> If the caller has decided to block their phone number from being seen by me and Telstra's database doesn't record that caller's number then I don't want it. If there is a record of a call taking place with 'X' as the number I'd like to see it.[80]

127. Although the complainant has submitted that he is entitled to know the phone numbers of those individuals who have called him because this is information personal to him, 'his right to access is not unqualified'[81]. In this case the inbound call number is also personal to the incoming caller.

128. In *Smallbone v New South Wales Bar Association*[82] Yates J cited with approval those factors identified by the then Privacy Commissioner in *C v Insurance Company*[83] as relevant to the assessment of whether providing access to documents would have an unreasonable impact on the privacy of other individuals, including relevantly here:

- whether the individuals would expect that their information would be disclosed to a third party, including whether an assurance of confidentiality was provided
- the extent of the impact on the individuals' privacy.

129. I have considered whether incoming callers would expect that their phone numbers would be disclosed to the complainant and to what extent access might impact on the privacy of those incoming callers.[84]

130. The Calling Number Display (CND) Code provides in its Explanatory Statement that:

> Callers in many situations may not wish the receiver to be able to identify their telephone number. Doctors who call patients from home, customers who call businesses but do not wish to be contacted in the future, and victims of domestic violence are some of the groups who may not want their numbers disclosed.[85]

---

[79] Telstra's closing submission to the OAIC, 19 November 2014, 10 [29] (emphasis in original).
[80] Complainant's submission to the OAIC, 12 March 2014, 1 [2].
[81] See *Smallbone v New South Wales Bar Association* [2011] FCA 1145, [58].
[82] [2011] FCA 1145, [49]-[50].
[83] [2006] PrivCmrA 3.
[84] My findings in respect of incoming call records are confined to the issue of inbound call numbers.
[85] Explanatory Statement, Australian Communications Industry Forum, *Calling Number Display Industry Code*, ACIF C522:2007, February 2007, (i).

131. It is reasonable to think that individuals who take up the option of a silent line or who block their line or number so that it doesn't appear when they call, do not wish (and would not reasonably expect) their phone number to be disclosed to the recipient of the call, at the time of the call or at some time thereafter.

132. Telstra's online brochure, '*A Short-ish Guide to How We Can Look Out For Each Other*' (online brochure), which provides an overview of Telstra's customer terms, as well as Telstra's Privacy Statement, includes information about sending your phone number to other phones and calling number display. It states the following:

> Some of our services, including mobile phone services, automatically send your phone number to other phones when you call or message them. This lets the other person see your number when you call or message them. You may be able to use blocking on your phone, or have us block your number for a monthly fee, so your number doesn't appear when you call. However, your number can't be blocked on messages (including Premium SMS messages) sent from your phone. Our mobile services also support the CND feature, so you can see the number of the person calling you (unless they've blocked it). If you're using a mobile, check the user guide to make sure your phone supports CND, and to see how you turn it on or off.[86]

133. Telstra provides additional online advice about silent line and call blocking options to customers on its 'Features and Services, Home Phone features package' webpage:

> If you have call blocking or line blocking enabled on your phone line, or you have a Silent Line, your Calling Line Identification (CLI) will generally not be disclosed to third parties.[87]

134. On the basis of Telstra's online advice, I am satisfied that callers who have a silent line or who have opted to block their line or CND if they have the CND feature could not reasonably expect that their numbers may be disclosed by Telstra to the recipient of the incoming call on the recipient's subsequent request.

135. If callers take active steps to make their phone numbers unavailable to recipients at the other end of a phone communication, in my view, any subsequent disclosure of that information to those recipients would be an unreasonable impact on the privacy of those callers.

136. Telstra has argued against the view that those incoming callers who did not contact the complainant through a silent line or block their line or CND implicitly

---

[86] Telstra Corporation Limited, *A Short-ish Guide to How We Can Look Out For Each Other* (September 2014) < https://www.telstra.com.au/help/download/document/things-you-need-to-know-about-telstra-services-c048.pdf >.

[87] Telstra Corporation Limited, *Features and Services, Telstra Home Phone features package,* <https://www.telstra.com.au/home-phone/features-services?ssSourceSiteId=consumer-advice#call-number>.

consented to their phone numbers being disclosed to him by Telstra.[88] A view that incoming callers have implicitly consented to disclosure assumes, without more, that consent is inferred from an incoming caller's failure to take up the option of a silent line or line or CND blocking.

137. Such a view does not take into account situations where the wrong number may have been dialled. Even putting that circumstance to one side, the fact that incoming callers have intentionally contacted the complainant without blocking their line or CND does no more, on its own, than establish the willingness of those callers to contact the complainant and have their number revealed at that time, not that they have consented to their phone information being disclosed by Telstra to the complainant on his request at some later date.

138. I accept that there are likely different levels of expectation between those callers who have blocked their line or CND or opted for a silent line, and those who have not.

139. Telstra's online advice sends a clear message that an incoming caller's phone number will be disclosed to the recipient of the call if the caller does not block their line or number (or have a silent line). This arguably may go to the drawing of an inference of reasonable expectation of disclosure of the number to the call recipient.

140. Notwithstanding this, Telstra does not indicate in any of its online information that it may at some later time disclose a person's phone information to the recipient of a call on the recipient's request. Although a recipient's phone will likely store details of an incoming call, any expectation of disclosure by Telstra is in my view is limited to disclosure at the time of the call.

141. Moreover Telstra's Privacy Statement creates an assurance of confidentiality by generating an expectation that personal information will be managed by Telstra in accordance with its obligations under the Privacy Act.[89] The disclosure by Telstra of a caller's phone number at some later date to the recipient of the call on the request of the recipient is inconsistent with any such expectation.

142. Not all disclosures of personal information will have an unreasonable impact on the individuals whose personal information is disclosed. Whether disclosure would have an unreasonable impact on the privacy of those individuals 'is a matter of practical judgment having regard of all the circumstances of the case'.[90]

143. In this case, for those callers who did not opt for a silent line or did not block their line or CND, there is a real possibility that the recipient could identify the caller. The recipient in this case is a journalist for a well-known newspaper. As I

[88] Letter from Telstra to the OAIC, 24 January 2014, 2.
[89] Telstra Corporation Limited, *Privacy Statement* (November 2014) <https://www.telstra.com.au/content/dam/tcom/personal/privacy/pdf/Privacy-statement-Nov-2014.pdf>.
[90] *Smallbone v New South Wales Bar Association* [2011] FCA 1145 , [47].

have said, calls being made to the complainant's mobile service creates an association between the complainant and the incoming caller, and may of itself say something, whether true or not, about the parties to the call.

144. In cases where the creation of such an association is unintentional (i.e. wrong number dialled), any future disclosure of information which identifies that association in my view represents an arbitrary interference with the privacy of the unintentional participant. I am satisfied that granting subsequent access to the phone information of callers who have become inadvertently associated with the complainant journalist would prejudice the privacy of those callers.

145. I am of the view that a subsequent disclosure of phone information that could identify unintentional callers as having contacted the complainant journalist would have an unreasonable impact on the privacy of those callers.

146. In circumstances where callers (who do not have a silent number or CND or line blocking) have intentionally contacted the recipient it is less certain whether subsequent access by the recipient to their phone numbers would result in an unreasonable impact on their privacy. It my view it is likely that in many circumstances, it might reasonably be expected that these callers would consent to the disclosure if they were aware of it.

147. I do not need to draw any firm conclusion on this point however, because of my consideration (below) of whether or not the numbers of unintentional callers, as well as silent numbers and the numbers of those with CND or line blocking, can be sufficiently masked to protect the privacy of the individuals holding those numbers.

Can access be granted to redacted inbound call number information?

148. The Privacy Act makes it clear that access to personal information held by an organisation should be provided as fully as possible, 'except to the extent that an exception applies'[91]. This intent is re-iterated in the *Guidelines to the National Privacy Principles*, which provide that:

> 49 … There are a limited number of situations where an organisation may deny an individual access to the personal information an organisation holds about them. Where such an exception applies to a request for access, an organisation would ordinarily need to give the individual access to the parts of the record that are not exempt.
>
> 50 … Access to a document containing personal information about people other than the individual requesting access need not be denied altogether. For example, in such a case, it may be possible to delete the other individual's

[91] *Privacy Act 1988* (Cth) sch 3 cl 6.1.

personal information from the document before it is released to the individual who made the request.[92]

149. Telstra has outlined the steps it would need to take in order to provide access to that information which is not, on the face of it, caught by the NPP 6.1(c) exception; in other words, to remove access to the phone numbers of those who contacted the complainant unintentionally and those who have a silent line or CND or line blocking.

150. Telstra has indicated that although it is generally not practically possible to identify from its records those callers who have blocked their line or CND[93], it may be possible for specialised staff to interrogate network data for no more than about 30 days to identify such callers.[94] However it is not at all possible for Telstra to identify from its records those customers who have unintentionally contacted the complainant.

151. I am therefore of the view that it is not possible to edit the incoming call numbers to provide only the numbers of those individuals who have intentionally contacted the complainant and who do not have a silent line or CND or line blocking.

152. I therefore find that Telstra can rely on NPP 6.1(c) to refuse the complainant access to the phone numbers of incoming callers.

153. Telstra's conduct in denying the complainant access to this information is therefore not in contravention of NPP 6.1.

Application of NPP 6.1(g)/NPP 6.1(h)

154. In its earlier submissions Telstra also contended that the release of phone information where callers have a silent line or line or CND blocking or have called a wrong number would potentially not only be against the wishes of the caller, but a breach of the *Telecommunications Act 1997* (Cth) (Telecommunications Act)[95] and in direct conflict with Telstra's obligations under the Code[96].

155. In view of my finding that Telstra is not obliged to provide the complainant with access to incoming call numbers by operation of NPP 6.1(c), I have not

---

[92] Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (September 2001), 49-50. These guidelines have been superseded by the Australian Privacy Principles guidelines which apply from 12 March 2014.

[93] Letter from Telstra to the OAIC, 25 July 2014, Attachment C, 2. Also Telstra's closing submission to the OAIC, 19 November 2014, 10 [29].

[94] Telstra's closing submission to the OAIC, 19 November 2014, 10, n 12.

[95] E.g.Telstra's submission to the OAIC, 24 January 2014, 2. Also Telstra's submission to the OAIC, 14 February 2014, 5-6.

[96] Telstra's submission to the OAIC, 15 August 2014, 2. Absent reference to a specific provision in the Code, Telstra would appear to be referring to the general obligations of carriage service providers to provide privacy protections in the use of CLI and CND.

considered whether or not Telstra could also rely on NPP 6.1(g) and 6.1(h) to deny the complainant access.

Charge for access

156. In his initial request to Telstra, the complainant anticipated being charged a fee for access to his information:

> If there is a cost associated with getting the data please advise what it may be.[97]

157. In his complaint to the OAIC the complainant re-iterated that he would pay for access to his metadata information if the cost was reasonable.[98] He goes on to say:

> But it really shouldn't be a cost I have to pay to begin with… this data should be freely accessible on request.[99]

158. A decision to charge for access to personal information is at the discretion of the relevant organisation. Under NPP 6.4 an organisation may impose a charge for access provided that it is not excessive.[100]

159. The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000[101] indicates that the intention of NPP 6.4 is to allow for organisations to charge for access to personal information only where complying with the request for access imposes 'substantial costs' on the organisation.[102]

160. Information provided by Telstra's LEL Operations Manager indicates that the costs associated with complying with requests from law enforcement agencies and other regulatory bodies for subscriber information and call charge records are not onerous and depending on the nature of the request may range from $10 for a simple request to at most $200.[103]

161. Telstra has nonetheless contended in its written submissions that the costs involved in assigning its personnel to a network data retrieval exercise would be 'very significant'.[104]

---

[97] Complainant's initial request to Telstra, 15 June 2013.
[98] Complainant's submission to the OAIC, 12 March 2014.
[99] Complainant's submission to the OAIC, 12 March 2014.
[100] National Privacy Principle 6.4:
If an organisation charges for providing access to personal information, those charges:
(a) must not be excessive…
[101] This is the amending legislation to the *Privacy Act 1988* (Cth) which introduced NPP 6.
[102] Notably under the post-12 March 2014 legislative regime, there is no reference to costs having to be substantial before organisations can charge for access. Under APP 12.8 which deals with access charges, an organisation must not charge an amount that is excessive. The Explanatory Memorandum for the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 indicates that a charge will be considered 'excessive' when an organisation charges more than the actual cost incurred by the organisation in providing access.
[103] Telstra's LEL Operations Manager, Meeting before the Commissioner, 18 November 2014.
[104] Letter from Telstra to the OAIC, 25 July 2014, Attachment B, 2.

162. Telstra has not provided any detailed information relating to the potential diversion of additional staff from their regular duties to metadata retrieval duties or what financial impact this might have on its operations. No specific costings have been provided.

163. Oral submissions from both Telstra's NIO General Manager and LEL Operations Manager suggest that there is already existing specialised Telstra staff engaged in the function of retrieving metadata in response to requests from law enforcement bodies and for network assurance purposes.

164. As I have said the information that the complainant is seeking is information that may be provided to law enforcement agencies and other regulatory bodies at a minimal cost.[105] It is difficult to see how the cost of the complainant accessing his own data can be so prohibitively high when this is information that is already (or may be) provided to these bodies thousands of times per year.

165. Based on the information I have available to me, the costs involved in retrieving the complainant's data are, in my view, unlikely to be substantial.

166. By way of confirmation, Telstra, in its recent online statement regarding customers' access to their metadata, has indicated that simple access requests for metadata are expected to cost around $25, while more detailed requests will be charged at an hourly rate. Telstra confirms that this is a similar cost recovery model to that currently applied to requests for metadata from law enforcement agencies.[106]

167. In considering whether Telstra is entitled to charge for access in this particular matter, I note that the resolution of this matter has been protracted, a direct result of Telstra's persistent hold to its initial position over the course of the complaint that metadata does not constitute personal information.

168. 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 and the resultant time taken, it would in my opinion be appropriate for Telstra to provide the complainant's personal information to him free of charge.

Damages

169. I have no information before me of any actual loss or damage suffered by the complainant, who has not requested compensation.

---

[105] See Parliamentary Joint Committee, Parliament of Australia, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (2013) Appendix H <http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm>.

[106] Kate Hughes, 'A principle of privacy' on *Telstra News* (6 March 2015) <http://exchange.telstra.com.au/2015/03/06/a-principle-of-privacy>.

170. I therefore decline to make a declaration under s 52(1)(b)(iii) of the Privacy Act relating to compensation.[107]

Determination

171. I declare in accordance with s 52(1)(b)(i)(B) of the Privacy Act that:

- the complainant's complaint is substantiated;
- Telstra has breached NPP 6.1 by failing to provide the complainant with access to his personal information in breach of NPP 6.1 of the Privacy Act.

172. I declare in accordance with s 52(1)(b)(ii) of the Privacy Act that the respondent must:

- within 30 business days after the making of this declaration, provide the complainant with access to the following personal information held by Telstra in accordance with complainant's request dated 15 June 2013 and further to that already provided by Telstra to the complainant, save that Telstra is not obliged to provide access to the phone numbers of incoming callers:
- Internet Protocol (IP) address information
- Uniform Resource Locator (URL) information
- Cell tower location information beyond the cell tower location information that Telstra retains for billing purposes (to which the complainant has been given access).[108]
- provide the complainant with access to the above information free of charge.

Timothy Pilgrim
Privacy Commissioner

1 May 2015

[107] Under s 52(1)(b)(iii) of the Privacy Act, I may find the complaint substantiated and make a determination that includes a declaration that the complainant is entitled to a payment of compensation for 'any loss or damage suffered by reason of' the interference with privacy. Under section 52(1A), loss or damage can include 'injury to the complainant's feelings or humiliation suffered by the complainant'.

[108] E.g., Telstra's closing submission to the OAIC, 19 November 2014, 12.

Review rights

A party may apply under s 96 of the *Privacy Act 1988* to have a decision under s 52(1) or (1A) to make a determination reviewed by the Administrative Appeals Tribunal (AAT). The AAT provides independent merits review of administrative decisions and has power to set aside, vary, or affirm a privacy determination. An application to the AAT must be made within 28 days after the day on which the person is given the privacy determination (s 29(2) of the *Administrative Appeals Tribunal Act 1975*). An application fee may be payable when lodging an application for review to the AAT. Further information is available on the AAT's website (www.aat.gov.au) or by telephoning 1300 366 700.

A party may also apply under s 5 of the *Administrative Decisions (Judicial Review) Act 1977* to have the determination reviewed by the Federal Circuit Court or the Federal Court of Australia. The Court may refer the matter back to the OAIC for further consideration if it finds the Information Commissioner's decision was wrong in law or the Information Commissioner's powers were not exercised properly. An application to the Court must be lodged within 28 days of the date of the determination. An application fee may be payable when lodging an application to the Court. Further information is available on the Court's website (http://www.federalcourt.gov.au/) or by contacting your nearest District Registry.