A review of Telstra Corporation Limited and Australian Privacy Commissioner

Australian Administrative Appeals Tribunal, [2015] AATA 991, 18 December 2015

The Tribunal's overturning of an earlier determination by the Australian Privacy Commissioner throws open the issue of when device information is 'about an individual whose identity may be reasonably ascertained from the information.'

In May 2015, the Australian Privacy Commissioner, Mr Timothy Pilgrim PSM, had found that Telstra had breached the Australian Federal Privacy Act 1988 (the 'Privacy Act') by failing to provide journalist Ben Grubb with access to requested metadata relating to his use of Telstra telecommunications services as collected and held by Telstra in various databases for various purposes, some purely technical e.g. operation of the network and monitoring its performance. This Determination (*Ben Grubb v. Telstra Corporation* [2015] AICmr 35, 1 May 2015) has been reviewed in this publication[1]. The case required application of the pre-March 2014 definition of 'personal information,' being 'information about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion' (this definition is be contrasted to the current Privacy Act definition of 'personal information,' which is information 'about an identified individual or an individual who is reasonably identifiable').

The Commissioner considered that the question of whether an individual's identity can 'reasonably be ascertained' from information required assessment as to how unreasonably high the level of effort necessary to link an individual through to non-identifying information must be before an entity receiving an access request can say that the access that is requested is not to information from which an individual's identity can reasonably be ascertained. It was not contended that Mr Grubb as an individual could be linked to some network data relating to use by Mr Grubb of his mobile phone through a multi-step process (requiring significant labour input and including manual matching) of tracing and matching records through multiple databases in Telstra's systems. Although Mr Grubb's identity was not apparent in relevant Telstra databases where relevant metadata was held, the device identifiers or IP addresses or other transactional information there held could be traced through from mobile tower records to operational and network databases and on to personally identifying databases (in particular, the Telstra customer billing database). Telstra regularly facilitated requests by law enforcement agencies for lawful assistance as to the use of mobile phones by persons of interest by undertaking such tracing and matching processes.

Of course, Telstra's practice of assisting law enforcement agencies as required by law did not of itself answer the question of whether existence of a possibility of tracing from source information to identifying information should lead to a determination as to whether an individual's identity can reasonably be ascertained from the information. The Privacy Commissioner quoted a decision by Deputy President Coghlan in *WL v. La Trobe University* [2005] VCAT 2592 that such consideration requires examination of the complexity of the inquiries that would be needed to ascertain the information and the degree of certainty with which possible connections between that information and the individual's identity could be made. In circumstances where an individual's identity could only be ascertained from health survey information that had to be extracted from different databases, cross-matched and then cross-matched to an external database "and even then the making of any possible connections would not identify with certainty" the relevant individual, DP Coghlan concluded that this went "beyond what is reasonable" (WL at para 52). By contrast, the Privacy Commissioner found that "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" (*Ben Grubb v. Telstra* at para 101).

Tribunal Deputy President S A Forgie, in the Administrative Appeals Tribunal's Decision overturning the Privacy Commissioner's Determination, stated that where an individual is not intrinsically identified in information, a two-step characterisation process should be applied. The first step is determining whether relevant information is "about an individual." The second step is working out whether an individual's identity "can reasonably be ascertained from the information or opinion." If relevant information is not "about an individual," that is the end of the matter. But if information is information "about an individual," the second step must be applied.

It was in relation to the first step that the reasoning of DP Forgie most clearly diverged from the Privacy Commissioner. After noting that the range of what may be considered to be information "about an individual" is infinite and included, for example, information relating to the person's physical description, residence, place of work, business and business activities, telephone number and so on, DP Forgie stated (at para 112):

"Had Mr Grubb not made the calls or sent the messages he did on his mobile device, Telstra would not have generated certain mobile network data. It generated that data in order to transmit his calls and his messages. Once his call or message was transmitted from the first cell that received it from his mobile device, the data that was generated was directed to delivering the call or message to its intended recipient. That data is no longer about Mr Grubb or the fact that he made a call or sent a message or about the number or address to which he sent it. It is not about the content of the call or the message. The data is all about the way in which Telstra delivers the call or the message. That is not about Mr Grubb. It could be said that the mobile network data relates to the way in which Telstra delivers the service or product for which Mr Grubb pays. That does not make the data information about Mr Grubb. It is information about the service it provides to Mr Grubb but not about him."

Similar reasoning may suggest that, for example:

- a transient or ephemeral device identifier, such as an internet protocol ('IP') address used to establish an internet session and manage interactions between an internet service provider and a user;
- a more pervasive identifier such a mobile phone's unique 15 digit International Mobile Station Equipment Identity ('IMEI') number;
- service records or records of use of a household device; and
- a motor vehicle licence plate;

may not satisfy the first step of this characterisation process, because it is not information "about an individual": rather, it is information about an inanimate object that may be associated with an individual. Or to put it another way, the fact that information about an inanimate object may be retrievable by reference to an identified individual does not of itself make the information about the object information about an individual.

The problem is that the first step has an element of circularity, as had been noted by the New Zealand Human Rights Review Tribunal applying a similar definition of 'personal information' in the case of *Apostolakis v. Sievwrights* (14 February 2005, HRRT 44/03[2]). The NZ Tribunal there stated:

"[59] The matter is further complicated because the answer to the question 'Is this personal information?' can, we suspect, depend on how the question is asked. If one were to approach an observer and ask: 'A owns a building which is insured. Is the fact that the building is insured 'personal information' about A?' the answer might well be 'no, it is information about the building.' On the other hand, if one were to approach the same person but ask 'Is the fact that A has insurance on her building 'personal information' about A?' then the answer might well be 'yes - it is information which tells me something about A's rights in respect of the building that she owns.'

The NZ Tribunal concluded that there is no 'bright line' test, suggesting instead that although a person may not be identifiable in the information, if there is a 'sufficient connection' to an individual that connection may justify a conclusion that the information is personal information about that person. However, this reasoning just interposes another phrase to be interpreted and applied: at what point is an inanimate object associated with an individual 'sufficiently connected' to that individual that the information ceases to be about the object and becomes about the individual? If information about use of a mobile phone, typically carried on a person through most of their waking hours and intimately associated with (and often creating an electronic record of) a person's life, is not information about an individual, what information recorded by Internet of Things devices is (to use the test suggested by the NZ Tribunal) 'sufficiently connected' to an individual? The AAT in the *Telstra* appeal did not refer to the New Zealand cases, but there does appear to be an underlying concept of closeness of association, or as the NZ Tribunal put it, whether there is a sufficient connection. Applying DP Forgie's reasoning, a distinction might be made between a Fitbit or other personal health device which clearly gathers information about an individual, and cellular network connectivity features of a mobile phone that enable continuous calls notwithstanding handoffs between mobile towers, where relevant location information is collected for call management, not for tracking movement of an individual.

In stating the second stage test, DP Forgie followed generally accepted reasoning in Australia and New Zealand as to whether an individual's identity "can reasonably be ascertained from" information as allowing reference to extrinsic materials, but only such extrinsic materials as are reasonably available. DP Forgie then gave a striking illustration of how this test might be applied:

"In dealing with a request [by an individual for access to personal information about them] under the Privacy Act, it does not follow that an organisation need scour the public domain to ascertain whether there is information that

can be married with the information or opinion it holds in order to ascertain the identity of the individual. What it means is that the organisation must keep in mind what might be matters of general knowledge. If, for example, the information were along the lines of 'singer and songwriter who died prematurely,' I do not think that it could be said that the identity of that individual can reasonably be ascertained from that information. If the information were 'female singer and songwriter who died prematurely,' I suggest that her identity would also not be reasonably ascertainable. If the information were 'English female singer and songwriter who was known for her eclectic mix of musical genres of soul, rhythm and blues and jazz but who died prematurely in July 2011' [Amy Whitehouse], I suggest that the identity of the individual can be reasonably ascertained from the information which would be regarded as part of the broad body of general knowledge" (at para 107).

DP Forgie then continued: "Beyond what might be considered to be general knowledge, I do not think that regard needs to be had to the wide range of information and means of searching information that is available in the public arena in determining whether an individual's identity is reasonably ascertainable from the information or opinion held in an organisation" (at par 108). This proposition appears overstated: release of purportedly de-identified information into the public arena in circumstances where a motivated intruder could be anticipated as able to apply means of re-identifying an individual is generally regarded as a disclosure of personal information.

The reasoning of the Administrative Appeals Tribunal is both novel and controversial. The Australian Privacy Commissioner had appealed the Tribunal's Decision to the Federal Court of Australia. A Full Bench of the Federal Court will hear the appeal, probably in August 2016. One possibility is that on appeal the Decision may stand and the Tribunal's reasoning limited to the specific context before it, namely, working out what information should be made available by a data controller in response to an access request by an individual. In that context, considerations of practicality and cost mitigate against overly broad disclosure requirements. By contrast, decisions by data controllers to release purportedly de-identified data sets into the public arena, where it may be reasonable to expect motivated intruders to seek to re-identify any individual through use of exhaustive searches or strong analytical techniques, might rightly be subject to a test which imposes a higher level of foresight and control. Of course, the words 'reasonably ascertainable' enable a range of context-specific tests to be developed.

As the Internet of Things continues to grow, we may be confident that cases addressing similar questions to those considered in *Ben Grubb v. Telstra* will arise for determination in many jurisdictions.

Peter Leonard Partner
Gilbert + Tobin Lawyers, Sydney
pleonard@gtlaw.com.au

1. E-Commerce Law Reports, Vol 15 Issue 3, pp 17-20, http://www.e-comlaw.com/e-commerce-law-reports/article_template.asp?Contents=Yes&from=eclr&ID=1046
2. Available at www.nzlii.org