



Our reference: D2017/004535

Mr John Stanton
Chief Executive Officer
Communications Alliance Ltd

Via email: stanton@commsalliance.com.au
CC: c.purdon@commsalliance.com.au

Dear Mr Stanton

Consultation on the draft *Integrated Public Number Database (IPND) Code (C555:2017)*

Thank you for the opportunity to comment on the *Integrated Public Number Database (IPND) Code* (the draft Code).

I understand that the 2017 Code revision emphasises processes that are intended to support data quality, including access by individual customers to personal information held in the IPND. The quality of IPND data is critical to the operational, emergency and law enforcement purposes of the database.

My comments below centre on how the draft Code deals with an individual's request for access to their personal information held in the IPND. I have focussed on how the draft Code interacts with the statutory protections provided to individuals under the *Privacy Act 1988* (the Privacy Act).

Access to personal information

Australian Privacy Principle (APP) 12.1 under the Privacy Act provides that:

If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

APP 12.3 sets out a range of exceptions to the general access principle. APPs 12.4 and 12.5 provide a measure of flexibility where it is not reasonable or practicable to give access to information in the manner requested by the individual. More information about how APP 12 applies is available in the [APP guidelines](#).

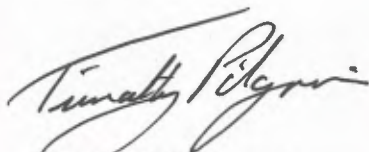
The IPND Manager (currently Telstra), as an APP entity that holds personal information, is required to comply with APP 12. Part 5.2 of the draft Code describes an 'industry agreed process' for customers to access their personal information in the IPND. This process directs individuals to request access to IPND data from their Carriage Service Provider (CSP) rather than from the IPND Manager.

I note that the draft Code does not expressly preclude individuals from seeking access directly from the IPND Manager. However, by this omission the draft Code fails to make it clear that individuals have this option. My preference is that the Code make it clear that access via the IPND Manager is also available, but that there is a favoured industry agreed process. This approach is consistent with section 116A of the *Telecommunications Act 1997*, which provides that an industry code does not derogate from a requirement under the Privacy Act.

I note that there are references to the operational feasibility of alternative processes for customers to access their personal information in the IPND in the Explanatory Statement. Statements of this type need to be considered in light of the IPND Manager's obligation to provide access, unless it is able to rely upon an exception in APP 12.

If you would like to discuss any of the comments above or have any questions, please contact Lucy Scott on (02) 9284 9824 or by email at Lucy.Scott@oaic.gov.au.

Yours sincerely



Timothy Pilgrim PSM
Australian Information Commissioner
Australian Privacy Commissioner

7 July 2017