30 January 2017

Ms Jonquil Ritter  
A/g General Manager  
Content, Consumer & Citizen  
Australian Communications and Media Authority  
PO Box 78  
BELCONNEN ACT 2616

Dear Ms Ritter

Thank you for your letter to the Secretary of 5 January 2016 regarding the Australian Communications and Media Authority’s proposed changes to the Integrated Public Number Database Scheme (the Scheme), which is due to sunset on 1 April this year and is in the process of being redrafted. I am responding on the Secretary’s behalf.

My comments are limited to the proposals to provide ongoing Integrated Public Number Database (the Database) access for research purposes and to allow research entities to provide de-identified data from the Database to their members. I note these proposed changes have been informed by the 2015 Review of the Database (the Review) undertaken by the Department of Communications.

Ongoing Database authorisations for research purposes

This proposal would implement recommendation 5 of the Review, which provides:

The ACMA should be enabled to approve ongoing or periodic access for an applicant, provided that the ACMA regularly reviews access and that a privacy impact assessment is completed [emphasis added].

The draft Scheme does not mandate regular review of standing authorisations. Instead, the consultation paper at page 7 notes that:

It is likely that any authorisation granted on an ongoing basis would be conditional on the research entity providing the ACMA with an annual report on the research entity’s use of IPND data. This would provide an annual review mechanism.

The department’s preference is for the review mechanism to be specified in the Scheme or by other instrument. This would ensure recipients of standing authorisations are clear on their obligations and encourage them to promote sound privacy practice in the management of sensitive data.
Disclosure of de-identified data by research entities to members

The department notes that increasing the availability of deidentified data increases the risk that it may be reidentified. Accordingly, we recommend the Scheme provide that recipients of deidentified data are not permitted to intentionally reidentify or attempt to reidentify it. Further, we recommend the Scheme also provide that recipients of deidentified data are obliged to destroy the data if it is unintentionally reidentified. An example of a regulatory requirement that operates in this way is Rule 7 of the Privacy Commissioner’s Privacy (Credit Related Research) Rule 2014.

The action officer for this matter is Antony Catt who can be contacted on 02 6141 3504.

Yours sincerely

Andrew Walter
Assistant Secretary
Civil Law Unit