Joint ACCAN/APF Response to Department of Communications Consultation on Proposed Recommendations for the Integrated Public Number Database (IPND)

The Australian Communications Consumer Action Network (ACCAN) is the peak body representing all consumers on communications issues including telecommunications, broadband and emerging new services.

The Australian Privacy Foundation (APF) is the primary NGO dedicated to promoting privacy rights in Australia.

We thank the Department for the opportunity to comment on the proposed recommendations for the IPND.

We offer the following responses to the proposed recommendations

Measures proposed by the Department to improve quality and accuracy of the IPND:

1. Enhancing the existing feedback processes between the IPND manager, data providers and data users

We support measures to enhance feedback processes on updating IPND, and thus improving the accuracy of IPND data.

2. Clarifying the regulatory arrangements to ensure subscribers can be provided with the information in the IPND relating to themselves, and to flag incorrect information for action by carriage service providers (CSPs) in a specified timeframe.

We are assuming that the personal information held by the IPND about a subscriber is confined to and identical with the information provided by the subscriber to a carriage service provider (CSP) in relation to a service.

For quite legitimate reasons that same subscriber may provide different personal information to another CSP in relation to a different service(s). In that case, the IPND would contain separate records, each identical to what is provided by the CSP.

For both those situations, when the IPND provides a subscriber with their information in relation to a particular service and the subscriber wishes to either correct or change that information, the subscriber should be advised to contact the CSP for that service to make the change or correction.

If the IPND contains any additional information on subscribers that is generated by the IPND Manager through processing (e.g. matching or linkage), then responsibility for handling any correction requests would remain with the IPND Manager.

We note that the Telecommunications Act may be interpreted as not supporting a subscriber's access to their personal information held by the IPND. However, as the OAIC states, under privacy legislation, subscribers who are individuals should have access to their personal information, subject to appropriate security measures to ensure the information is given only to the individual concerned. The IPND Manager, as an APP entity under the Privacy Act, must respond directly to any access request, and not simply refer a requester to their CSP.

We note, however, that if an individual wishes to correct (or change) the personal information held by the IPND, any changes should be made through the individual's CSP. If an individual subscriber, having obtained access from the IPND Manager, seeks to correct IPND information that has been provided by a CSP, it would be appropriate to refer them to the relevant CSP. Any changes would subsequently flow back to the IPND. This sequence would result in improved data accuracy and consistency for both the CSP and the IPND Manager.

As noted above, however, if any data held by the IPND was not simply that provided by a CSP but was instead generated by the IPND or obtained from other sources, then the correction of that data should be the responsibility of the IPND.

3. Enhancing awareness-raising measures to oblige CSPs to alert their subscribers of their IPND information, and to advise subscribers regularly of the importance of providing correct information.

Given the importance of correct IPND data, particularly in emergency situations, we support this recommendation. We note that CSPs and the IPND Manager have obligations under the Privacy Act to give notice to individuals of various matters, which would include the provisioning of the IPND.

A layered approach to the provision of information would be acceptable, with links leading to successive levels of detail, but a minimum core of information about the IPND must be provided to all CSP customers – they need to be made aware that the personal information they provide as customers is used not just by their CSP but that CSPs are legally required to forward their details to a central database used for a variety of purposes.

Measures proposed by the Department in relation to improving the way the IPND information is disclosed and used:

4. Broadening the range of users able to apply for access to IPND information (including anonymised information about unlisted numbers), including for a wider range of researchers, the Australian Bureau of Statistics (ABS), NBN Co and others subject to a case by case privacy impact test and demonstration of being in the public interest.

This recommendation covers a wide range of potential uses, and needs to be 'unpacked'.

In relation to research use, there are at least two very different types of research use.

Use of IPND information for research about telecommunications services and trends, involving aggregate statistics, and not using the personal particulars of subscribers other than to match or link records, is in the public interest, and should be facilitated. Such research can include information about unlisted numbers. We refer below to this type of research use as Type A. Applications for access for Type A research should remain subject to a public interest test, though not necessarily on a case by case basis (see below). Organisations likely to fall into this category would include the Australian Bureau of Statistics, NBN Co. However, developments in analytic capabilities (popularly known as Big Data) have increased the possibility of re-identifying anonymized data, and cast doubt on assurances about privacy that were previously able to be relied on. Any authorisation for access to IPND data for Type A research should only be granted once credible assurances have been given about protection from re-identification.

Access to subscriber information held in the IPND to use as a sample frame for survey research necessarily involves the use of personal information to contact subscribers (even if the researcher does not need to know the identity of the subscriber). We refer to this type of research as Type B. The research industry have argued that there is a public interest in allowing wider access to IPND information for Type B research, and have also argued that in some cases the public interest will justify access even to unlisted number information (e.g. to ensure that samples are statistically representative).

To ensure that survey research is subject to appropriate professional standards, and is not simply a 'front' for marketing or other purposes, the industry submits that it should be defined as research conducted in accordance with the Privacy (Market and Social Research) Code 2014, developed by AMSRO and registered by the Information/ Privacy Commissioner under the Privacy Act 1988.

ACCAN and APF have serious concerns about Type B research use of the IPND. While we understand the public interest arguments, allowing wider research use would be a major departure from the intent and purpose of the current regime.

Broadening research usage would be expected to lead to more unsolicited research calls. The strong response to the Do Not Call Register (9 million registered numbers and approximately 1 million new numbers registered each year, according to ACMA figures) indicates that a significant number of consumers want to minimise unsolicited research or marketing calls in general. More particularly, consumers have a reasonable expectation of the privacy of mobile numbers, and are accustomed to exercising their own discretion as to who has access to them. ACCAN and APF would have serious concern if changes to the use of the IPND resulted in further unsolicited research calls, which many consumers do not welcome any more than they do marketing calls – many of which deliberately but misleadingly introduce themselves as 'research'.

In the context of research industry proposals, we note there are other legitimate means by which individuals' numbers can be sourced for research purposes from other databases. The most obvious is White Pages, which also includes mobile numbers on an opt in basis. Even when taking account of the carve out of Do Not Call Register numbers, unlisted numbers and silent lines, this still represents a significant resource for general research purposes, albeit not fully comprehensive like the IPND.

ACCAN and APF submit that it is premature to allow any wider access to IPND information for LDCS. Any proposed use for LDCS would need to be very carefully assessed against individuals' reasonable expectations of privacy. Provision of such a facility with LDCS is a complex issue which would require further consultation.

5. Allowing the Australian Communications and Media Authority (ACMA) to approve ongoing or periodic access for an applicant, provided that the ACMA regularly reviews access and that a privacy impact test is completed.

We would support three categories of access: ongoing, periodic and on a case by case basis. Ongoing access (i.e. without a set time limit or sunset clause) would be provided only to organizations that have a demonstrable need for continuing access to IPND information, and the highest level of safeguards. We would envisage that ongoing access would only be considered for organisations that were subject to legislative safeguards (e.g. the ABS, the ACMA and Australian Institute for Health and Welfare).

Periodic access could be provided to organizations such as NBN Co for current subscriber information for provisioning and research into telecommunications services. All other requests for data should be granted, if at all, only on a case by case basis.

For all access arrangements, access should be granted by the ACMA only after an application has satisfied a public interest test. All applications should be accompanied by a privacy impact assessment (PIA) meeting a standard to be set by the ACMA for the specific purposes of IPND access, and developed in consultation with the Information/Privacy Commissioner.

As well, for all access granted (ongoing, periodic or case by case) the relevant organisation/researcher should be required to report (regularly in the case of ongoing and periodic access), both to the ACMA and publicly, on the actual use(s) of data, and the outcomes by reference to the justification in the original application/PIA.

6.☐Improving the transparency of the IPND Scheme

We support the recommendation to publish applications and decisions about the use of IPND data.

7. Streamlining the rules for the production of public number directories from the IPND.

We agree with the Department's recommended approach that would allow anti-scraping technology to be used instead of artificially limiting the number of entries which can be displayed at one time or retrieved in a single search. The use of such technology, however, should only be with the approval of the ACMA, which should be required to satisfy itself that the particular technology to be used will provide an effective and equivalent solution. Otherwise, the current limits on the number of entries that can be displayed at one time should remain.

Measures proposed by the Department in relation to the management of the IPND:

8. Improving transparency of the IPND Management

We support the suggested measures that would require Telstra to demonstrate how it separates its role as part-owner of the publisher of the White Pages and the manager of the IPND. This is however only a sub-set of the wider concern about potential conflict of interest and unfair commercial advantage inherent in Telstra being the IPND Manager. We submit that Telstra should be required to publicly report on all aspects of how it manages this issue, including, as suggested, the standard forms of agreements with IPND data users and an audited financial report.

28 July 2014