Australian Privacy Foundation

email: mail@privacy.org.au

website : www.privacy.org.au

Review of the Integrated Public Number Database (IPND)

Submission to the Department of Broadband, Communications and the Digital Economy

December 2011

The Australian Privacy Foundation

The Australian Privacy Foundation is the main non-governmental organisation dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians. Since 1987, the Foundation has led the defence of the right of individuals to control their personal information and to be free of excessive intrusions. The Foundation uses the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed. For further information about the Foundation and the Charter, see www.privacy.org.au

Please note that APF does not have a single postal address – we prefer communication by e-mail. If a postal address is required please contact the signatory.

Publication of submissions

We note that we have no objection to the publication of this submission in full. To further the public interest in transparency of public policy processes, APF strongly supports the position that all submissions to public Inquiries and reviews should be publicly available, except to the extent that a submitter has reasonable grounds for confidentiality for all, or preferably part of, a submission.

We have highlighted in bold our main recommendations.

Introduction

The Australian Privacy Foundation (APF) has been an active participant in the policy discussions surrounding the establishment of the IPND and related issues, such as the Emergency Call Services Determination and the Do Not Call Register.

The Discussion Paper acknowledges (but not until 2.4) that 'The IPND is a significant store of personal information, and there are major privacy considerations related to the collection, access and use of IPND information.' It does not add that telecommunications information, in certain contexts, can be amongst the most sensitive of personal data. There is a natural tendency to regard telephone numbers as a relatively innocuous or trivial common currency in everyday life, but both the numbers themselves, and the link to subscriber name and address, can be very sensitive for some subscribers – hence the

existence of a system of unlisted numbers or silent lines, and at a different level, the existence of the Do Not Call Register – introduced only recently as a 'special purpose' privacy law in response to major public concern about unsolicited calls. The fact that the IPND must (necessarily for its primary purposes) include unlisted numbers, and yet can and is used for a wide range of secondary purposes, poses particular issues.

Another reason why the IPND raises important privacy issues is that it is an example of a 'statutorily licenced breach' of normal privacy principles. Like the credit reporting system, the IPND mandates the sharing of personal information obtained by organizations from their customers for the provision of a commercial service, and its use for unrelated secondary purposes without their consent. National Privacy Principle 2 in the Privacy Act would normally prohibit such disclosures and uses without consent, as they are clearly not 'related uses within the reasonable expectations of the individuals concerned' (exception (a)) and do not fall within any of the other exceptions other than 'required or authorized by law' (exception (g)). This exception exists expressly to accommodate systems such as the IPND where Parliament has decided that another public interest in effect 'trumps' the normal operation of the privacy principle.

In the case of the IPND, there is also a licenced breach of the collection principle, NPP1, as the Telecommunications Act in general, and the IPND scheme in particular, *mandates* the collection of specific personal information, some of which may not be necessary for the delivery of the service requested by the customer. As with NPP2, such non-conforming collections are rendered lawful by the wording of the principle, which allows for collection to be necessary by virtue of a legal requirement (which must however be explained to individuals (NPP1.3 and 1.5)).

While these exceptions ensure that the IPND does not contravene the Privacy Act, it is incumbent on those administering the IPND to recognize that it is a 'privileged' variation and to seek to minimize the licensed intrusion into individuals' privacy that is necessarily involved.

In this context, APF welcomes the distinction drawn in the Discussion Paper between 'critical' and 'non-critical' uses and users of IPND data. This distinction assists a discussion of the appropriate balance between privacy and other public interests in relation to each category of use/user.

Also of fundamental significance is the fact that Australia is the only jurisdiction (at least from those compared) to allow multiple uses of its IPND or equivalent database. This is unfortunately only raised at the end of the Discussion Paper (4.2), almost as an afterthought. We submit that it should have been mentioned at the outset – absent this knowledge, readers may have simply assumed that the current Australian situation was the norm, when in fact it is atypical.

It is unfortunate that the government has delayed its response to the ALRC Recommendations, in Part J of Report 108 on privacy, on Telecommunications, as resolution of some of the wider issues canvassed in that report would have provided valuable context for the IPND specific issues. Instead, we are all having to use the specific case of the IPND to address important issues which have wider implications – there is a danger that an incoherent and inconsistent response will emerge. Given this unfortunate sequencing of policy development, it is essential that the government takes the time to consider the wider implications of changes to the IPND regime for the wider telecommunications privacy framework. We have commented where we can with this objective in mind.

Collection of IPND Information (DP 2.1)

DP Questions:

1. How could the way that data is collected be changed to improve accuracy?

2. More generally, how can the collection of IPND data be improved?

It is important to recognise that not all customers (subscribers) would accept the premise that accurate and complete information about them in the IPND provides a benefit to them that outweighs their privacy interest. The government and its agencies can legitimately promote benefits both to individuals (such as emergency assistance) and to the wider public interest, but some individuals will not be persuaded, particularly given the wider and ever-increasing range of 'non-critical' uses of the IPND. A certain level of inaccuracy due to customer reticence is inevitable – any attempt to enforce compliance CSPs would require draconian measures which would be disproportionate to the public interest benefit.

The Discussion Paper mentions 'awareness' requirements (page 5) but does not ask any specific questions about them. APF notes that in addition to the cited requirement in the IPND Code, CSPs are also required under NPP1.3 to take reasonable steps to ensure that their customers are aware specifically about 'any law that requires the personal information to be collected' ((1.3(e)) and about uses and disclosures (1.3(c) and (d)). We question whether most CSPs are fully complying with these requirements, and submit that both ACMA and the Privacy Commissioner (OAIC) should monitor and enforce these obligations more vigorously.

As an additional transparency and accountability measure, we submit that either DBCDE or ACMA should be required to publish and maintain a current register of all IPND users, including organisations with authorisations for secondary uses.

We submit that there should be an up to date register of all IPND users.

Access to IPND data (DP 2.2)

The presentation in the Discussion Paper e.g. in Figure 2, could usefully have referred to 'the IPND Manager (Telstra)' rather than to 'Telstra' as the latter potentially confuses readers about Telstra's role – it is of course also an IPND Data Provider and, potentially, an IPND User.

The definition of IPND User in the Discussion Paper is flawed in that it refers to "organisations that use IPND information to provide services to end users, subscribers and the public." Some IPND users – specifically law enforcement agencies - do not provide 'services' in the sense that this definition implies.

Figure 2 is also misleading in implying that the application of the Privacy Act is limited to collection of personal information. The principles in the Act relate to all phases of information handling – collection, use, disclosure, storage and disposal; to data quality and security at all stages, and provide access and correction rights – all of these principles apply to all participants in the IPND scheme – CSPs, the IPND Manager and IPND data users except for a few (e.g. small organisations, and of course political parties and politicians) which may be exempt. While Part 13 of the Telecommunications Act provides detailed rules about use and disclosure, these only supplement NPP2 for private sector organisations (and IPPs 10 & 11 for agencies) and the IPND scheme supplements the generic collection, quality and security obligations, Part 13 does not replace the application of any of the privacy principles, and the Discussion Paper could usefully have reminded readers of this.

DP Questions:

3. Is the disclosure regime for IPND data adequate, too broad or too narrow? Why?

4. How can the disclosure regime for IPND data be simplified?

The disclosure regime is too broad in that it provides for multiple purposes and many non-critical uses, which creates difficulties in terms of data quality and its 'fitness for purpose'. We expand on this general view in the answers to specific questions below. In answer to Q.31 we submit that some non-critical uses should be discontinued.

Whilst simplification is generally desirable, it should not be a primary objective – the IPND scheme should be as complex as it needs to be to appropriately balance competing public interests in relation to the different categories of uses and users.

New Users (DP 2.2.1)

DP Questions:

5. Should new users of IPND data be allowed? What principles should guide access to IPND data by new and existing users?

We submit that the government should strongly resist the temptation for the IPND to become a common resource for a variety of other public and private interests. Privacy principles, with their emphasis on limited uses of personal information for specified purposes, contain an implicit presumption against centralized multi-purpose databases. We also refer again to Table 3 in the Discussion Paper which shows that Australia is the only one of the five jurisdictions mentioned to allow multiple uses.

The Discussion Paper specifically raises the possibility of the IPND being used to update the Do Not Call Register (DNCR). **We submit that the relationship between these two databases (IPND and DNCR) needs to be considered more widely.** We would need to see evidence of significant problems with direct updating of the DNCR by CSPs, or other significant reasons, to be convinced that this should be done instead via the IPND.

On the other hand, **we submit that there is a strong case for the output from the IPND for some secondary purposes to be automatically 'cleaned' by the IPND Manager before release against the DNCR**. This should apply to those uses which will result in contact being made with the subscriber, including 'electoral research' and 'other research', and even, potentially, public number directories (see below).

Unfortunately, the government has seen fit to exempt research calls and political canvassing from the application of the DNCR. We lobbied against this at the time, and continue to maintain that these exemptions are unsustainable in the long term, as they clearly contradict individuals' expectations when

they register on the DNCR – most people do not differentiate between the purpose of unsolicited calls and would prefer their 'opt-out' to apply to most such calls (we accept the case for a continued exception of emergency warnings, which should override do not call and silent line preferences)

The possible application of the DNCR to public directories derived from the IPND also involves the complex issue of unlisted numbers (aka 'silent lines').

There are two major reasons why telephone numbers are unlisted. The first, for a high proportion of all mobile numbers, is because the subscriber has not 'opted in' to a directory entry. The second, for most of the unlisted geographic of fixed line numbers, is because individuals have made a conscious decision to 'opt-out'. This in turn may be due to one of two broad categories of reasons. Firstly because the subscriber does not wish to received unsolicited calls – in this respect the DNCR has provided an alternative, but the relationship is complex – some people may choose to be unlisted but not on the DNCR, and vice versa. Secondly there are subscribers who have a genuine safety or security concern – these include significant sub-categories of individuals who would risk significant harm if their telephone number, with or without other details, was made known to certain other parties. Some of those in this latter category choose a 'suppressed address' option where this is offered.

The unlisted number issue is further complicated by the fact that some CSPs, including the dominant fixed line provider Telstra, charge a fee for an unlisted number. This acts as a deterrent for subscribers and has in our view, expressed in numerous submissions, always been unjustifiable and objectionable. We note that the ALRC in its Report 108 accepted this and recommended that the Telecommunications Act be amended to prohibit the charging of a fee for an unlisted (silent) number on a public directory (Recommendation 72-17). **We submit that the government should take the opportunity of the IPND Review to accept and implement this recommendation**.

We also submit that further consideration be given to the relationship between the IPND and the DNCR in the context of a review of the DNCR and its exceptions.

See our answer to Q.17 about access by individuals to their own records – if it is necessary to make them authorised IPND data users in order to allow such access then this should be done.

Data Elements (DP 2.2.2)

DP Questions:

6. Are the current restrictions on what data elements IPND users can access appropriate? If not, why and what changes should be made?

7. What data elements should be in the IPND? What principles should guide the addition or removal of data elements?

These questions should be reversed – in privacy terms the first goes to collection principles while the second addresses use and disclosure.

In relation to question 7, the issue of *what* information is required to be provided to the IPND Manager is clearly critical from a privacy perspective, and involves questions of necessity and proportionality. The starting point should be that only information proportionally necessary for the *critical* uses of IPND data is required, and not any additional information which is only necessary for secondary *non-critical* uses (this should only be collected with the free and informed choice of the subscriber).

Table 1 addresses this but only at the level of broad types of data – a detailed analysis should be conducted at the level of the individual data fields. We recognise that some information which may not be necessary for *one* of the critical purposes (such as subscriber address for emergency services – something we have questioned in relation to the Emergency Call Services Determination) may however be necessary for another critical purpose (subscriber address for law enforcement) – this is illustrated in Table 1 by the examples of prior public number (only necessary for law enforcement) and identity information (not necessary for emergency warning). The combined effect may be that all of the information currently required to be provided is necessary for one or more of the critical purposes, but we submit that this needs to be clearly established, in order to satisfy the collection principles in the Privacy Act.

The sample IPND entry at Attachment C to the Discussion Paper shows how addresses are recorded.

There are fields for 'Service Address' (Data element 7) and Directory Address (element 8) and a further field 'Alternative address flag' (element 17) which 'Indicates that the service address provided may not be where the service terminates'[1]. There appears to be some uncertainty about the precise meaning of service address and directory address and how these relate to any 'billing address' that a CSP will almost certainly have for customer. We understand that many of the data quality concerns expressed by critical IPND data users relate to these uncertainties.

We submit that data quality issues in this area are a direct consequence of the 'forced' use of information collected for one purpose (provision of telecommunications services) for different purposes i.e. the statutory licencing of a breach of the normal privacy principle to which we referred in our Introduction. Each category of use of the IPND data – whether critical or non-critical – will have its own reasons for wanting to know about a particular type of address – emergency services will typically want to locate premises or whereabouts, whereas law enforcement agencies, and many of the non-critical users, may be more interested in making contact with a particular individual than knowing where they are at particular moment in time.

The more the scheme tries to accommodate all of the different user requirements, the more it will necessarily collect and store more information, and involve greater intrusion into the personal affairs of subscribers. We submit that the government should resist any pressure from IPND data users (or from the IPND Manager on their behalf) to make any changes to the Scheme that would place greater requirements for detailed address information on subscribers. Genuine concerns about, for instance, non-availability of accurate service location information to emergency services should be addressed through consumer education rather than compulsion.

One example of the tendency to collect more information than is strictly required is the type of use (residential, business or government). Data element 10 in the sample entry is a usage code for

[1] We note that Emergency Services treat all 04xx (mobile) services in the same way as IPND records with the Alternative Address flag set, because of uncertainy about the subscriber's current location (Attachment D to the Discusssion Paper pp. 1&2)

'Information about the entity using the number' with these three variables and a fourth - 'not available'. APF was involved in early discussions about the data standard for the IPND and strongly made the case for this only being recorded only where it was known to the CSP.[2] There is no statutory requirement for subscribers to nominate their intended use and while some CSPs differentiate residential and business and government users in their commercial offerings, there must not be any compulsion on subscribers to 'accurately' describe their status. We hope that no 'pressure' on subscribers to specify residential or business has 'crept back' into the way that CSPs collect customer information for onward transfer to the IPND, and that neither IPND data nor the IPND Manager have been actively seeking to reconcile this usage code with e.g. the subscriber name and/or address. Absent any statutory requirement, if a business customer wants to subscribe on a residential plan, or vice versa, this should be their choice, and the IPND scheme should not operate in such a way as to deny them that choice. The fact that law enforcement and emergency services might find the type of service information useful[3] should not automatically translate into a requirement for it to be mandatory or pressure on subscribers to provided it.

The Discussion Paper cites examples of additional data elements that could be added such as next of kin for emergency purposes, and acknowledges that any such expansion would raise privacy concerns. **We submit that the threshold test for any additional data elements must remain very high to prevent the IPND becoming any more of a 'multi-function' database than it already is (function creep)**.

Question 6 relates to access to the various data elements. **We support the principle of differential access, with IPND data users having to justify which data elements they need** – well expressed in 2.2.2 as 'data minimisation'.

The Discussion Paper implies that there are currently no detailed controls on which IPND data users can access which data elements. We had thought that there were, somewhere in the confusing array of sections of the Act, instruments and codes/standards. If not, there should be, and a detailed table should be drawn up and circulated for further comment.

One example of differential access is that providers of Location Dependent Carriage Services (LDCS) do not need access to all IPND fields in order to provide routing services (whether or not these involve differential charges). There is however a case for LDCS providers to have access to limited location information even for unlisted numbers. Provision of suburb information may threaten the safety of some unlisted subscribers, but provision of State/Territory and a 'sub-region' aggregated from suburb data may provide significant benefits to individuals which could outweigh any residual privacy risk. An alternative would be to give unlisted subscribers an informed choice as to whether they wanted limited location data to be disclosed to LDCS providers

We submit that there should be further consultation on a specific proposal for limited access by LDCS providers to limited location data for unlisted numbers, and whether this should be offered as a choice to unlisted subscribers.

[2] This is reflected in the fact that 'type of subscriber' (and service address location) is only provided 'where practicable' (Telstra Licence Conditions cited in Attachment D of the Discussion Paper, page 1)
[3] Discussion Paper, Table 2 and Attachment D,page 2

Access through the IPND Scheme (DP 2.3)

DP Question:

8. Are the objectives of the IPND Scheme still relevant? How could the objectives be recast for a better outcome?

The Discussion Paper only asks about objectives in the context of secondary non-critical uses – section 2.3 confusingly sets out the objectives of the authorisation process as though they are the objectives of the entire IPND scheme. The distinction made earlier in the Discussion Paper between critical and non-critical uses of IPND data is helpful, and a question about objectives should have been asked at that point.

We submit that the primary objective of the IPND scheme should be to meet the needs of critical users whilst minimising involuntary privacy intrusion. Non-critical or secondary uses should be seen as subordinate, with a higher hurdle to be jumped to justify both collection of data in the first place, and subsequent access, and where appropriate, greater choice and stronger conditions.

DP Question:

9. What additional conditions should apply to IPND information accessed through the IPND Scheme?

The ALRC recommended a security breach notification requirement in relation to the IPND (Report 108 Recommendation 72-15). There is now an active wider debate about the need for a mandatory data security breach notification scheme both as a complement to privacy laws to address increasingly common instances of security lapses involving personal data, and to support other security objectives. Issues in the design of such a scheme include the threshold tests that should apply to requirements to notify either a regulator (such as the Information Commissioner) and/or the affected individuals.

Pending the introduction of a wider national scheme, we submit that all participants in the IPND Scheme, including holders of authorisations for secondary non-critical uses, should be required to notify the Office of the Australian Information Commissioner where there has been a substantive or systemic data breach resulting in the disclosure of protected information (criteria for 'substantive or systemic'[4] would be needed but there are many precedents in laws of other jurisidictions).

Under existing own-motion investigation powers, the Information Commissioner would then be able to investigate whether a security breach has involved an interference with an individual's privacy under the Privacy Act.

At present, the Commissioner can only make non-binding recommendations as a result of an own-motion investigation, Pending proposed changes to the enforcement powers in the Privacy Act, the IPND

[4] This is the test recommended by the ALRC in Recommendation 72-15

scheme should require IPND participants to comply with any recommendations from the Information Commissioner arising from an own-motion investigation, including specifically any requirement to notify affected individuals

We submit that the IPND scheme should be amended to require IPND scheme participants to :

(a) Notify the Australian Information Commissioner of any substantive or systemic data security breach, and

(b) **Comply with any recommendations from the Australian Information Commissioner arising from an investigation into a data security breach, including recommendations concerning notification of affected individuals.**

Public Number Directories (DP 2.3.1)

DP Questions:

10. Are the current IPND arrangements a barrier to innovation and competition in the directories product market? What regulatory changes would encourage greater innovation?

Encouragement of competition and innovation in the directories product market should only be a secondary objective and must remain subject to the primary objectives of providing for the critical uses whilst minimising involuntary privacy intrusion.

11. Should all publishers of directory products be required to use the IPND as the source of their data? Why/why not?

All publishers of public number directory products (not just currently defined PNDP publishers) should be required to use the IPND. The company which controls the IPND Manager, should it publish directory products, should be required to use the IPND as the source of its data. There are several reasons for this

- To ensure that all PNDP publishers are subject to the same rules and safeguards (a level playing field)
- So customers of CSPs other than the company controlling the IPND Manager are not required to provide personal information to a third-party business (i.e. Sensis), due to commercial arrangements
- To simplify the system and reduce the likelihood of errors
- To ensure that the IPND Manager has strong business reasons to ensure the accuracy and currency of IPND listings

Note that this issue would be avoided if the IPND Manager was not Telstra – see our answer to Q.27

We submit that if the company which manages the IPND (that is, currently, Telstra) publishes directory products it should be required to obtain its directory data exclusively from the IPND.

Following the same arguments, providers of directory assistance services (in practice Telstra on behalf of itself and many other CSPs) should also be required to source all of the information from the IPND.

DP Question:

12. Alternatively, should the same use and disclosure restrictions in Part 13 of the Tel Act apply to all directory products, regardless of where the information is sourced? Why/why not?

The general use and disclosure provisions of Part 13 and of the Privacy Act do, as they should, apply to all publishers of directory products. The question is whether the *additional* requirements of the IPND scheme relating to PNDP publishers (including those in Part 13) should apply to all directory product publishers. We note that the ALRC recommended that they should (Recommendation 72-16) and concur with this. See also our answer to Q 11.

Again, the same requirements should apply to the provision of all directory assistance services.

We submit that the specific additional requirements of Part 13 relating to the IPND should apply to all directory product publishers and to all providers of directory assistance services

There is an issue concerning the coverage of directory publishers – it would not be appropriate for the IPND scheme to apply to all organisations (or individuals) making publicly available small selective lists of phone numbers e.g. sectoral or local directories – some of the conditions that apply to PNDP publishers would be impossibly onerous and are unnecessary. We are uncertain as to whether the current definitions avoid this potential problem.

Access by researchers (DP 2.3.2)

DP Questions:

13. Are the categories of permitted research purposes too broad, adequate or too narrow? Why?

14. What high-level principles should govern the addition or removal of permitted categories of research?

15. Should the ACMA authorise ongoing access for particular organisations? If so, what protections should be put in place to ensure that the privacy of subscribers is upheld?

It is disappointing that the Discussion Paper does not explain what authorisations are currently in force for research access – how can stakeholders answer these questions in an informed way without knowing whether and if so how the provision for research access has been used. The fact that the Minister has made provision for three categories of research is of limited value without knowing how these have been used and whether ACMA has imposed any limits or conditions in its authorisations. See our earlier recommendation for a public register of all IPND users.

APF strongly supports the ALRC report 's questioning of access to the IPND for 'electoral research' – this 'special treatment' continues the hypocrisy of the major political parties collusion to exempt themselves from the normal operation of privacy principles that are imposed on the wider community (Privacy Act Section 7C, and similar exemptions in other laws). So-called 'electoral research' (a cover term for political canvassing) should receive no special privileges. This category should be removed from the legislative instrument.

The other two categories of research specified in the instrument are public health (undefined other than to include epidemiological research) and 'research conducted by or on behalf of the Commonwealth …. which will contribute to the development of public policy' (an extremely wide definition). Both of these are subject to a condition that the 'research is not conducted for a primarily commercial purpose', but this of course allows for incidental commercial purposes, and this could also potentially be manipulated by a primarily commercial organisation 'laundering' its project through a false 'research' front.

APF submits that these two categories of research are far too wide and that there is no justification for such a generous exceptions to the principle that use and disclosure of personal information should, by default, be only with the consent of the individuals concerned (whether at the time of collection or subsequently).

The case for exceptions to this general principle has been made and resolved in relation to the Privacy Act with a much more limited set of exceptions for 'health and welfare' research access to 'health information', subject to a strict regime involving ethics committee approvals. Researchers of any description do not otherwise enjoy privileged access to other (non-health) information, and this should also be the case for IPND information.

APF submits that if it was to be decided to retain privileged access to IPND information for any research purposes, there should firstly be an amendment to s285(3) of the TA to strengthen the test that the Minister must apply in prescribing 'kinds of research' (as recommended by the ALRC[5].

The process and conditions for authorisation of specific research within the terms of the legislative instrument should be as follows:

- **It should remain subject to project specific authorisations from ACMA**
- **Applicant researchers should have to explain why they cannot obtain the desired personal information from other sources, and justify how the public interest in their research outweighs the privacy interests of IPND data subjects (subscribers) (this re-inforces and complements the effect of the test the Minister must apply in designating 'kinds of research')**
- **Applicant researchers should have to explain how they will use the IPND information and what notice, and choices, they will give to any individuals they contact using IPND information**
- **The default requirement should be that researchers contacting individuals using IPND information should give them an immediate opportunity not to participate and to have their information flagged as not to be further used (the alternative of deletion could result in the details re-appearing in subsequent data batches and being used again). Operationalising this requirement needs to be considered further in the context of suppression lists including the Do Not Call Register (see discussion below on opting out)**

[5] Report 108, Recommendation 72-14

If the third category of research is to be allowed, we submit that it should not be limited to research by or on behalf of the Commonwealth, but should be a generic exception for any level of Australian government, subject to a condition that the agency or contractor involved is subject to an equivalent set of obligations as are found in the Privacy Act.

We understand that most 'research' use of IPND data involves contacting subscribers i.e. the IPND data is used as a sample frame. It may be that there are some categories of research use where the interest is in the aggregate characteristics of telephone subscriber population and there is no intention to contact subscribers. Such research would pose minimal privacy risks and subject to appropriate safeguards should be allowed.

There should be an exception for access to IPND data by relevant regulators (including ACMA and the Australian Information Commissioner) for the purposes of research into the operation of the IPND scheme. Such research may or may not involve contacting subscribers. We are not sure why this could not be authorized under the third category, but if not, the fact that this access is not available appears to be an oversight and unintended consequence of the drafting of the Scheme and should be rectified. An exception outside the 'research' category may be necessary to allow for monitoring or auditing that might fall outside a definition of research (see our response to Q.20 below).

In accordance with our general submission in response to Qs 1&2 above, a list of organisations authorised to use IPND data for research (and/or IPND auditing) should be published and kept up to date.

We note that there is no separate section of the Discussion Paper dealing with Location Dependent Carriage Services (LDCS) as one of the categories of non-critical users (although it comes up as an issue in our responses to Qs 7 and 29). The use of IPND information for the purposes of LDCS was the subject of a consultation by the Department (then DOCITA) in 2007, to which APF made a submission[6]. Amendments to the TA relating to LDCS were made in 2009 without further consultation, and we commented on this in May 2009, in the wider context of the failure of the Communications Alliance Code processes. We are surprised and disappointed that the current Discussion Paper does not at least briefly revisit and explain the history of the use of IPND information for LDCS.

Interaction between the Privacy Act and Part 13 (of the Telecommunications Act) (DP 2.4.1)

DP Questions:

16. Should meeting the tests in the Privacy Act be considered insufficient to allow disclosure of IPND information under Part 13? How should the disclosure regime for IPND information differ to the regime in the Privacy Act?

The issue raised by the ALRC needs to be addressed, to avoid any suggestion that the Privacy Act use and disclosure principles provide an alternative to the stricter controls in the Telecommunications Act. We

[6] See http://www.privacy.org.au/Papers/DCITA-re-IPND-LDCS-0708.pdf

also repeat our submission to the ALRC that sections 280(1)(b) and s297 of the TA should be amended to read '***specifically*** authorised' (this is in line with our general position on the use and disclosure principles in the Privacy Act).

It has always been our understanding of the interaction that NPP 2 (and IPPs 10 & 11 for agencies) continue to apply but that the provisions of Part 13 provide more specific rules about permissible uses and disclosures. Unfortunately this does not appear to be widely understood and **we submit that ACMA and OAIC could do more to explain the relationship between the TA and PA requirements, firstly to CSPs, but then also to the public** (see ALRC Recommendation 73-10).

Access by subscribers (DP 2.4.2)

DP Question:

17. What are the advantages/disadvantages of allowing subscribers to see and correct the IPND information that relates to their services? What checks would be required to ensure that information was not accessed or altered inappropriately or fraudulently?

Subscribers should be able to apply to the IPND Manager for direct access to the IPND entries relating to themselves. This is not only a fundamental right under the Privacy Act, but is important to as a check on the quality and integrity of the IPND data, and therefore in the interests of all IPND users. There is significant potential for the IPND record to be different from the data supplied by a provider, through technical or human error, so it is not sufficient for subscribers to have access to the input data from providers. **The obstacle created by subscribers not being authorised users in the IPND scheme should be removed.**

Direct access will of course mean that the IPND Manager has to take appropriate steps to verify the identity of applicants, but this is the same obligation faced by all other organisations subject to the Privacy Act access principles, and plenty of guidance from the Office of the Australian Information Commissioner and elsewhere, about appropriate steps.

In relation to correction rights, it is important for the integrity of the scheme that the IPND Manager does not make changes without reference to the source data provider, but there are two alternative mechanisms. The IPND Manager could be required to notify subscribers seeking correction of the identity of the source provider, and functional contact details (changes made as a result would then flow through to the IPND in regular updates) Alternatively, the IPND Manager could be made responsible for resolving correction requests with the source data provider, relieving the applicant from having to deal with two bodies.

There are clear parallels between the IPND Data Provider/Manager relationship and that between credit providers and credit reporting agencies in the credit reporting scheme regulated by the Privacy Act. The government has proposed amendments to this scheme which have recently been examined by a Parliamentary Committee. They include revised rules about cooperation in the handling of access and

correction requests. **We submit that DBCDE should liaise with the Information Policy Branch of the Attorney-General's Department with a view to adopting similar rules for access and correction to IPND data to those which apply to credit reporting information.**

Opting out of IPND Services (DP 2.4.3)

DP Question:

18. Should subscribers be able to opt-out of having their IPND information accessed by non-critical IPND users on a category by category basis? Why?

We have already addressed this question in the context of several previous questions, where it is relevant to the resolution of other issues. See for instance Q.5 re Do Not Call Register; Q.6 re location data for LDCS, and Qs 13-15 re research.

We submit that the default principle should be that subscribers can opt-out of having their information accessed by non-critical data users wherever practicable, and unless there is a clearly demonstrated and justified reason why it is not appropriate.

Enforcement of access restrictions (DP 2.4.4)

DP Questions:

19. What measures would enhance the enforcement of IPND obligations?

20. Should civil penalties, as well as criminal ones, apply where IPND information has been disclosed in breach of the rules? Why?

More regular and comprehensive audits of IPND data are desirable, and should include verification of accuracy and currency of data, not simply by comparing addresses to a database, but by contacting a sample of consumers (see the last paragraph of our response to Qs 13-15 above, concerning removal of obstacles to such use).

Unauthorised disclosure of IPND information could have considerable impact on those individuals whose privacy would be breached and should be considered a significant interference with privacy, Sanctions and penalties should reflect this. The government has announced its intention to amend the Privacy Act enforcement provisions, and these will hopefully be introduced in 2012. They will however focus on civil penalties. **For serious and intentional breaches of IPND provisions in the Telecommunications Act, criminal penalties are appropriate and should remain, but ACMA should also be able to impose civil penalties for lesser breaches and this should be an option under the TA**.

Needs of IPND Users (DP 3.1)

DP Questions:

21. The above qualities appear crucial for the IPND to meet the requirements of IPND users. What other characteristics are important? Are any of the IPND attributes listed above not important? Why/why not?

22. Is a regulated database, like the IPND, required to meet the needs of IPND users? Are all of the needs of IPND users legitimate? Why/why not?

It is essential that the IPND be strictly regulated given that it represents a 'statutorily licenced breach' of normal privacy principles (as explained in our Introduction) and because it contains centralised information about most Australians which can be highly sensitive in certain contexts. The need for strict regulation is compounded by the fact that the Australian IPND, in contrast to equivalents in other comparable jurisdictions, is used for multiple purposes.

New services (DP 3.2.1)

DP Questions:

23. What technology and identifiers should be in the IPND? In the future, on what basis should new technologies or identifiers be included in the IPND?

24. How can the flexibility of the IPND be maximised to account for future market and technology changes?

These are questions best answered by others, but APF will have a strong interest in their answers, as they may well have significant privacy implications.

Location Information (DP 3.2.2)

DP Question:

25. What role should the IPND have in delivering dynamic location information to IPND users? How could dynamic VoIP location information be delivered?

We submit that dynamic location information should not be incorporated in or directly linked to the IPND. This would radically change the character of the scheme and would be technically highly complex. Direct association between static IPND information and dynamic location information would make the combined data even more attractive to secondary non-critical users, and would make it even more difficult to resist function creep that could lead to further privacy intrusion.

We submit that critical users, who already have an interest in dynamic location information as well as static IPND information, should make arrangements either in-house or between like users which can be appropriately tailored to their specific needs, and with appropriate privacy safeguards.

There are many privacy issues raised by the use of mobile phone location information, which have been canvassed in past inquiries[7], some of which remain outstanding and unresolved. These include, crucially, the ability for end users to disable tracking (whether through GPS or via base stations/nodes), and the ease with which they can do so, selectively, as they may wish to enable tracking for some services. These issues are not directly relevant to the IPND in its current form but would be important issues for discussion if there was any move towards linking IPND data with dynamic location information.

Governance & Management (DP 3.3)

DP Questions:

26. What are the advantages/disadvantages of the current management structure of the IPND?

27. Should Telstra continue in its role as IPND Manager? What alternatives are there?

We believe there is a fundamental conflict of interest in Telstra, as the dominant CSP and a major Public Number Directory Publisher, also being the IPND Manager.

We submit that the IPND should be operated by an independent entity, preferably by or on behalf of a public sector agency that is subject to the full range of accountability mechanisms. The objectives of the IPND scheme are primarily public interest ones related to its critical uses (law enforcement, national security and emergency services, and it would be inappropriate for this monopoly public resource to be provided as a commercial service or otherwise be subject to market forces (other than competitive tendering for the contract).

Economic costs of the IPND (DP 3.2.3 – incorrect numbering – should be 3.3.1?)

DP Question:

28. How can access costs be lowered in the long term? What are the compliance costs for data providers, and how can these costs be minimised in the long term?

This is a question best answered by others, but APF will have a strong interest in their answers, as they may well have significant privacy implications.

[7] E.g. 2009 ACMA Consultation on proposed amendments to the Telecommunications (Emergency Call Service) Determination – APF submission at http://www.privacy.org.au/Papers/ACMA-ECSDetermn-090927.pdf ; and 2004 ACA Discussion Paper *Location Location Location*: The future use of location information to enhance the handling of emergency mobile phone calls – APF submission at http://www.privacy.org.au/Papers/ACAMobileLocn0404.doc

Competitors (DP 4.1)

DP Question:

29. Do all IPND users require a regulated database provided by the telecommunications industry, or could they seek subscriber information from private data collectors or through other databases? Why?

We submit that some if not all of the non-critical uses could be serviced without access to the IPND – as they presumably are in the jurisdictions shown in Table 3 that only allow a single purpose for their equivalent databases.

There may be a case for public number directory products to be sourced from the IPND in the interests of data quality, and for *some* LDCS services to have access in the interests of consumers receiving more efficient and targeted services including from government agencies.

We submit that serious consideration be given to amending the IPND scheme to remove access to some non-critical users, subject to an appropriate transition period to allow for the establishment of alternatives.

Overseas solutions (DP 4.2)

DP Questions:

30. Are there features of database used overseas that Australia should adopt?

31. Compared to other countries in the table above, Australia is the only country to use its database for a wide variety of purposes. What are the advantages/disadvantages of this? Should the IPND be separated into different databases, each database serving a single, specific purpose?

We submit that the apparent uniqueness of Australia's multi-purpose IPND scheme is a good reason to review the appropriateness of this arrangement, given the significant privacy 'downside'.

We submit that serious consideration be given to narrowing the IPND scheme to provide only for the critical uses, perhaps with the addition of public number directory products and some LDCS uses.

For further information please contact:

Nigel Waters, Board Member
Australian Privacy Foundation
board5@privacy.org.au Tel: 0407 230342
APF Web site: http://www.privacy.org.au

Please note that APF's preferred mode of communication is by email, which should be answered without undue delay. APF does not have an organisational postal address. If postal communication is necessary, please contact the person named above to arrange for a postal address.