

Review of the Integrated Public Number Database

APCO Australasia Response to Discussion Questions

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

Response: The IPND should reside within the National Address Management Framework (NAMF) which is a national, coordinated approach to address management using a consistent, *standards-based framework*, which will guide the process for verifying addresses and provide a standard for the exchange of address data.

The Ministerial Online and Communications Council (a Ministerial Council of the Council of Australian Governments) (COAG) endorsed the NAMF at its meeting on 12 December 2008 meaning that the NAMF will be implemented by the Australian Government and all states and territories).

Relevant Standards are AS4590 – 2006 relating to the exchange of address information and the newly released AS4819 establishing the manner in which “addressing” should be performed.

The NAMF will reference a number of data sets to form a single authoritative data source used to validate the accuracy of addresses and form the single “point of truth” for users of a NAMF-compliant framework. The IPND should be one of these datasets as the ultimate aim of the NAMF is to provide a unique address where “*one address equals one location*” (1).

In addition to a Standards based approach the development of consistent addressing policies by States and Territories such as that adopted by the Western Australian Government would also be of assistance.

(1) <http://www.anzlic.org.au/get/2469841188.pdf>

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

Response: See the response to Question 1. In addition to compliance with the requirements of the NAMF consideration could be given to the use of the National Editing Service (NES) application developed by the Victorian Spatial Council and adopted by the Public Sector Mapping Agency (PSMA) to allow the checking and validation of information in the IPND by authorised users of the application based upon the lessons learnt about its use to date.

The PSMA has also developed a validation/compliance assessment process location based service providers to the public/private sectors against which their respective databases can be tested to achieve the issue of an NAMF Compliance Certificate.

The allocation of funding to provide both the resourcing and technologies required to improve addressing accuracy, particularly within the Local Government sector, is a barrier to improving the accuracy of addressing generally and in turn relates to the future accuracy and hence validity of the IPND as an “authoritative database’ for Critical Users.

The “roll out” of the National Broadband Network also provides a once in a generation opportunity to validate data held in the IPND.

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

Response: As indicated in the Discussion Paper “Commentators have noted that the disclosure regime for the IPND can be confusing and potentially contradictory” which goes to the question of what is the purpose of the IPND now as compared to when it was originally created and can the IPND in its current form meet the needs of its Users (Critical and Non Critical) as defined within the Discussion Paper. The answer to this question and the response to Question 4 will inform the changes required to the disclosure regime.

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

Response: The importance of location, real time information and the management of information spatially brings the IPND under greater scrutiny because of the commercial value social media has associated with the provision of location based services to meet market needs. The point has been reached, as recognised through the release of the IPND Discussion Paper, where an assessment of the ability of the IPND to meet the needs of both critical and non critical users will need to be made.

The future needs of the Critical Users over the next 5 years (estimate) will change significantly with the introduction of Next Generation 000 in conjunction with the NBN and wireless technologies such as 4G – LTE to meet public expectations of service from public safety agencies.

The Critical Users need to consider their future needs from the IPND which will inform the changes required to the regulatory, privacy and disclosure regimes to produce the level of integration required in the simplest format consistent with the importance of the role being performed by the IPND.

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

Response: New Critical Users should automatically have the same level of access to IPND data available to other Critical Users. However it would seem to be important that new Critical Users specify their data requirements and the proposed use of the data for the purpose of sharing with other Critical Users. This would provide the opportunity to identify if the new Critical User’s data and proposed use is of interest to other Critical Users. Access to new Non Critical Users would be a matter for assessment by the IPND Manager in terms of the impact on the IPND. However the establishment of principles of equity of access for commercial, not for profit and research organisations that are transparent and contestable in their manner of application by the IPND Manager would be useful to applicants, the IPND Manager and the public.

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

Response: Critical Users should be able to access those data elements relevant to the legislation by which they are established and give the power to function as bodies.

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

Response: See response to Question No 6.

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

Response: The key issues identified in the IPND Discussion Paper are the “public interest” test, the link to privacy and the ability to investigate breaches of the arrangements under which access to the IPND and its data is provided. Consideration of the Objectives of the IPND in a hierarchical sense i.e. the overarching IPND Objectives and then those specific Objectives of the Critical Users and the Non Critical Users would provide guidance as to how an integrated set of Objectives could be created linked to the public safety and location services markets.

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

Response: See the response to Question No 8. The setting of an integrated set of Objectives matched to Market needs met by accessing the IPND and IPND data through a set of Principles defining access and security would inform any additional conditions to be applied.

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

Response: The current level of access to the IPND and use of IPND data by the commercial sector would be a measure of the value placed by the sector on both the access and the data provided through this access i.e. the level of “value add” to the products and services generated by the commercial sector from the use of the access and the data. This value would also provide an indication of the “barrier” to market entry if this access was restrictive or not available. Regulatory changes to the IPND relating to improving access and the quality and accuracy of the data elements linked to location within the IPND would have a flow through “value add” to both the access and the data obtained through this access. This improved value should encourage innovation and competition in the location based services market.

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

Response: The use of the IPND is a commercial decision for the publishers of directory products and will be driven by the acceptance of their products by the market. However organizations or individuals using the IPND to provide a product or service need to be confident that they are working with accurate address data and it should be expected that these organizations and individuals would undertake their own risk assessment of the use of the IPND versus other databases.

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?

Response: Where information used to produce directory products is sourced in whole or part from Government databases the users of the directory products should expect that the information will be to a consistent level of quality and accuracy produced through use of appropriate and consistent regulatory regimes and principles.

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

Response: Access to the IPND and IPND data for research purposes should be subject to the “public interest” test defined within a regulatory regime and assessed against agreed principles. As stated in response to Question No 10 the current level of access to the IPND and use of IPND data by the research sector would be a measure of both the value of this access and the data provided through

this access i.e. the level of “value add” to the research outputs produced the research sector from the use of the access and the data. The assessment of applications on a project by project basis is supported.

The important issue that the IPND Discussion Paper highlights is that “*There are no high-level principles which guide policymakers in either allowing or denying access to the IPND for research purposes.....*” and there should be.

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

Response: High level principles governing the addition or removal of permitted categories of research should address both the public interest test and also the outcomes from research in the context of being a “public good”.

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?

Response: Refer to the response to Question 14 and also previous responses relating to the need for a regulatory regime based on a hierarchy of IPND Objectives and Principles determining access.

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?

Response: No response is provided to this Question as it requires specialist knowledge of privacy legislation

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?

Response: See response to Question 2 and the reference to the potential use of the NES application

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

Response: This is a very broad question and relates as much to the contemporary definition of “privacy” and the purpose and outcomes from the application of data accessed through the IPND. In regard to access to IPND data by Critical Users there should not be an “opt out” option to the provision of data that will be used to protect the lives and property of Australians.

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

Response: See the response to Question No 20. In addition publication of the identities of organisations not complying with IPND obligations could be considered in a manner similar to that used by the Federal Communications Commission in the United States to highlight the use of 911 funding for other than 911 purposes.

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

Response: If the disclosure of IPND data jeopardised the ability of Critical Users to protect the lives and property of Australians then penalties should be able to be imposed commensurate with the impact of the disclosure on the Critical Users.

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?

Response: Table 2 represents the needs of to-day's IPND Critical Users but needs to take into consideration the future needs of Critical Users and the information that will be available for presentation to the Emergency Call Persons e.g. smart sensors will utilise smart grids to deliver information about the location from which the request for access to public safety agencies originated together with information from database matching delivered to the ECP to establish Situational Awareness.

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?

Response: See the response to Question No 23.

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?

Response: A detailed analysis of the changes that will take place in the Next Generation 000 element of the public safety communications environment needs to be undertaken to determine the place the IPND will take in this environment. This analysis may already have been undertaken, is being undertaken, or is being planned with the responses to the IPND Discussion Paper being used as inputs.

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

Response: See the response to Question No 23

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

Response: Identifying the location of calls from mobile phone users seeking access to public safety agencies through nominated emergency call services is a common challenge facing the global public safety communications sector. The rapid uptake of GPS enabled smart phones and other mobile devices will contribute to solving this problem however it needs to be considered in the much broader question of how will the public expect to access the emergency call services in the future using their preferred means of communications e.g. social media, text, voice etc.

Globally countries are preparing for "Next Generation" access to public safety services e.g. NG 911 in the USA, therefore the decision needs to be made as to whether the IPND is to be a static or dynamic database in regard to holding information relating to the location of users of mobile phones or whether this information is provided to the emergency call services by other means.

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

Response: See the response to Questions 23 and 27. Telstra has considerable experience performing the roles of the IPND Manager and the ECP which will be valuable in maintaining both services during the period of change that is expected in the way the 000 service will be accessed and provided with the progressive introduction of new technologies and increasing public expectations of the service. The end result of the suggested needs analysis and system design would then allow the provision of both services to go to competitive tender. However the future IPND or its replacement may be considered to be too important a database or combination of databases to be operated by the private sector. This is the position of the public safety agencies in respect to suggestions that private sector wireless broadband networks can provide the additional capacity to carry public safety data during major events. On the other hand the NBN in conjunction with new technologies may provide the opportunity to consider new methods of delivery of the 000 service on a regional basis.

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

Response: See the response to Question No 26. Telstra has been the IPND Manager since it was first established in 1998 and also performs the role of the Emergency Call Person (ECP) for the 000 service. In both respects Telstra is a significant party in the public safety communications environment. Whilst the Telecommunications Universal Service Management Agency (TUSMA) legislation says the role of the ECP will be put to tender within the next 5 years Telstra will continue to be paid to perform the role of the ECP until such time that these arrangements are changed.

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?

Response: Given the significant changes expected to occur in respect to the IPND's Critical Users as a result of the introduction of New Generation public safety communications technologies and Non Critical Users through technology evolution, convergence and social media it is suggested that a new financial model will need to be developed for the IPND which could address the matters raised.

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?

Response: See responses to Questions Nos 10, 11 and 12. The use by IPND Users of information from private data collectors or through other databases is a commercial decision for both Critical and Non Critical Users who would be expected to undertake their own assessment of the sources of this information and any associated risks. The need to use this data would be driven by the inability of the IPND to provide the data required by the User even though the Critical Users should expect to benefit from the ability to access a regulated database.

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

Response: This question should be the subject of research into why other countries have chosen to create single rather than multi use data bases and which method is better placed to cater for new technologies and the changing needs of the IPND Users.

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?

Response: See the response to Question No 30.

Submitted: 16 November 2011

**Contact: Geoff Spring
Chairman APCO Australasia**

Mob: 0411 130 184
E mail: geoff.spring@apcoaust.com.au