COMMUNICATIONS ALLIANCE LTD

DEPARTMENT OF BROADBAND, COMMUNICATIONS AND THE DIGITAL ECONOMY (DBCDE)

DISCUSSION PAPER ON THE INTEGRATED PUBLIC NUMBER DATABASE REVIEW

COMMUNICATIONS ALLIANCE SUBMISSION JANUARY 2012

TABLE OF CONTENTS

INTRODUCTION

Communications Alliance is pleased to have the opportunity to provide this submission in response to the Department of Broadband, Communications and the Digital Economy's review of the Integrated Public Number Database (IPND).

Since its implementation in 1997, the IPND has been an effective mechanism in meeting the public policy objectives underpinning its establishment. Since that time, the objectives of the IPND have been augmented, as the use of the IPND as an information source has been expanded for a range of approved purposes.

Industry has established and updated systems and processes that ensure the IPND operates effectively, that the privacy of information is protected and that both data providers' and an expanded number of data users' needs are accommodated. Industry does not have any significant concerns about the costs to data providers and data users of accessing the IPND since the most recent cost structure was introduced in 2007/08.

Since 1997, the technology mix over which services are offered has changed. There is now a much higher penetration of mobile services and a significantly increased number of data and internet based applications. The prevalence of mobile and VoIP services means that the location of a customer is now much more variable and, as a consequence, the reliability of IPND-based address information as an indicator of customer location may be reduced. The deployment of the NBN over the next 8 to 10 years will bring further changes to the way people communicate and where services are located.

Given these changes and the degree of both regulatory and operational developments in the industry at present, Communications Alliance believes that stability in the current IPND arrangements is important. The industry agrees that the IPND will continue to be essential in its current form in the short- to medium-term, but considers it appropriate to review the changes required to fulfil IPND users' needs in the longer-term. It believes that this longer-term review must give weight to the following principles:

- any future IPND data sourced from carriage service providers (CSPs) should only extend to the information CSPs would be expected to obtain as part of their normal business for the purpose of provisioning carriage services;
- any future IPND model must be capable of being fully integrated with existing industry upstream and downstream processing arrangements, including the effective delivery of Triple Zero call handling and referral to emergency service organisations (ESOs); and
- customers' privacy needs to be protected and high levels of security need to be ensured with regard to the management of the database and securing the transfer of records to approved data users (including ensuring high levels of reliability and data quality standards). Such processes should be auditable and data quality standards need to be enforceable.

About Communications Alliance

Communications Alliance is the primary telecommunications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to provide a unified voice for the telecommunications industry and to lead it into the next generation of converging networks, technologies and services. The prime mission of Communications Alliance is to promote the growth of the Australian communications industry and the protection of consumer interests by fostering the highest standards of business ethics and behaviour through industry self governance. For more details about Communications Alliance, see http://www.commsalliance.com.au.

1. Use of IPND data by directory producers

Communications Alliance notes that access to the IPND remains a useful way to enable publishers to produce public number directories, especially if concerns about accuracy can be addressed (for example, using the mechanisms described in section 4). Directory publishers should also continue to have the option of choosing to negotiate and establish direct data supply arrangements with carriers, CSPs or other data sources. The industry notes this remains a viable option, with most new competitors and entrants in the market utilising other data sources (in addition to or instead of the IPND) to develop their databases of information.

2. Issues in the quality of information in the IPND

Communications Alliance notes from the Discussion Paper that the quality of IPND data is being questioned by data users accessing the IPND.

2.1 Alternate Address Flag (AAF)

It is important that the AAF in the IPND for customers is applied consistently and its use fully understood by the Emergency Call Person (ECP) and ESOs. For example, for fixed lines and mobiles the AAF default setting is a "false" status, whereas for IP based services, the setting should be set to "true" only if the service has a nomadic capability. Users of IPND data must be aware of whether or not IPND address data is a reliable indicator of the location of the user of the telecommunications service where the service is mobile or has a nomadic capability.

The rollout of the NBN and the growing numbers of IP based services increases the potential for issues related to mobility and the relevance of fixed data in the IPND. Accordingly, with the roll out of the NBN, there needs to also be some analysis undertaken on the potential for customers to use their NBN-based voice service in a geographic phone location other than at the recorded service address in the IPND.

It is important that data providers follow existing guidelines (Communications Alliance IPND Data Industry Guideline G619:2007) to ensure the accuracy of data supplied. Data providers are able to implement address validation software before sending address data to the IPND. Data providers' adherence to the guidelines, for example, consistent correct flagging of the AAF, supports established Triple Zero call handling process and enables the best use of IPND data as it is today. The relevant section of the guideline reads as follows:

> ***Alternate Address***
> *IPND field 17 is a mandatory field used to assist in identifying the physical location of the Customer and assists Emergency Service Organisations in their communications with the caller.*
>
> *The flag is set to* ***True*** *where the Service Address provided may not be the physical location where the service originates, and therefore the Customer calling from this geographic number may not be at the physical address derived from the IPND. Typically, this can apply to calls made from a Local Service connected to a PABX, when using nomadic services such as VoIP, or when calling from geographic numbers used to relay emergency calls.*

*The flag is set to **False** where the Service Address provided is the physical location where the service originates or when the Public Number is a Mobile Service Number.*

NOTE: Data Providers cannot be held responsible for the ongoing reliability of the information provided to the IPND Manager where Customers take action that is beyond the ability of the CSP to identify or control.

2.2 Enhancements

A number of initiatives to enhance location information for emergency services and emergency warnings are being taken by the industry:

- Deployment of emergency services is based on the customer's service address listed in the IPND or their actual location if the AAF indicates that the customer should be asked. The AAF ensures that Triple Zero and ESOs are aware that a service may not be located at the address listed in the IPND. This prompts emergency call person for Triple Zero to verify the location with a caller before referring that call to the required ESO.
- The industry is currently developing systems and processes designed to improve the ability to locate customers in an emergency situation. For emergency calls from mobile services, CSPs are now required to provide ESOs with the most precise mobile location available for the customer where the ESO is unable to obtain that information from the caller. These arrangements currently apply on an "as required" basis. Further work is now being undertaken by industry to deliver such location information on all calls made to Triple Zero from a mobile device.
- In terms of provision of emergency alerts, the industry is also developing a capability to identify mobile devices in use within a defined "emergency" area. These changes will address potential problems associated with reliance on mobile customer based addresses within the IPND for providing emergency alerts to mobile customers.

The mobile industry is also undertaking a separate set of activities aimed at verifying customer details for prepaid mobile services at activation for law enforcement purposes. This process will still be subject to ID fraud, ID theft, transfer of services between users post activation and any customer change of address not notified to the mobile service provider. Current and planned identity validation of prepaid mobile customers does not validate the association of the customer to the service address supplied by them.

While less critical, IPND data quality issues also impact on use of the IPND for non-critical purposes, eg, research and political polling.

Industry acknowledges that the Australian Communications and Media Authority (ACMA) also undertakes periodic audits of IPND address data. However, those audits only validate an address *per se* (i.e. confirm that it is a valid address) but do not confirm whether the customer has any association with the address listed in the IPND, or the customer's address at the time that an inquiry is made of the IPND to identify the customer's address.

Communications Alliance notes that the overall accuracy of the IPND information relies upon customer supplied information and customer advice to update their CSP should details such as the service user or the service address change.

In any event, the solutions outlined here do not provide an overall solution, and Communications Alliance considers that consideration could be given to how the accuracy of information in the IPND can be improved. This should include, for example, efforts by the

ACMA to educate customers about the importance of providing accurate and up-to-date address information to their CSPs.

3. Future approaches to data collection

3.1 Social media contact information

The IPND was developed at a time when customers relied upon fixed line services. New social media such as Facebook, Twitter and Skype, other methods of communication are becoming common. In particular, Communications Alliance notes that there is increasing potential for requests to ESOs to come from these social media sources and it may be relevant for the ESOs to consider their future methods for accessibility – which may include a direct feed between the individual seeking an emergency service and the ESO. As an example of the trend towards social media, in September 2009, two girls were trapped in a drain and used Facebook to make contact with friends who then called Triple Zero on the girls' behalf, leading to assistance from ESOs.[1]

The trend towards use of social media offers opportunities for ESOs to broaden their means of being contacted, but industry questions whether this trend suggests social media contact details should be included in the IPND. ESOs may be able to interact usefully with several information sources. The IPND in its current form appears to be narrow and limited in this context. A more future oriented approach points to the ESO establishing links in the cloud, and with the potential use of social media platforms as a means of calling for help as well as a means of obtaining additional information for ESOs.

If alternative sources of data are to be considered for inclusion in the IPND, these are likely to have significant implications for industry by way of data access, sourcing and extraction as well as an array of consumer privacy issues. A fundamental concern is that this would mean a move away from the current model whereby CSPs provide to the IPND only the type of information they would obtain as part of their normal business of provisioning carriage services. Industry believes that any extension of existing data sources would create a tension with the National Privacy Principles[2] and would impose an unnecessary burden on CSPs. Industry also believes it would be contrary to customers' expectations, and that an initial and threshold issue for consideration would be the extent to which customers would be comfortable to provide social media contact details to their CSP. It will be equally important to consider, as a threshold issue in any review, the reliability of such source data and its usefulness for IPND users.

Industry believes that the future model for the ESO involves a direct interface to the various social networks. This interface could be independent of CSPs, and does not require CSP involvement, as they do not collect customers' social network login details.

It is timely to note the emerging mobile location sourcing work being undertaken by the US Federal Communications Commission (FCC) in reviewing 911 requirements. The Enhanced (E911) sets out requirements for GPS enabled mobile handsets which are meant to facilitate 911 call tracking and enhance 911 call centres' ability to use text messages, photo data and improve the response to emergency events.

All of these issues would need to be worked through to establish whether there are cost effective ways of using such information in an IPND, equivalent type database or through direct feed from the customers' equipment. However, the industry's view is that these

[1] ABC News, "Trapped girls call for help on Facebook" (available at http://www.abc.net.au/news/2009-09-07/trapped-girls-call-for-help-on-facebook/1420352 at 4 January 2012).

[2] National Privacy Principle 1.1 provides that "An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities."

reviews should not distract from the need for the ACMA to educate customers about the importance of providing accurate up-to-date information to their CSPs so they can be contacted and located in an emergency situation. Similarly, all CSPs have an important role to play in ensuring their customers provide the required information and understand its significance.

3.2 IP addresses/location information

With the advent of the roll out of the NBN, IP address information may become more useful to locate customers of data and VoIP services. However, there would need to be more analysis about how useful this information would be and its reliability. In this respect, it needs to be recognised that there are limits to how useful IP addresses can be in providing location information: for example, increasing use of Wi-Fi and Femtocells for making calls means that CSPs cannot always provide accurate caller location information.

If the information is seen as useful, industry believes there would also need to be further analysis about whether this information needs to be captured in the IPND and access to that information made available to other IPND users. Industry notes that some IPND users (ie law enforcement agencies) have other mechanisms available to obtain this information, although it is recognised that there may be benefits to those IPND users in reviewing those arrangements.

3.3 Customer provision of information

Currently, CSPs send public number customer data to the IPND. In considering future models, the Discussion Paper seeks comments on the benefits of customers providing such data directly. Adoption of the former approach would involve a fundamental change in the way the IPND model currently applies and gives rise to a range of issues for consideration, including:

- the construct of the IPND and existing data sources;
- associated IT capability requirements and the need for new IT capability to be developed (including how these costs would be allocated);
- reliability of data where customers fail to update or provide correct data (eg whether the information would need to be cross-checked against other databases);
- security standards to mitigate against inappropriate access to, and changes being made to, data;
- whether such data is appropriate for use in critical emergency and law enforcement situations (including noting the possibility of information being made deliberately inaccurate so it is not useful for law enforcement purposes);
- reconciliation of data records to testing of data accuracy;
- whether CSP involvement in the model remains relevant or necessary;
- privacy and security arrangements and who bears responsibility where data is incorrect or inaccurate; and
- what processes would apply where customer data is corrupted.

The development and growing applications of new technologies illustrate the increasing ability of customer devices to provide information about the customer's location. For example, in-built communication devices are now being rolled out in vehicles in Europe; consideration should be given to whether agencies including ESOs and law enforcement authorities should be able to access and use such information. However, industry notes that such information could be provided directly to ESOs and would not necessarily be appropriate to include in the IPND. There are likely to be serious privacy considerations that

would need to be addressed, especially if the information is provided by CSPs without customers specifically requesting that it be provided. For this reason, industry suggests any such information should be provided to ESOs directly from customers. While CSPs provide location information to ESOs through the MoLI system, provision of such information to ESOs should not evolve to encompass the ongoing collection and monitoring of location information by CSPs – especially since this is not the type of information CSPs would otherwise collect in the ordinary course of their business. Nor should CSPs or the IPND Manager be required to provide individual notifications to customers when their records are updated. Given the sheer volume of records added or modified each year, industry believes a requirement to individually notify customers of changes would be impractical and would significantly raise the costs to IPND users.

Mobile smartphones and some models of satellite mobile phone have inbuilt GPS capability. This GPS information may be far more accurate than any mobile network derived information. There is limited use planned for deaf user access to the National Relay Service (NRS) for emergency calls. Such a system indicates the potential benefits for the broader population if mobile handsets can forward location information on emergency calls (see below for more details).

4. Future approaches to the ECP and ESO model

Consideration needs to be given to whether the ECP and ESO model should operate the same way in future.

The recently developed smartphone application for iPhones and Android devices for use by people with speech and hearing impairments is an example of a potential future model that could reduce reliance on IPND data. This application creates a data session to the NRS which relays the information directly to the ESO. The application also initiates the GPS in the device and forwards the location information to the NRS. The device can also be polled to obtain additional GPS fixes and to better identify the location of the customer, although its utility does remain subject to the customer providing and maintaining up-to-date personal information. Where such data is available, it reduces reliance on IPND data by ESOs. By the end of 2012, smartphone penetration is expected to be at approximately 90%, meaning that such applications could become much more widespread. However, there are a range of technical and policy issues that would need to be considered, including handset capabilities and whether manual activation of GPS by customers is necessary and the privacy consequences of such an approach.

Industry proposes that consideration should be given as to how these types of smartphone applications could be applied to the broader community. Whilst recognising that there will always be segments within society who will not use or have access to such devices and that IPND data would continue to be relevant for fixed-line services, these applications provide scope for a better service to the community in speed of delivery of accurate caller location information. Where a genuine emergency call/contact is received, pre-loaded data might be able to be presented to an ESO where a customer is able to place the call but unable to converse due to factors such as fumes/smoke, or where speech would put them into greater danger.

5. Technical Feed

The current technical feed to and from the IPND is via dedicated links with encryption boxes. These requirements have been put in place to ensure that there are adequate levels of security applying to the transfer and retrieval of large amounts of sensitive customer information and because they are tested and reliable — for example, the security offered by these dedicated links has ensured there have been no breaches of privacy related to the

IPND since it was established in 1997. These arrangements have been effective in protecting the privacy of customer information and ensuring organisations sourcing data are approved to do so.

Communications Alliance recognises that there may be other options (including those associated with IP networks) that have the potential to improve access and reduce costs. However, these would need to be guaranteed to deliver the same standards of security and required service levels, and could require significant changes to existing IT systems and processes for all data providers and users of the IPND.

Communications Alliance recommends a fully funded and detailed analysis be undertaken to assess the viability and cost effectiveness of such options.

6. IPND Manager

Communications Alliance notes that any changes to the current IPND Manager arrangements would give rise to a range of issues that would need to be carefully considered, including:

- which alternative entities would be suitable and willing to take on the responsibility;
- how the risks associated with changes in the existing arrangements could be effectively managed;
- the capability requirements and whether any new IT capability would need to be developed by the alternative entity (and if new capabilities are required, how the cost would be managed);
- how an alternative entity would be selected;
- how the costs to the industry and IPND users of adapting to the new arrangements would be funded; and
- how IPND users and industry would be expected to transition to any new operational arrangements.

Communications Alliance notes that the industry is undergoing significant changes at present – both operational (given the rollout of the NBN and next-generation wireless services) and regulatory – and that the appropriate timing for any changes to the management of the IPND would need to be carefully considered.

In the meantime, the industry notes that there may be more immediate options to improve the management of the IPND. For example, certain access seekers must seek approval to use the IPND from the ACMA, whereas others may directly approach the IPND Manager. The industry considers that a more effective solution would be for all access seekers to be approved by the ACMA on the basis that this would create a clearer separation between, on the one hand, granting access (which is best performed by an independent regulator) and, on the other, the operational aspects (which could continue to be managed by industry).

In terms of prices, industry believes that if the current arrangements are to continue, it is appropriate that the IPND Manager be permitted to continue to obtain a reasonable return on investment. If significant updates to the IPND are proposed, consideration would need to be given to how these could be funded.

7. Do Not Call Register (DNCR)

Further consideration should be given to whether an additional use of IPND data might be to maintain the currency of the DNCR. This would allow for numbers that have either been

disconnected or which no longer belong to the person to which they were allocated (at time of DNCR registration) to be removed from the DNCR.

The industry believes this would help address concerns that the DNCR is becoming inaccurate and out-of-date, since it is not automatically updated to reflect changes to customers' details and contact numbers. Over time, these concerns are likely to lead to the DNCR becoming less accurate, effective and useful – and increasingly unrepresentative of customers' preferences. The IPND offers one solution to address this problem.

8. Location Dependent Carriage Services (LDCS)

Communications Alliance strongly believes that access to information about unlisted numbers in the IPND should be extended to CSPs in the short term, to allow customers with unlisted numbers to take advantage of LDCS (for example, by dialling a LDCS number and being connected immediately to the closest branch office). Where the IPND is used to provide LDCS, the customer's location information is only used for call routing (network) purposes – for customers with unlisted numbers, the information is not provided to any other party, including the recipient of the call. Communications Alliance believes such use of IPND information is therefore consistent with the expectations of customers with unlisted numbers who are primarily concerned with the *publication* of their information.

The ability of customers with unlisted numbers to use LDCS is not only convenient for such customers but in many cases has significant public interest implications given that LDCS may be used for important public safety, medical and security services. For example, Federal and State Governments promote the use of '13' numbers for communications with police and the State Emergency Service for some states. To correctly and efficiently route these calls, CSPs need access to the IPND. Communications Alliance queries whether it is acceptable from a public interest point of view for customers with unlisted numbers not to have quick and reliable access to the most relevant point of contact for such critical services.

Given the strong public interest issues and the fact that LDCS may be relied upon in critical situations, industry believes LDCS should be available for all end users and should not be dependent on whether a customer has chosen to permit LDCS. Industry expects this issue to become increasingly important given moves by the ACMA to decrease the geographic significance of fixed-line numbers – which means that the number itself will be of decreasing usefulness in determining the location of the caller.

Communications Alliance understands this suggestion has previously been put to the Government at an industry level but was not pursued due to issues raised by the Privacy Commissioner. The industry believes any privacy concerns are capable of resolution and would be grateful for the opportunity to further discuss this issue.

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 9
32 Walker Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
TTY 61 2 9923 1911
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507