Review of the Integrated Public Number Database

Submission by the Australian Communications Consumer Action Network to the Department of Broadband, Communications and the Digital Economy

December 2011

About ACCAN

The Australian Communications Consumer Action Network (ACCAN) is the peak body that represents all consumers on communications issues including telecommunications, broadband and emerging new services. ACCAN provides a strong unified voice to industry and government as consumers work towards availability, accessibility and affordability of communications services for all Australians.

Consumers need ACCAN to promote better consumer protection outcomes ensuring speedy responses to complaints and issues. ACCAN aims to empower consumers so that they are well informed and can make good choices about products and services. As a peak body, ACCAN will activate its broad and diverse membership base to campaign to get a better deal for all communications consumers.

Contact:
Danielle Fried, Disability Policy Adviser

Suite 402, Level 4
55 Mountain Street
Ultimo NSW, 2007
Email: info@accan.org.au
Phone: (02) 9288 4000
Fax: (02) 9288 4019
TTY: (02) 9281 5322

Introduction

ACCAN appreciates the opportunity to contribute to this review. We have only included answers to questions that we feel well placed to comment on as the peak body representing Australian telecommunications consumers.

ACCAN's main areas of concern in regards to the IPND are:

- Accuracy for the purposes of emergency calls and emergency warnings
- Privacy and freedom of information
- Consumer awareness.

This submission includes the following recommendations to improve the administration of numbering data and emergency location information:

1. The Integrated Public Number Database (IPND) Manager should notify consumers by mail, on IPND letterhead, preferably with an Australian Government crest in order to assure readers of its credibility, within a short period of time (such as one week) when a record is created or altered, in order to confirm that this information is correct. Consumers would need to re-confirm these changes in their details to minimise errors. Consumers who do not respond within a set period of time should be followed up by phone, mail or other means. This process should be reflected in the IPND Industry Code.

2. The ACMA and the IPND Manager should expand the promotion to consumers of the importance of notifying Carriage Service Providers (CSPs) and/or the IPND (see question 17) if their personal details have changed, focusing on the significance this has on access to emergency services.

3. The name of the IPND should be changed to become more consumer-friendly, memorable and descriptive - for example, the National Phone Number Register.

4. Information about the IPND, using its new name, should be printed in large font and in common community languages on all ISP/RSP/phone bills.

5. The ACMA should develop an IPND disclosure regime, including high-level principles and processes, and these should be made public.

6. The ACMA should keep a public register listing IPND users, including researchers.

7. In the case of listed numbers, LDCS providers should have access only to the fields/data they require in order to accurately route a call – that is, the sub-region and State/Territory of the address in the case of geographic numbers (and the sub-region and State/Territory of the device in the case of roaming/mobile/VOIP numbers, should this be incorporated into the IPND - see question 25). This should be the case whether a phone number is 'listed' or 'unlisted' ('silent').

8. In the case of unlisted ('silent') numbers, the ACMA should lead further consultation as to whether ACCAN's Recommendation Seven should be implemented, or whether holders of unlisted numbers should be given an informed choice as to whether they want this data disclosed to LDCS providers.

9. Holders of IPND Scheme authorisations should be required to notify the Office of the Australian Information Commissioner where there has been a substantive data breach resulting in the disclosure of protected information.

10. The ACMA should encourage debate as to whether there is a "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"[1].

11. Directory products published by the same company which manages the IPND (that is, currently, Telstra) should be required to obtain its directory data exclusively from the IPND.

12. Any organisation proposing political research via the IPND Scheme must provide to the ACMA the questions to be asked of consumers, and the ACMA must take these questions, and their objectives, into account when considering authorisation under the IPND Scheme.

13. Access to the IPND should remain subject to project-specific authorisations from the ACMA.

14. 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 is the effect of the test proposed by the ALRC in Recommendation 72-14 of Report 108).

15. 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).

16. Sections 280(1)(b) and s297 of the *Telecommunications Act* should be amended to read "*specifically* authorised..."

17. The ACMA and OAIC should better publicise, both to CSPs and the public, the fact that NPP 2 (and IPPs 10 and 11 for agencies) continue to apply but that the provisions of Part 13 provide more specific rules about permissible uses and disclosures.

18. Consumers must have access to their own complete set of IPND information, preferably direct from the IPND Manager, subject to identity verification.

[1] See submission from the Australian Privacy Foundation, yet to be published

19. Consumers must have the ability to edit their own data, subject to identity verification.

20. Both the consumer's CSP and the IPND Manager must be made aware of any consumer-initiated changes to a consumer's IPND data.

21. Consumers should be allowed to opt out of having their IPND information accessed by non-critical IPND users on a category by category basis.

22. Consumers must not be charged by their CSP should they elect to have an unlisted entry ('silent line') and/or suppressed address.

23. The ACMA must broaden the scope of IPND audits to verify accuracy and currency of data.

24. Both privacy breaches and failure by CSPs to provide current and/or accurate information – or failure by the IPND Manager to record that information – must incur significant penalty, to reflect the seriousness of the infringement.

25. If technically feasible, dynamic location information should be included in the IPND.

26. Dynamic location information for users of relay and satellite services must also be included.

27. The IPND should remain a single database, despite its various purposes.

Response to Discussion Paper 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?***

ACCAN submits that current arrangements work against data being accurate and current.

As we have noted previously[2], consumer information in the IPND can be inaccurate, out of date or incomplete. This places consumers who require emergency services at risk. ACCAN is concerned that the current arrangements for the collection of data create unnecessary confusion and needless difficulties for consumers, whether that is in accessing their own data, or correcting inaccuracies.

ACCAN is aware that the Community and National Interest division of the ACMA commissions a sub-contractor to conduct an audit of the IPND annually, and this includes investigating data accuracy. The latest figures have shown an improvement in accuracy from 89% accuracy in 2006 to 96% in 2009-10[3]. This leaves nearly 4% of numbers with inaccuracies that could prove life-threatening in an emergency situation. Further, this 'accuracy' measurement in fact measures only how well a listed address matches to an actual address, using the Geo-coded National Address File (G-NAF) database; it does not in fact measure whether a customer's information is current and correct. So the real accuracy rate is likely to be significantly less than 96%.

ACCAN believes that most consumers are unlikely to be aware of the IPND, despite the fact that the IPND Industry Code[4] requires that data providers advise their customers about the use and disclosure of a subset of IPND information. In fact, it appears that most consumers believe GPS or a similar system to be in place to allow emergency service organisations to find them[5], at least when they are using their mobile phone.

Consumers are unlikely, then, to be unaware that:

- When they update their information with their CSP, the CSP must arrange to change:
    - Its own internal data
    - IPND information via the IPND Manager (i.e. Telstra)

[2] ACCAN, *Customer location information and numbering data*, March 2011, http://accan.org.au/index.php?option=com_content&view=article&id=274:customer-location-information&catid=146:emergency&Itemid=316
[3] http://www.acma.gov.au/WEB/STANDARD/pc=PC_312218
[4] Australian Communications Industry Forum, 2008, http://www.acma.gov.au/webwr/telcomm/industry_codes/codes/ipnd_code_c555_2008.pdf
[5] The Australian Communications and Media Authority, *Mobile location information: Location assisted response alternatives*, May 2010, p.6, http://www.acma.gov.au/webwr/_assets/main/lib311840/mobile_location_information_location_assisted_response_alternatives.pdf

- Directory information via Sensis (i.e. Telstra)

- They should let their CSP know of any updated details which correspond to an IPND field.

ACCAN notes that the ACMA has already produced information for consumers about the importance of providing current address details to a CSP[6]. This could be promoted more widely.

ACCAN also recommends that the name of the IPND be changed to become more consumer-friendly, memorable and descriptive - for example, the National Phone Number Register – and that information about the database be printed in large font and in common community languages on all ISP/RSP/phone bills, including online bills.

Even if a customer is aware of the existence of the IPND, it is very difficult for a consumer to determine what details are held in the IPND, as they are required to retrieve information through their CSP rather than directly from the IPND Manager. A consumer is unable to contact the IPND Manager directly to request their data, so that the consumer can check it for accuracy. It is unclear what rights to their own data a consumer has, and which organisation is responsible for providing such data to consumers. ACCAN is aware of at least one instance in which a customer has requested their full IPND data using a variety of methods, and was never provided with this complete data set. Further, if a customer suspects that their information is inaccurate, they must contact their CSP and hope that the information is passed on to the IPND Manager – if they are even aware of the IPND.

Under the current regime, upon being advised of updated information from a customer, the CSP must inform the IPND Manager of the changed data, but in practice this does not always occur, or may not occur in a timely fashion. For example, the CSP may provide an update to Sensis but the information might not be directed to the IPND Manager as well. Sensis and the IPND systems do not share information and this has the potential to lead to inaccuracies as details are updated in one system and not the other.

The approach to managing the accuracy of information in the IPND should be improved. An improved system would ensure that all relevant stakeholders, including consumers who need to inform their CSP of any change to their details, or request access to their IPND data in full or part, are clear about their responsibilities in the IPND data chain.

Recommendation One:

- **The Integrated Public Number Database (IPND) Manager should notify consumers by mail, on IPND letterhead, preferably with an Australian Government crest in order to assure readers of its credibility, within a short period of time (such as one week) when a record is created or altered, in order to confirm that this information is correct. Consumers would need to re-confirm these changes in their details to minimise errors. Consumers who do not respond within a set period of time should be followed up by phone, mail or other means. This process should be reflected in the IPND Industry Code.**

[6] *In an emergency, can you be found?*, http://www.acma.gov.au/WEB/STANDARD/pc=PC_312369. See also Question 18.

Recommendation Two:

- **The ACMA and the IPND Manager should expand the promotion to consumers of the importance of notifying Carriage Service Providers (CSPs) and/or the IPND (see question 17) if their personal details have changed, focusing on the significance this has on access to emergency services.**

Recommendation Three:

- **The name of the IPND should be changed to become more consumer-friendly, memorable and descriptive - for example, the National Phone Number Register.**

Recommendation Four:

- **Information about the IPND, using its new name, should be printed in large font and in common community languages on all ISP/RSP/phone bills.**

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 for IPND data is too broad in some ways and too narrow in others. ACCAN agrees that the regime is confusing and potentially contradictory. The IPND Manager's Carrier Licence Conditions, Telecommunications Act 1997, IPND Scheme, Privacy Act and TIA must all be consistent. ACCAN looks forward to the Australian Privacy Foundation's submission in regards to this matter.

Further, there needs to be a clear process for disclosure, one which uses high-level principles to ascertain whether a disclosure is in the public interest. IPND users, including researchers, must be disclosed on a public register.

Recommendation Five:

- **The ACMA should develop an IPND disclosure regime, including high-level principles and processes, and these should be made public.**

Recommendation Six:

- **The ACMA should keep a public register listing IPND users, including researchers.**

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

ACCAN does not recommend new categories of user, although we do recommend the position that an individual is a 'user' of their own data. See question 17 for further information.

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

It is not easy to differentiate between a Directory Address[7] and a Service Address[8]. Further discussion of these definitions, as well as the possible inclusion of a Billing Address, may be useful in determining which data elements IPND users should be able to access.

ACCAN suggests some changes to the way LDCS providers access data. There are two issues of concern:

- It is inappropriate for LDCS providers to have access to all IPND fields, for reasons of privacy[9]

- Holders of unlisted ('silent') numbers may be (unwittingly) disadvantaged in attempting to call numbers which require routing. This is because the IPND cannot be used by LDCS providers where a consumer has an unlisted number.

  Provision of suburb information, however, may threaten the safety of some unlisted subscribers. ACCAN therefore recommends that suburb data be aggregated to provide 'sub-region' information to LDCS providers, as well as State/Territory information. This would provide a balance between privacy requirements and the benefits to individuals of being able to make appropriately routed calls. Alternatively, holders of unlisted numbers could be given an informed choice as to whether they wanted limited location data to be disclosed to LDCS providers

Recommendation Seven:

- **In the case of listed numbers, LDCS providers should have access only to the fields/data they require in order to accurately route a call – that is, the sub-region and State/Territory of the address in the case of geographic numbers (and the sub-region and State/Territory of the device in the case of roaming/mobile/VOIP numbers, should this be incorporated into the IPND - see question 25). This should be the case whether a phone number is 'listed' or 'unlisted' ('silent').**

Recommendation Eight:

- **In the case of unlisted ('silent') numbers, the ACMA should lead further consultation as to whether ACCAN's Recommendation Seven should be implemented, or whether holders of unlisted numbers should be given an informed choice as to whether they want this data disclosed to LDCS providers.**

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

ACCAN believes that Emergency Service Organisations and industry are best placed to respond to this question; however, please see Question 25.

[7] Australian Communications Industry Forum, *IPND Data Industry Guideline ACIF G619:2007*, p. 7; http://www.commsalliance.com.au/__data/assets/pdf_file/0016/1726/G619_2007.pdf
[8] Australian Communications Industry Forum, *IPND Data Industry Guideline ACIF G619:2007*, p. 9; http://www.commsalliance.com.au/__data/assets/pdf_file/0016/1726/G619_2007.pdf
[9] See *National Privacy Principles*, particularly 1 and 2, Office of the Australian Information Commissioner, http://www.privacy.gov.au/materials/types/infosheets/view/6583

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

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

ACCAN believes that the IPND Scheme's objectives remain relevant. However, see also ACCAN's Recommendations Five and Six in regards to public interest tests and accountability. ACCAN supports the view that privacy breaches should be appropriately reported and investigated.

ACCAN also notes that there is currently debate in the field as to whether it is appropriate for the Office of the Australian Information Commissioner (OAIC) to be the sole recipient of information that a substantive data breach has occurred, and whether individuals who may be affected should also be informed.

Recommendation Nine:

- **Holders of IPND Scheme authorisations should be required to notify the Office of the Australian Information Commissioner where there has been a substantive data breach resulting in the disclosure of protected information.**

Recommendation Ten:

- **The ACMA should encourage debate as to whether there is a "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"[10].**

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

ACCAN believes that industry is best placed to respond to this question.

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

12. Alternatively, should the same use and disclosure restrictions in Part 13 of the Telecommunications Act 1997 apply to all directory products, regardless of where the information is sourced? Why/why not?

ACCAN has no comment on whether *all* publishers of directory products be required to use the IPND as the source of their data, but ACCAN believes that it is certainly the case that 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. This is for three reasons:

[10] See submission from the Australian Privacy Foundation, yet to be published

- To ensure that all directory products are bound by the same rules to ensure a level playing field
- So customers of CSPs other than the IPND Manager's are not required (due to their CSP's commercial arrangement with Sensis) to provide personal information to a third-party business (i.e. Sensis)
- 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

Recommendation Eleven:

- **Directory products published by the same company which manages the IPND (that is, currently, Telstra) should be required to obtain its directory data exclusively from the IPND.**

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?

ACCAN notes that the IPND is effectively a mandatory register and that therefore it is appropriate to severely restrict access to it for non-critical users. Compare this, for example, with the *Do Not Call Register Act* 2006, which legislates an opt-in register and allows for a greater range of categories for access.

ACCAN is comfortable to an extent with the current three categories of research under the IPND Scheme. However, we note that health research proposals and possibly research proposals by government are likely to have undergone an ethics review before getting to the point of requesting an authorisation through the IPND Scheme. Political research, however, is unlikely to have undergone such a review. Political research, conducted ethically and appropriately, is likely to be beneficial to the body politic. Push polling or political canvassing, on the other hand, conducted in the guise of political research, is likely to be harmful to the body politic. The ACMA must have clear guidelines to differentiate between the two, and must have access to the range of questions to be asked.

Recommendation Twelve:

- **Any organisation proposing political research via the IPND Scheme must provide to the ACMA the questions to be asked of consumers, and the ACMA must take these questions, and their objectives, into account when considering authorisation under the IPND Scheme.**

ACCAN supports the Australian Privacy Foundation's submission in making the following recommendations.

Recommendation Thirteen:

- **Access to the IPND should remain subject to project-specific authorisations from the ACMA.**

Recommendation Fourteen:

- **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 is the effect of the test proposed by the ALRC in Recommendation 72-14 of Report 108).**

Recommendation Fifteen:

- **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).**

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?

ACCAN supports the views of the Australian Privacy Foundation in the following recommendations.

Recommendation Sixteen:

- **Sections 280(1)(b) and s297 of the *Telecommunications Act* should be amended to read '*specifically* authorised...'**

Recommendation Seventeen:

- **The ACMA and OAIC should better publicise, both to CSPs and the public, the fact that NPP 2 (and IPPs 10 and 11 for agencies) continue to apply but that the provisions of Part 13 provide more specific rules about permissible uses and disclosures.**

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?

Currently, it appears that it is almost impossible for consumers to gain access through any means to their own complete IPND data. This is despite the fact that the Privacy Act gives everyone the right to have access to this data. This access would also help to ensure that IPND data is accurate and current. Consumers should therefore be considered 'IPND users' of their own data.

Both access to, and editing of, IPND data by consumers should of course be managed appropriately, in line with the Privacy Act. For example, identity checks should be required, including current address verification.

Any edits made by a consumer must of course flow on to the CSP (in the case that the customer has changed their data via the IPND Manager) and the IPND Manager (in the case that the customer has changed their data via their CSP).

Recommendation Eighteen:

- **Consumers must have access to their own complete set of IPND, preferably direct from the IPND Manager, subject to identity verification.**

Recommendation Nineteen:

- **Consumers must have the ability to edit their own data, subject to identity verification.**

Recommendation Twenty:

- **Both the consumer's CSP and the IPND Manager must be made aware of any consumer-initiated changes to a consumer's IPND data.**

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?

Yes. The IPND is essentially 'marketed' to the public as an emergency database[11] - consumers are encouraged to provide correct and current information to their CSP specifically so that they can be found in an emergency. Therefore, although ACCAN strongly supports the mandatory provision of information to critical IPND users (that is, emergency calls and emergency warnings), consumers should be able to opt out of having their IPND information accessed by non-critical users on a category by category basis. This is supported by Section 14 of the Privacy Act 1988[12], including Principle 2 of the National Privacy Principles[13]. ACCAN also, however, supports the access to limited fields by LDCS providers (see Recommendation Seven).

Further, consumers who essentially 'opt out' of having their data used by public directory publishers – that is, consumers who elect to have unlisted entries and/or suppressed addresses – should not be penalised financially for this. For many consumers, this is not simply a 'moral' privacy issue; it directly concerns their and their family's safety. Consumers must have the right not to share their details with a public directory publisher and with the public in general, without having to pay for this right.

Recommendation Twenty-one:

[11] See for example http://www.acma.gov.au/webwr/_assets/main/lib100534/ipnd_awareness_campaign_postcard-dec_2010.pdf
[12] http://www.privacy.gov.au/materials/types/infosheets/view/6541#a
[13] http://www.privacy.gov.au/materials/types/infosheets/view/6583#npp2

- **Consumers should be allowed to opt out of having their IPND information accessed by non-critical IPND users on a category by category basis.**

Recommendation Twenty-two:

- **Consumers must not be charged by their CSP should they elect to have an unlisted entry ('silent line') and/or suppressed address.**

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 accurate audits of IPND data are required to ascertain accuracy. This means verifying accuracy and currency of data, not simply by comparing addresses to a database, but by contacting a sample of consumers (in writing, where possible, in order to ensure credibility to the reader). The IPND Scheme itself may be able to be used to achieve this, given that public policy research conducted by a Commonwealth authority or agency is allowed under the Scheme.

The illegitimate disclosure of IPND information is extremely serious. ACCAN is not in a position to judge whether both civil and criminal penalties are required – we simply note that this must be considered a significant breach of privacy, and one which could have considerable impact on those individuals whose privacy has been breached. Penalties should reflect this.

Further, however, it is not only privacy breaches which require significant penalty. Failure of a CSP to provide accurate or current information must also be recognised as a very serious breach and penalised as such. Simply, for example, having to provide a court-enforceable undertaking, while useful for improving data integrity for the CSP concerned, may not be a significant enough deterrent to prevent other CSPs from failing to adhere to their IPND obligations.

Recommendation Twenty-three:

- **The ACMA must broaden the scope of IPND audits to verify accuracy and currency of data.**

Recommendation Twenty-four:

- **Both privacy breaches and failure by CSPs to provide current and/or accurate information – or failure by the IPND Manager to record that information – must incur significant penalty, to reflect the seriousness of the infringement.**

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?

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?

ACCAN believes that industry is best placed to respond to these questions.

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

Clearly, the delivery of dynamic location information to Emergency Service Organisations (ESOs) is essential. ACCAN has previously argued[14] that a 'push' model should be implemented, with location information provided using the most accurate method possible (GPS, in the case of many mobile devices, for example). Calls to emergency services from VoIP and mobile devices are likely to continue to increase, intensifying the need for accurate and timely provision of location information from mobile/nomadic call services.

The issue as to how dynamic location information is provided to ESOs may well be a technical one. ACCAN certainly supports in principle the IPND being used if this is technically feasible, given our position regarding the utility of multiple databases (see ACCAN's Recommendation Twenty-seven).

As noted in ACCAN's previous submission to the ACMA[15], however, it is essential that this dynamic location information data not be limited to VoIP and mobile devices. Users of the following services must also have the assurance of being able to be located, and having this location noted in a dynamic field of IPND, should that be the method chosen to provide location information to ESOs:

- The National Relay Service's internet relay service[16] to Triple Zero
- The National Relay Service's Speak and Listen service[17] (whether originating from mobile or landline) to Triple Zero
- The Australian Communication Exchange's video relay service[18]
- The Australian Communication Exchange's web-based captioned telephony service[19]
- The proposed SMS emergency service
- The proposed 'Smart 106' emergency smartphone 'app'
- Emergency calls from users of satellite services.

---

[14] ACCAN, *Customer location information and numbering data*, March 2011, http://accan.org.au/index.php?option=com_content&view=article&id=274:customer-location-information&catid=146:emergency&Itemid=316 and ACCAN, *Response to the draft Telecommunications (Emergency Call Service) Amendment Determination 2009*, November 2010, http://accan.org.au/files/Submissions/ACCAN%20Submission%20to%20draft%20Emergency%20Call%20Services%20Determination%20AMENDMENT.pdf

[15] ACCAN, *Response to the draft Telecommunications (Emergency Call Service) Amendment Determination 2009*, November 2010, http://accan.org.au/files/Submissions/ACCAN%20Submission%20to%20draft%20Emergency%20Call%20Services%20Determination%20AMENDMENT.pdf

[16] http://www.relayservice.com.au/making-a-call/internet-relay/

[17] http://www.relayservice.com.au/making-a-call/speak-and-listen/

[18] http://www.aceinfo.net.au/index.php?option=com_content&view=article&id=5&Itemid=16

[19] http://www.aussiedeafkids.org.au/newsletter_oct09_art6.html Note: This service is not currently available, although handset-based captioned telephony is.

The use of the internet to carry 'phone' calls will eventually change the relevance and nature of geographic numbers; in fact, this is already occurring, as outlined in an example recently brought to the attention of the Emergency Call Service Advisory Committee[20], which appears to stem from the fact that the subscriber of a VoIP service with whom a number is associated may reside anywhere in the world – and the end user may be a different person or organisation, who again may reside anywhere in the world. This is because the use of telephone numbers for VoIP services differs from those applicable to public switched telephone network (PSTN) services in a number of significant ways. VoIP only represent the user identity of an internet service (or application); they do not necessarily represent a subscription identity to a physical network provider (CSP). The application provider may not have a physical presence in the Australian jurisdiction – even if they are assigning subscription identities from the Australian PSTN number pool. This issue would seem to further support an IPND which includes dynamic location information for VoIP services.

Recommendation Twenty-five:

- **If technically feasible, dynamic location information should be included in the IPND.**

Recommendation Twenty-six:

- **Dynamic location information for users of relay and satellite services must also be included.**

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

ACCAN believes that industry is best placed to respond to this question.

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

The IPND must be robust and reliable – it goes without saying that there must be a trustworthy method of tracking emergency call origination locations and sending (eventually location-accurate) emergency warnings. The essential work of managing the IPND, however, does not need to be undertaken by Telstra necessarily. Should a reasonable alternative become available, ACCAN would be interested in considering this. Any transition, of course, must be managed extremely carefully, in the interests of consumer safety.

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?

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?

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

ACCAN believes that industry is best placed to respond to these questions.

[20] http://www.acma.gov.au/WEB/STANDARD/pc=PC_2502

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?

ACCAN believes that the use of separate database would likely lead to more errors, given the large and complex number of lines of communications which would be required to share data. It is also likely that use of a single database would be less expensive than the establishment and maintenance of a number of databases. As long as privacy provisions are available (see Question 18) to allow consumers to opt out of non-essential uses, a single database for these various purposes is preferred.

Recommendation Twenty-seven:

- **The IPND should remain a single database, despite its various purposes.**