Australian Government
Department of Communications

Review of the Integrated Public Number Database

April 2015

GPO Box 2154 Canberra ACT 2601 Australia • telephone 02 6271 1000

Disclaimer

The material in this report is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this report.

This report has been prepared for consultation purposes only and does not indicate the Commonwealth's commitment to a particular course of action. Additionally, any third party views or recommendations included in this report do not reflect the views of the Commonwealth, or indicate its commitment to a particular course of action.

Copyright

Contents

Terminology and acronyms vi
Executive Summary ix
List of Recommendations xii
Introduction 1
What is the IPND and what does it do? 1
The Review - drivers 5
Technological change 5
Review of Privacy Law and Practice 5
The Review - process 7
Public engagement 7
Other sources of information 7
International examples 7
Structure of this report 8
Need for the IPND 9
How has the IPND been used? 9
Changing technology 10
Consumer expectations 11
Need for information by critical users 11
Need for information by non-critical users 12
Finding 12
Quality and Accuracy of the IPND 13
The issues 13
Views of stakeholders 13
Obligations of CSPs 14
Testing accuracy 14
IPND accuracy study 15
The accuracy study's findings 15
Accuracy of the IPND compared to other similar databases 16
Reasons for inaccuracy 16
Options to improve accuracy of the IPND 17
Checking the accuracy of current IPND data 18
Enhanced feedback loops 19
Access to records by individual subscribers 19
Enhanced awareness raising measures 21
Security and Privacy 23

Why protect information? 23
Use and disclosure 24
ALRC review 26
Who should have access? 26
Access for critical users 27
Access for non-critical users 29
Who should decide? 29
Unlisted numbers 29
Unlisted on category by category basis 30
LDCS access to unlisted numbers 32
Public Number Directories 33
Rules for IPND Public Number Directories 33
Sources for Public Number Directories 34
Other ALRC recommendations about IPND 36
Unauthorised alteration of records 36
Notification of data breaches 37
Civil penalties 37
Research 37
Definition of 'enforcement agency' 38
Disclosure of unlisted number for emergency services 38
Finding 38
Additional data users 40
Likely changes in future demand 40
Additional non-critical users 40
New types of researchers 41
Stakeholder views 42
Principles for approving research 45
Other new non-critical users 45
Standing authorisations 48
Finding 48
Additional data fields 49
Stakeholder views 49
Critical users 51
Dynamic internet based information 52
Information provided through the MoLI program 53
National geo-coded addressing 53
Date of birth 54

International Mobile Subscriber Identity 54
Update to the type of service field 55
Finding 55
Management of the IPND 56
Transparency of role of IPND manager 56
Current management of the IPND 56
Stakeholder views 56
Accountability and transparency of the IPND manager 57
Technical requirements 58
Views of stakeholders 58
Impact on stakeholders 59
Cost of access and management of the IPND 59
Views of stakeholders 59
Current compliance costs 60
Cost of access for data users 60
Regulatory issues to gaining access 61
Case study: Process of acquiring access to the IPND 62
Finding 63
Future of the IPND 65
Development process 66
Incremental change 67
Appendix 1 – List of public submissions and submission process. 69
The submission process 69
Appendix 2 – Summary of 2012 workshop 72
Appendix 3 – Summary of 2014 Stakeholder meeting 75
Appendix 4 – Results of IPND accuracy study 78
Appendix 5 – Sample IPND Entry 88

Terminology and acronyms

Anti-scraping technology is technology that prevents the theft of data or intellectual property from a website.

Asymmetric digital subscriber line (**ADSL**) is a type of digital subscriber line (DSL) technology, a data communications technology that enables data transmission over copper telephone lines.

The **Australian Communications Consumer Action Network (ACCAN)** is a peak consumer advocacy body on communications issues, including telecommunications and broadband.

The **Australian Communications and Media Authority (ACMA)** is Australia's communications regulator, and among other things, has responsibility for enforcing much of the Telecommunications Act.

The **Australian Law Reform Commission (ALRC)** is an independent statutory authority that reviews Commonwealth laws.

The **Australian Privacy Foundation (APF)** is a non-governmental organisation dedicated to protecting the privacy of Australians.

Carriage Service Providers (CSPs) are telephone companies or internet service providers (ISPs) that supply communications services to the public using radio communications facilities, telephone lines or optical fibre owned by carriers. All CSPs that issue telephone numbers must provide information to the Integrated Public Number Database (IPND).

Carriers are organisations that own radio communications facilities, telephone lines or optical fibre which are used to supply telecommunications services to the public. Many carriers are also CSPs.

Critical users of the IPND, for the purposes of this report, refer to those users of the data that gain access to support emergency services, law enforcement and national security functions.

Department of Communications (the Department) was the **Department of Broadband, Communications and the Digital Economy (DBCDE)** prior to September 2013.

Directory Assistance (DA) services are services that help end-users of telephone services find the telephone number of other end-users.

Do Not Call Register (DNCR) is a register to enable people to register their telephone or fax numbers so that they do not receive certain unsolicited telemarketing and fax marketing calls. The DNCR is administered by the ACMA.

Emergency Call Person (ECP) is the operator of an emergency call service. The ECP for Triple Zero and 112 is Telstra. The ECP for 106 is the operator of the National Relay Service.

Emergency Call Service (ECS) is a nationwide operator-assisted service that connects a caller, free of charge, to police, fire or ambulance in a life threatening or time critical situation. There are three emergency call services in Australia – Triple Zero (000) for landlines, 112 for mobile phones and 106 that provide text-based calls through teletypewriter or computers primarily for people with a hearing or speech impairment.

Emergency Warning System (EWS) a telephone-based warning system set up in 2009 to use IPND data to send warnings to connected telephones in the locality of an emergency event.

End-users are the actual users of a telephone or internet service.

The **Integrated Public Number Database (IPND)** is a database of all listed and unlisted telephone numbers and associated customer data.

IPND data providers are CSPs that provide subscriber information to the IPND manager. In practice, most CSPs do not provide data directly to the IPND manager, but instead provide it to third parties, which aggregate the information, then provide it to the IPND manager.

The current **IPND manager** is Telstra, which is responsible for operating and providing access to the IPND.

IPND users are organisations that use IPND information to provide services to end-users, subscribers and the public. This report distinguishes between critical and non-critical IPND-users.

Integrated Services Digital Network (**ISDN**) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network.

Location Dependent Carriage Services (LDCS) are carriage services that enable calls to be routed based on the location of the caller—for example, calling 131 444 diverts a call to the closest police station. LDCS are used for a range of services, from services provided by government to taxi and pizza services.

Mobile Location Information (MoLI) is location information that is based on the estimated location of a handset, rather than the billing or service address.

Non-critical users of IPND data are, for the purposes of this report, those users of the data that gain access to support functions such as directory assistance, production of public number directories or to conduct research.

Numbering Plan or the **Telecommunications Numbering Plan 1997** is the legislative instrument setting out the framework for the telephone numbering of carriage services in Australia and the use of telephone numbers in connection with the supply of these services.

The **Office of the Australian Information Commissioner (OAIC)** is an independent Australian Government agency with functions relating to privacy legislation, freedom of information and government information policy.

Public number directory (PND) (also known as a 'phone book' i.e. the Telstra White Pages®), is a listing of subscriber names and telephone numbers.

Public Switched Telephone Network (PSTN) is a world-wide circuit switched telephone network. The PSTN allows the interconnection of telephone services from all over the world.

Subscribers are people or organisations that have a contract with a CSP for the supply of telephone or internet services as end-users.

Voice over Internet Protocol (VoIP) is a telephone service that communicates using the Internet Protocol (IP). Some VoIP services allow the end-user to easily move the service to different geographical locations. These services are known as 'nomadic VoIP' services.

Executive Summary

The IPND is a centralised database containing records of all Australian telephone numbers and associated customer details. In June 2014, it contained 64.8 million records of connected services.

The information in the IPND includes customer name, customer address, phone number, whether the service is fixed or mobile, whether the service is listed or unlisted and details about the service provider. IPND information is used in different ways to assist data users provide a range of services. These users can be divided into 'critical' and 'non-critical'.

The critical users are: the emergency call services (ECS), the emergency warning system (EWS) and national security and law enforcement agencies.

Critical users use IPND information to protect life and property and to investigate serious crime. Without the IPND, many critical services that people rely on every day would not function efficiently. A failure of the IPND manager to provide accurate, timely and current information to critical users can have serious consequences. For example, any failure of the IPND to provide location information to the Triple Zero emergency call service could place the lives of callers at risk.

Non-critical users of IPND information include public number directories publishers, directory and operator assistance providers, location dependent carriage service (LDCS) providers and researchers for electoral, health and government policy research.

These users provide a range of services and products to government, subscribers and the general public that would not be possible-or would be much more difficult-without a system like the IPND.

The review process

This report presents the results of a review conducted by the Department of Communications (the Department) of the effectiveness and continued need for the IPND, in light of changes to telecommunications technology. It also responds to relevant recommendations of the 2008 review of privacy law by the Australian Law Reform Commission. During the review, the department engaged with key stakeholders, sought submissions, conducted two stakeholder workshops and commissioned a comprehensive study of the quality and accuracy of the IPND.

The review was informed by high level strategic considerations, including the need to:

- ensure critical users have access to accurate information needed to perform their functions
- protect the privacy of individuals through appropriate safeguards on use and disclosure
- minimise costs to industry and data users.

Summary of key findings and recommendations

Since the IPND was first established in 1998, the telecommunications industry has changed: mobile phones are now largely universally used in Australia, and increasing numbers of households no longer have landline ('fixed') telephone services. These developments place pressure on the traditional data sources underpinning emergency call services as well as some activities of law enforcement and national security agencies. Despite these changes, the community expects that these agencies will continue to be effective, and that emergency services will be able to locate individuals in an emergency.

The current 'critical users' of IPND data use it to support functions that protect life and property in emergencies, and to investigate serious crime. The needs of critical users are the reason the collection, secure storage, approved access and use of information from the telecommunications industry continues to be justified. That said, access to and usage of IPND data by critical users' needs to be done in a way that protects individuals' privacy as well as minimising the impositions on the communications industry.

Almost everyone in Australia uses telecommunications services and the review found that the customer information collected by telecommunications carriage service providers (CSPs) remains a practical source of information to enable the activities of critical services. However, the IPND in its current form has become less useful to its critical users, and changes in technology mean that critical information is increasingly sourced in other ways with little coordination.

As IPND Manager, Telstra has provided a secure and reliable service. However, there is little information about how Telstra determines access charges and handles its various roles as carrier, publisher of the White Pages® and IPND manager. There is also little or no current incentive for Telstra to update and refine the IPND over time, and some industry stakeholders have argued that the cost of interfacing with the IPND's legacy systems is significant. The management and regulation of customer information could therefore be improved.

During the review, the Department proposed an option to transition from the current static IPND to a new system to provide better functionality to users, maximise the benefits of emerging technologies, streamline existing regulation and limit the future costs to industry. This was tested extensively with key stakeholders. However, the Department considered there was not enough support for this proposal at this stage to warrant the extensive effort and cost in developing a new system. Nevertheless, the report includes details of that option, for possible future reference, and suggests that the current system be retained until at least the completion of the Department's review of the Triple Zero Operator and the letting of the tender for the Triple Zero operator in 2016.

The report makes nine recommendations regarding the IPND. These recommendations can be broadly grouped into four thematic areas:

- **Data quality and accuracy** – recommends the enhancement of processes to ensure timely updating/changes to data, the improvement of data quality as part of the next IPND code review and raising subscribers' awareness of the importance of providing correct information about their service.
- **Improved access** – recommends the broadening of non-critical user access to IPND data on case by case basis and for the Australian Communications and Media Authority (ACMA) to grant access to users for specific purposes where appropriate safe guards can be met.
- **Governance** – recommends greater transparency of ACMA decisions made under the IPND scheme and of the IPND manager, via broader public release of governance and accountability documentation
- **Interdependencies** – recommends investigating the need for a new system after the completion of the Department's Review of the Triple Zero operator and the implementation of the Triple Zero contract arrangements from 2016.

Terms of reference for the review of the IPND

On 17 November 2011, the then Department of Communications and the Digital Economy (the Department) – now the Department of Communications - commenced a review of the IPND to assess:

- the effectiveness and utility of the IPND
- the ability of the IPND to innovate and keep pace with technological and market changes

- the privacy implications of the IPND.

The complete terms of reference for the review are as follows:

Table 1 – Integrated Public Number Database Review Terms of Reference

The Integrated Public Number Database (IPND) is a centralised database of all Australian telephone numbers and associated subscriber information. The IPND provides information to support a range of services, including the Triple Zero emergency call service, the dissemination of telephone-based emergency warnings, investigations of law enforcement and national security agencies, and the creation of public number directories.

However, market and technological changes are placing pressure on the IPND to remain relevant.

The IPND review will enquire into and in early 2012 advise on whether the IPND is fulfilling its objectives, whether these objectives are still relevant and any reforms that should be undertaken. A key part of the review will be to consider the role of the IPND in a National Broadband Network environment and the transitionary arrangements required.

The review will examine and report on:

1. The effectiveness and utility of the IPND, including:
    a. the ongoing need for a centralised database, with consideration of:
        i. how the IPND compares against alternative solutions in overseas jurisdictions
        ii. what alternative would need to be implemented to meet the needs of critical users if the IPND is not continued.
    b. the governance and management of the IPND (including the cost of providing the IPND)
    c. the quality and accuracy of IPND information
    d. whether enhancements can be made to the IPND's regulatory and operational arrangements to promote the public interest.

2. The ability of the IPND to innovate and keep pace with technological and market changes, including, but not limited to:
    a. the functionality of the IPND and whether it has kept pace with the expectations of the Australian community and IPND users (particularly critical users such as the Triple Zero emergency call service)
    b. the categories of IPND users, and whether they can be further aligned with the public interest
    c. the interaction between the IPND and the National Broadband Network
    d. what functionality a future IPND, or its alternative, needs to contain.

3. The privacy implications of the IPND, including:
    a. maintaining appropriate protections;
    b. access, use and disclosure of IPND information; and
    c. any relevant recommendations from the Australia Law Reform Commission's *For Your Information: Australian Privacy Law and Practice* report.

List of Recommendations

The recommendations set out in this report are as follows:

Recommendation 1

The quality and accuracy of data in the IPND should be improved by:

- enhancing the existing feedback processes between the IPND manager, data providers and data users including by exploring improved automated processes and ensuring changes are made in a timely way
- industry working to improve the quality of information in the next review of the IPND Code (note - such as by requiring that all data providers use validation software).

Recommendation 2

The regulatory arrangements should be amended to ensure subscribers can:

- be provided with the information in the IPND relating to themselves
- flag incorrect information for action by CSPs in a specified timeframe.

Recommendation 3

In order to raise awareness of the IPND, CSPs should:

- alert their subscribers of their IPND information
- advise subscribers regularly of the importance of providing correct information.

Recommendation 4

The range of users able to apply for access to IPND information (including anonymised information about unlisted numbers) should be broadened to include a wider range of researchers – for instance, the Australian Bureau of Statistics (ABS), NBN Co and others subject to a case by case privacy impact assessment and public interest test.

Recommendation 5

The ACMA should be able to approve ongoing or periodic access for an applicant, provided that the ACMA regularly reviews access and that a privacy impact assessment is completed.

Recommendation 6

The ACMA should be able to approve electronic public number directories to display unlimited numbers of entries from the IPND if appropriate 'anti-scraping' measures are in place.

Recommendation 7

The ACMA should publish information about applications and decisions made under the IPND Scheme.

Recommendation 8

In order to improve the transparency of the management of the IPND, Telstra should make available:

- the measures it takes to separate its role as part-owner of the publisher of the White Pages® and the manager of the IPND
- its standard form of agreement with data users
- annual audited financial reports for the IPND.

Recommendation 9

The current IPND should be retained for the medium term and the need for a new system should be investigated again after the completion of the Department's Review of the Triple Zero operator and the implementation of the Triple Zero contract arrangements from 2016.

The Department will be seeking feedback from industry and relevant stakeholders on these recommendations.

The IPND is established by a complex interaction of primary legislation, legislative instruments and industry codes and standards.

Consistent with the Government's deregulatory agenda it is suggested industry would implement changes on a voluntary basis in the first instance. Any regulatory changes would look to simplify the regulatory arrangements to progress the reforms within this report. Where possible the Department will try and implement the recommendations without additional regulatory measures being imposed.

Introduction

This section provides an overview of the Integrated Public Number Database (IPND) and the purposes it serves. It describes the regulatory and operational framework for the IPND and the reasons for the review.

What is the IPND and what does it do?

The IPND is a centralised database containing records of all Australian telephone numbers and associated customer details. In June 2014, it contained more than 64.8 million records of connected services.[1] Services listed in the IPND include:

- traditional fixed line telephone services
- mobile phone services
- VoIP services associated with a telephone number
- shared numbers (including 13 and 1800 numbers)
- payphone services
- dial up internet services.

The information in the IPND includes customer name, customer address, phone number, whether the service is fixed or mobile, whether the service is listed or unlisted and details about the telecommunications company providing the customer with the service. Appendix 5 contains a complete sample IPND entry.

Carriage Service Providers (CSPs) collect data from their subscribers and provide it to the IPND manager, which has been Telstra since the IPND was established in 1998.

IPND information is used in different ways to assist in a range of services. For the purposes of this report, these services can be divided into 'critical' and 'non-critical'.

The critical users are:

- the emergency call services (ECS)
- the emergency warning system (EWS)
- national security and law enforcement agencies.

Critical users use IPND information to protect life and property and to investigate serious crime. Without information from the IPND, many critical services that people rely on every day would not function efficiently. For example, emergency service organisations use location information drawn from the IPND to dispatch emergency services in response to calls from members of the public. Any failure of the IPND to provide accurate and timely location information to the emergency call service could place the lives of callers at risk.

Information in the IPND is also used for a range of other purposes.

[1] ACMA *Communications Report 2012-13,* p.24

Non-critical users of IPND information are:

- public number directories publishers
- directory and operator assistance providers
- location dependent carriage service (LDCS) providers
- researchers for electoral, health and government policy research.

These non-critical users provide a range of services and products to government, subscribers and the general public that would not be possible, or be much more difficult, without access to a system like the IPND.

Why was the IPND established?

With the entry of new carriers and CSPs into the telecommunications sector in the 1990s, the IPND was designed to be a centralised and comprehensive source of telecommunications information for emergency services and directory assistance, and to allow competition in the telephone directory markets.

Prior to the creation of the IPND, critical users of this information would contact the telecommunications carriers for information about subscribers on a manual and case-by-case basis. With the introduction of competition in the telecommunications market and the possibility of a large number of new providers, a comprehensive and industry-wide database was required in order to allow this information to be accessed in a timely way.

How has the policy changed over time?

Since its establishment, the IPND has undergone some changes to account for new policy challenges. Major changes include:

- from 2007, limited access to the IPND was enabled for government, electoral and health researchers. As part of this, the IPND scheme was established to assess requests by researchers and public number directory producers.
- in 2009, reforms enabled IPND information to be used for telephone-based emergency warnings, and clarified that IPND information could be used for Location Dependent Carrier Services.

How is it established?

The IPND is established by a complex interaction of primary legislation, legislative instruments and industry codes and standards.

The key pieces of legislation are:

- *Telecommunications Act 1997* (the Telecommunications Act)
- *Telecommunications (Interception and Access) Act 1979* (the TIA Act)
- *Privacy Act 1988*
- *Telecommunications (Consumer Protection and Service Standards) Act 1999*

Relevant statutory instruments include:

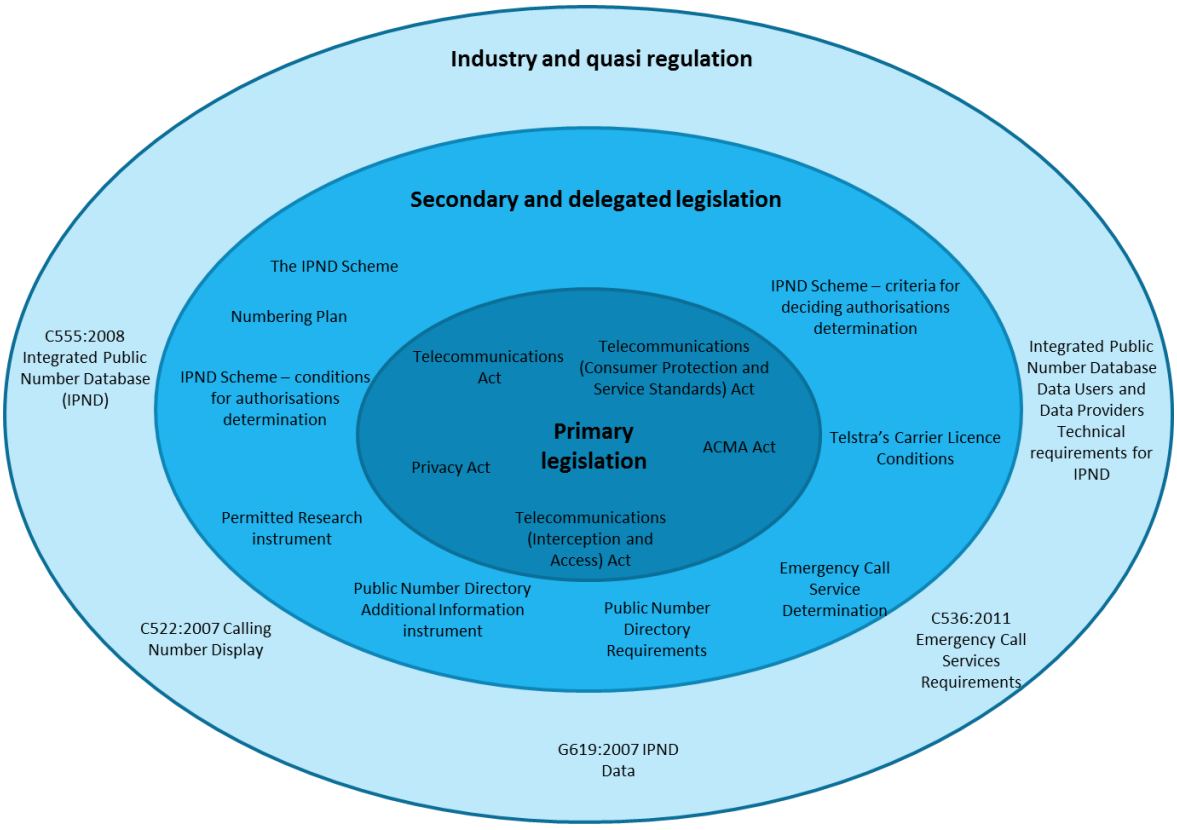
- Telecommunications Integrated Public Number Database Scheme 2007
- Telecommunications (Integrated Public Number Database – Public Number Directory Requirements) Instrument 2007 (No. 1)
- Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997 (the carrier licence conditions)
- Telecommunications (Emergency Call Service) Determination 2009

Industry codes have been developed to address the technical requirements for the provision of data and emergency call services requirements. Telstra has also produced technical requirements for data users and providers. These relationships are illustrated below.

These work together to:

- require Telstra to establish and maintain the IPND
- require CSPs to provide information to the IPND manager in a certain form
- regulate the circumstances under which information in the IPND can be used
- protect the security of this information.

Figure 1. Illustration of regulatory framework



How does the IPND actually work?

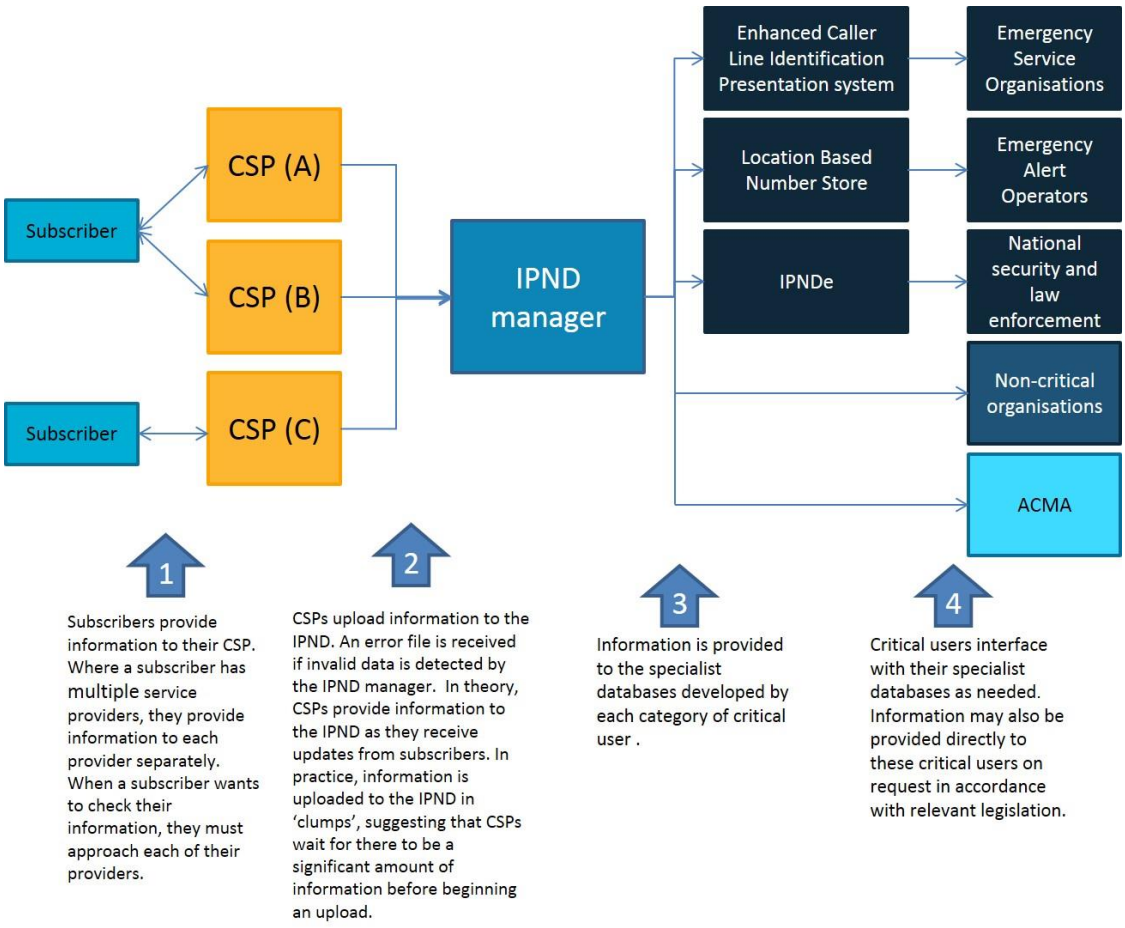
In operational terms, the IPND is a central database on a private network under the control of Telstra as the current IPND manager.

Data providers provide updated information from CSPs to the IPND manager by secure link each business day.[2] The IPND manager then provides information from the database to the data users. Updated information should be available to emergency services and law enforcement agencies within a matter of hours.[3]

Since 2007, the ACMA has been responsible for authorising access to producers of public number directories and researchers who then must seek access to information from the IPND manager. All other types of users seek access directly from the IPND manager.

Under its licence conditions, Telstra is able to recover operating costs and a reasonable rate of return on capital from CSPs seeking access to the IPND.[4]

Figure 2. Current data model of the IPND



[2] Communications Alliance *Integrated Public Number Database Industry Code ACIF C555:2008,* p.17

[3] *ibid* p.21

[4] Clause 10 of *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*

The Review - drivers

The Department, with the agreement of the former government, chose to undertake this review because of two main factors:

- a realisation that technological change was affecting the utility of the current IPND
- the recommendations of a large scale review of Australian privacy legislation.

Technological change

The telecommunications industry has changed significantly since the IPND was first established. Mobile services have become close to ubiquitous, and Voice over IP (VoIP) services have grown in popularity. These and other changes in the telecommunications market have changed the way that the emergency call services, law enforcement and national security agencies have conducted their work. Over time, new IPND users such as the EWS and researchers have been introduced.

The telecommunications market will continue to change. For example the current rollout of the National Broadband Network (NBN) will drive an increased uptake of IP-based telephony.

While the telecommunications market and IPND users have changed over time, the IPND has largely remained static. There have only been limited technological upgrades to the system over the years. When changes to legislative and operational arrangements have occurred, they have largely been to address specific policy issues as they have arisen.

Review of Privacy Law and Practice

In 2008, the Australian Law Reform Commission of Australian (ALRC) completed a comprehensive review of privacy legislation and published a multi-volume report *For Your Information: Australian Privacy Law and Practice* (the ALRC Report).[5] As a consequence, key changes to the *Privacy Act 1988* (the Privacy Act) came into effect in March 2014, including the introduction of a single set of Australian Privacy Principles (APPs). These principles replaced the existing Information Privacy Principles (IPPs) that applied to public sector organisations and the National Privacy Principles (NPPs) that applied to private sector organisations.

Part J of the ALRC report related to the handling of personal information under the Telecommunications Act. It made 34 recommendations to improve the operation of the legislative framework.

Some of these recommendations have already been implemented, and changes have been made to the Privacy Act. Of the remainder, the following six recommendations are of specific relevance to the IPND and are being addressed through this report.

[5] ALRC *For Your Information: Australian Privacy Law and Practice* Report 108, available www.alrc.gov.au/publications/report-108

Table 1 – Recommendations of the ALRC report of relevance to the IPND

72-11	The *Telecommunications Act 1997* (Cth) should be amended to clarify when a use or disclosure of information or a document held on the integrated public number database is permitted.
72-12	Clause 3 of the Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997 should be amended to provide that 'enforcement agency' has the same meaning as that provided for in the *Telecommunications (Interception and Access) Act 1979 (*Cth*)*.
72-13	Section 285 of the *Telecommunications Act 1997* (Cth) should be amended to provide that a disclosure of an unlisted number is permitted if the disclosure is made to another person for purposes connected with dealing with the matter or matters raised by a call to an emergency service number.
72-14	The Australian Government should amend subsection 285(3) of the *Telecommunications Act 1997* (Cth) to provide that before the Minister specifies a kind of research for the purposes of the use or disclosure of information or a document contained in the Integrated Public Number Database, the Minister must be satisfied that the public interest in the relevant research outweighs the public interest in maintaining the level of protection provided by the Telecommunications Act to the information in the Integrated Public Number Database.
72-15	The Telecommunications (Integrated Public Number Database Scheme - Conditions for Authorisations) Determination 2007 (No 1) should be amended to provide that an authorisation under the integrated public number database scheme is subject to a condition requiring the holder of the authorisation to notify the Privacy Commissioner, as soon as practicable after becoming aware: a) of a substantive or systemic breach of security that reasonably could be regarded as having an adverse impact on the integrity and confidentiality of protected information; and b) that a person to whom the holder has disclosed protected information has contravened any legal restrictions governing the person's ability to use or disclose protected information.
72-16	The *Telecommunications Act 1997* (Cth) should be amended to provide that directory products that are produced from data sources other than the Integrated Public Number Database should be subject to the same rules under Part 13 of the Telecommunications Act as directory products which are produced from data sourced from the Integrated Public Number Database.[6]

[6] Volume 3 of the ALRC report

The Review - process

Public engagement

Throughout the review, the Department has attempted to balance the divergent views of the various stakeholders. As the first stage of the review, a public discussion paper was released. In response, the Department received 26 public submissions which are listed in Appendix 1 and available on the Department's website[7].

A number of confidential submissions were also received. These cannot be published but have been used to inform some of the discussion in this report.

The Department conducted a stakeholder workshop on 6 March 2012 to evaluate proposals for improving the IPND. A summary of the key issues discussed is at Appendix 2.

Departmental officers also engaged with the public by participating in social media discussions at www.whirlpool.net.au, a website that discusses broadband industry and consumer issues.

Departmental officers have also held bilateral meetings and informal discussions with industry, privacy, consumer and government stakeholders as needed. The primary purpose of those meetings was to evaluate recommendations to replace the current IPND with a new system to address the limitations of the current IPND.

As a result of those extensive discussions, a revised set of draft recommendations was developed. These were discussed at a stakeholder meeting held on 18 June 2014. A summary of the key points made at that workshop is at Appendix 3. Subsequent comments on the draft recommendations also inform this report.

Other sources of information

Other relevant material considered during the review includes:

- A study of IPND accuracy by Woolcott Research Pty Ltd, commissioned by the Department in February 2012. (Further information on this study can be found in the IPND Accuracy Study section of this report.)
- The Triple Zero Research study, commissioned by the Department in April 2012.

International examples

The Department examined telecommunications arrangements in other countries as part of this review to see if they could provide helpful technological or governance solutions. Where relevant, some examples of international technological solutions are included in this report. Broadly, the legislative and commercial arrangements in other jurisdictions are quite different to those in Australia, and there does not appear to be an example of a central database fulfilling as many functions as the IPND does. In some countries, there were several different databases serving particular functions.

[7] www.communications.gov.au/telephone_services/telephone_numbering/integrated_public_number_database_ipnd

Structure of this report

This report presents the results of the review of the IPND. The review examined the effectiveness and continued need for the IPND, in light of changes to telecommunications technology. It includes considerations of relevant recommendations of the 2008 review of privacy law by the Australian Law Reform Commission.

The main body of this report examines the following key issues:

- Whether there is a need for the IPND
- The quality and accuracy of the data in the IPND
- Whether the current arrangements provide the appropriate balance between privacy and utility of the information in the IPND
- Whether the IPND is effective in its current form
- Whether the current management and governance arrangements are appropriate.

Recommendations arising out of the Review are included at the start of the report and within each section of the Report.

Need for the IPND

This section discusses whether the IPND is fulfilling its policy objectives and considers whether there is an ongoing need to collect, store and disclose telecommunications user and location information.

How has the IPND been used?

IPND information is utilised under its regulatory and operational framework by a variety of users. Table 3 illustrates how the various users have employed IPND data in practice and whether this has changed from the original policy intent.

Table 2 - Use of IPND Data by category of user

Category		Original policy intent	Actual use
Critical users	Emergency Call Services (ECS)	It was intended that IPND information would be used by ECS to enable the efficient dispatch of emergency services.	The ECS uses information in the IPND as was intended, to associate a physical location with an incoming telephone call. Identity information in the IPND is also used by the ECS. As the telecommunications industry has changed, other data sources have been increasingly used to supplement the IPND and to fill the emerging gaps particularly for the location of people using mobile phones.
	National security and law enforcement agencies	It was intended that these agencies would access the IPND to assist in the investigation of crime.	These agencies access information in the IPND as was intended. IPND is used like an index. For example, an agency might have information about an address of interest and uses the IPND to discover which telephone numbers are associated with that address.
	Telephone Based emergency warning system (EWS)	New use from 2009. It was intended that the EWS use information in the IPND to determine which telephone numbers are associated with a particular geographic area.	The EWS uses information in the IPND as intended. Some historical problems in the IPND make it less effective for EWS purposes. For example, disconnected services are not always removed from the IPND in a timely way. This caused EWS capacity problems in sending out warnings about the chemical fire in the suburb of Mitchell in the ACT in 2011.
Non-critical users	Public number directory (PND) producers	It was intended that PND producers be able to use information in the IPND to publish public number directories, for profit.	In practice, a range of information products are produced. Regulatory changes in 2007 tightened the rules to limit PND producers to those authorised by the ACMA. Very few directory producers use the IPND data for the purpose of producing PNDs.[8]

[8] VHA submission, p.7

	Health, electoral and government research	New use from 2007. It was intended that researchers have access to information about listed numbers.	In practice, the IPND has rarely been used for research purposes. At 30 June 2014 only one entity held a research authorisation.[9] Numerous submissions requested changes to the criteria for access to enable more effective access for researchers.
	Location Dependent Carriage Services (LDCS) providers	New use from 2009. It was intended that IPND location information be used to route calls.	The IPND is used to route calls for some LDCS services from listed numbers. Other LDCS services use geographic information directly associated with a telephone number (such as the area code). With increasing use of mobile and VOIP technologies, there are fewer reliable geographic indicators in telephone numbers, which has placed greater pressure on LDCS providers to utilise the IPND.
	Directory and operator assistance (DA) services	It was intended that DA use IPND information to provide a service to end-users to find the telephone number of another end-user.	In practice, the IPND has had limited use to provide a DA service.
Administrative use	The ACMA	It was intended that the ACMA access the IPND to check industry compliance.	The ACMA accesses the IPND as intended, to carry out compliance investigations and audits.

In summary, IPND information is widely used, particularly by critical users. However, use by non-critical users, other than LDCS, is relatively limited and less widespread than originally expected.

Changing technology

Over recent years, there has been a significant increase in the number of mobile phone services and a decline in fixed line services.

[9] ACMA *Annual Report 2013-14*, p.120

In 2012, the ACMA reported that consumers were increasingly using VoIP applications that were not tied to the provider providing a carriage service and are usable from any computer accessing the internet. The ACMA reported that in the 12 months until June 2012, the total number of users of mobile VoIP increased by 133 per cent to 616,000. VoIP services via a home computer, laptop or tablet device increased by 28 per cent to 4.0 million users.[10] The following year, these numbers continued to grow with a 74 per cent increase in mobile VoIP to 1.06 million services and a 6 per cent increase (to 4.55 million) in other VoIP services.[11]

In July 2014, the ACMA estimated that the total number of adult mobile phone users without a fixed-line home phone increased by 33 per cent over the previous 12 months to more than 4.9 million, or 27 per cent of the adult population. This increase was consistent with the trend of the previous two years.[12]

Consumer expectations

A departmental study of consumer experience and expectations of the Triple Zero service in 2012 found that most consumers still expect to be able to contact the emergency services via landline or mobile phone. However, a significant minority of 20 per cent of survey participants identified VoIP, SMS or web services as possible contact methods for the emergency services.[13] The percentage would be expected to be higher in 2015 given the increase in the usage of mobile devices.

Consumers still have high, perhaps at times unrealistic, expectations about the information available to emergency services. For example, anecdotal evidence exists where young people have reportedly used social media to send a request for assistance with a mobile phone, rather than using the same mobile phone to make a direct call to the emergency call services.[14] In that case, the users had mistaken expectations about the level of integration of new technology into the emergency call services.

In contrast, there is a relatively low level of community awareness of the IPND and the way this information may be used.

Need for information by critical users

Critical users have expressed a need for continued access to customer identity and location data. However, these users have become increasingly dependent on sources other than the IPND, particularly for location information on mobile services. If current trends continue, the IPND will become much less useful for these critical users, and users and industry may become increasingly reliant on these other sources of information which are not coordinated with the IPND.

However, it is not clear that this in itself is a problem. For example, industry and emergency services have been working to develop an automated system for mobile phone location called 'push MoLI'.

---

[10] ACMA *Communications Report 2011-12*, pp.14-15

[11] ACMA *Communications Report 2012-13*, p. 4

[12] ACMA *Communications Report 2013-14*, p.14

[13] Former Department of Broadband, Communications and the Digital Economy 'Triple Zero Research Study,' June 2012

[14] VHA submission p.4

This system can be used by critical users to assist in providing an emergency response and could work in parallel with the information obtained from the IPND.

Need for information by non-critical users

Non-critical users of IPND information provide a range of services and products to government, subscribers and the general public that would not be possible, or be much more difficult, without a system like the IPND. Except in the case of the LDCS, non-critical users have not used the IPND as much as would have been expected. But changes in consumer choices and reliance on mobiles have meant that there has been a growing level of interest in gaining access to the IPND, as well as interest in gaining access to a wider range of information than is currently available.

Finding

The IPND is used regularly, particularly by critical users to support emergency services and conduct investigations of serious crime. Critical Users have indicated an ongoing need for a system that contains information about telephone service subscribers and their locations.

Quality and Accuracy of the IPND

This section discusses the quality and accuracy of IPND information and considers how this could be enhanced.

The issues

The IPND is only as helpful as it is accurate, and there are potentially life-threatening consequences if information is incorrect.

Different types of organisations have varying levels of interest in the accuracy of different types of data. For instance, emergency services are more concerned about location of a caller, while law enforcement and national security bodies generally have a requirement for accurate identity information.

Only a minority of subscribers are aware that their information is included in the IPND or of the reliance of emergency services on its accuracy.

Views of stakeholders

A number of respondents to the IPND review's discussion paper expressed significant concern at the level of accuracy in the IPND. There were also concerns about the apparent lack of incentive for the IPND manager to confirm the accuracy of information, and for CSPs to provide accurate information.

Submissions acknowledged that the accuracy of IPND data is important for delivering critical services. For example, the NSW Police Force's submission stated:

> The NSW Police Force has previously written to the ACMA relating to a high profile case where the IPND contained inaccurate information. The victim in this case died while police were attempting to accurately locate the unit the victim was calling from. The IPND address only provided the street address, not the unit block or unit number. It took attending police 45 minutes to locate the actual location, during which time the victim had leaped from her balcony.[15]

The NSW Police Force submission noted that - in this case - the ACMA subsequently took action against the CSP involved in passing on inaccurate information to the IPND. Fortunately, such incidents are extremely rare.

Inaccurate IPND information has been also shown to reduce the effectiveness of the Emergency Warning System (EWS). In 2011, a telephone emergency warning was issued in response to a chemical explosion in Mitchell, in northern Canberra. The EWS system dialled telephone numbers from the IPND that were listed as connected but, in fact, many were disconnected and invalid.

[15] NSW Police Force submission, p.2

Indeed many of the telephone numbers were only 7 or 8 digits long which indicated they had not been active for several years. The result was that the emergency warning was not able to run its course, and some connected numbers were not able to be dialled in a timely way.[16] This, amongst other problems, reduced the effectiveness of the emergency warning in that instance.

Obligations of CSPs

CSPs are obliged to provide accurate information to the IPND, and make reasonable efforts to ensure that it remains up to date. All CSPs that supply a carriage service to an end-user with a 'public number' are required to provide information to the IPND manager as part of the standard service provider rules in the Telecommunications Act.[17] In addition, CSPs that supply an emergency telephone service have additional obligations under Part 4 of the Telecommunications (Emergency Call Service) Determination 2009 (the emergency call service determination). For example, sub-clause 43(a) provides that a CSP that supplies an emergency telephone service to a customer must make arrangements to ensure that information initially received by the IPND manager is kept as up to date as practicable. In addition, sub-clause 43(b) provides that, if the CSP becomes aware that the information is out of date, it must ensure that the IPND manager receives revised information by the end of the next business day.

CSPs are also obliged to follow the industry code for IPND data transfers. This code recommends (but does not require) the use of data validation software.[18] Once information is provided to the IPND manager, the data is checked for compatibility and may be returned to the CSP if this is found to be non-compliant. However, with a database of 64.8 million records, there are challenges in verifying the accuracy of all the information supplied.

Testing accuracy

The ACMA is responsible for enforcing the standard service provider rules and the emergency call service determination. The ACMA has undertaken a range of enforcement activities to ensure that CSPs are complying with their obligations. In addition, the ACMA currently conducts periodic audits of the IPND by testing IPND data against the Geocoded National Address File, an index of physical addresses collated from state authorities.[19] This process enables the ACMA to test whether the addresses in the IPND are valid and exist in order to assess how useable the address information in the IPND was for emergency dispatch purposes.

The last full audit of the IPND was undertaken in 2009 and found that 83.9% of the IPND data was highly accurate for emergency dispatch purposes while 96.3% was considered to be of good useability. The ACMA has subsequently undertaken a program of IPND compliance investigations into providers with poor audit histories. For instance, in 2011-12, the ACMA tested the compliance of 25 CSPs with the IPND requirements and found that, while the majority had 95 per cent or greater

[16] ACT Governments 'Use of Emergency Alert during the Mitchell Hazardous Material Fire' available at http://esa.act.gov.au/wp-content/uploads/Report-on-the-use-of-EMERGENCY-ALERT-for-Mitchell-fire-September-20111.pdf

[17] Subclause 10(2) of the standard service provider rules in schedule 2 of the Telecommunications Act

[18] Communications Alliance *Integrated Public Number Database (IPND) Industry Code ACIF C555:2008*, 5.12

[19] http://www.psma.com.au/?product=g-naf

accuracy, one CSP was formally warned for its non-compliance.[20] The ACMA can issue sanctions against CSPs for non-compliance.

IPND accuracy study

The ACMA's audit process has proved to be a valuable way to determine the validity of data entered by CSPs, but it only looks at service address information, and cannot test whether a subscriber actually resides at the listed address. This is because the ACMA audits are designed to test the usability of the data for the purpose of emergency dispatch.

To gain a better understanding of the overall quality of information in the IPND, in 2012, the Department engaged Woolcott Research Pty Ltd (Woolcott) to conduct a survey of 3,000 subscribers. This survey was designed to check the information that subscribers provided to Woolcott against the relevant IPND listing. The survey was stratified to ensure that statistically reliable results were obtained from metropolitan and non-metropolitan locations, from landlines and mobile services and from residential and business subscribers.

The accuracy study's findings

The IPND accuracy study found that only 24 per cent of IPND records had completely accurate directory address and name information. However, one of the key errors encountered was in relation to first names because a large proportion of this information appeared in the surname field. While this is technically an error (and could prove problematic for searches done to the database), this information is still available and arguably still usable for the purpose of dispatching emergency services. Without this error, the accuracy of name and directory address information was 71 per cent.

Businesses and mobile entries were both found to have higher percentage of entries that were either highly accurate or highly inaccurate. That is, business and mobile entries were more likely to have accurate name information, but when it was incorrect, it was more likely to have more serious errors. Interestingly, residential mobile entries had the *highest* accuracy out of all the tested cohorts but, it should be noted, the sample was drawn from the relatively small number of listed mobile services. In the case of residential land line entries, many residential and landline entries had first name information entered into the surname field.

Overall, the directory address field was accurate for 84 per cent of records. Approximately one in six records contained incorrect or missing information that would limit its usability for the production of directory products, the routing of calls for LDCS or for research.

The study found only 34 per cent of respondents indicated that they were aware that their telephone company provided details to a database that is used for the Triple Zero emergency call service and the national emergency warning system.

[20] ACMA *Communications Report 2011-2012*, p.68

People's awareness of the IPND had no perceptible impact on the likelihood of their record being accurate. This may be because, even where a subscriber is aware of the importance of the IPND, there is no straightforward way for them to improve the accuracy of their own records.

Full results of the study are in Appendix 4.

Accuracy of the IPND compared to other similar databases

The Department attempted to compare the results of this study with other similar Australian-based and international databases but had only limited success.

There is significant anecdotal evidence that the accuracy of the IPND is poor compared to the White Pages®, the most similar data set. Advice from Sensis, the publisher of the White Pages®, suggests that this is chiefly in relation to business listings, where Sensis makes considerable effort to improve the quality of data it receives from CSPs. However, the Department was not able to identify any quantitative analysis of the accuracy of the White Pages®.

Another example is the WHOIS database which provides the contact details of the licensees of internet address resources, such as IP addresses or domain names. This allows contact to be made with licensees for a range of circumstances, including for the enforcement of laws and intellectual property rights. The Internet Corporation for Assigned Names and Numbers (ICANN) is the international organisation responsible for the WHOIS database for the global generic top level domains (gTLDs) such as '.com', and '.net'. WHOIS includes the name of the domain name owner, the address, the email and telephone of the domain name owner. In 2010, ICANN conducted an accuracy study of the WHOIS in the gTLDs.[21] That study was able to validate the address details for 92.2 per cent of the sample on at least one of the criteria established in the study, although the rate of complete accuracy in all of data fields was significantly lower. It is worth noting that, while this public database is used to provide information to law enforcement agencies to conduct investigations, it is not relied on for the delivery of emergency services and there are fewer incentives and regulatory pressures for registrants to provide accurate and current information. Despite these difficulties, ICANN's WHOIS accuracy study demonstrated a similar level of accuracy to the IPND.

Reasons for inaccuracy

No static database or data set can ever be completely accurate, especially one comprising some 64.8 million records. In the IPND context, reasons why data may be inaccurate include:

- **Subscriber update error:** A subscriber may not always update their information with a CSP. For instance, when a mobile service subscriber who receives bills via email moves house, they may not advise the CSP.
- **False information:** A subscriber could provide false information to their CSP intentionally.
- **Time lag:** There can be a time lag between a CSP receiving an update from a subscriber and uploading information in the IPND. The prevalence of this error was measured in the IPND

[21] ICANN *Draft Report for the Study of the Accuracy of WHOIS Registrant Contact Information* www.icann.org/en/compliance/reports/whois-accuracy-study-17jan10-en.pdf

accuracy study, but is not distinguishable from other errors. However, upload statistics to the IPND indicate that data providers tend to update information in large blocks rather than more regular smaller blocks.

- **Change error:** A CSP might enter information that is different to the information provided by the subscriber. For example, a customer may advise their CSP of their unit and street address, but the CSP might only supply the street address to the IPND. The prevalence of this error was measured in the IPND accuracy study, but is not distinguishable from other errors.

The data elements subject to these various types of accuracy errors are summarised in the table below

Table 3 – Accuracy errors for IPND data elements and possible reasons

Data element	Subscriber update error	False information	Time lag	Change error
Telephone number	No	No	Yes	Unlikely
Identity information (e.g. name, address and telephone number.)	Yes	Yes	Yes	Yes
Service address	No, except for mobile services	No, except for mobile services	Yes	Yes
Directory address	Yes	Yes	Yes	Yes
Information about the type of subscriber (e.g. business etc.).	Yes	Yes	Yes	Yes
Name of CSP	No	No	Yes	Yes
Information about whether the service is fixed or mobile/nomadic	No	No	Yes	Yes
Listing status	No	No	Yes	Yes

Options to improve accuracy of the IPND

The results of the IPND accuracy study suggest that the accuracy of the IPND could be improved – this would make the data more useable, particularly by critical users.

There are a number of options that could enhance accuracy of the system over the longer term. These include:

1) checking the accuracy of data already in the IPND
2) enhanced feedback loops
3) access to records by individual subscribers
4) enhanced awareness-raising measures.

Checking the accuracy of current IPND data

As noted above, anecdotal evidence suggests that the address information in the White Pages® is more accurate than the information in the IPND. This is likely to be because of the fact that subscribers can access the White Pages® easily, and can quickly take action if their contact information is not accurate.

One option to improve the information in the IPND about listed fixed and VoIP records in the immediate future would be to compare or 'wash' the IPND address information against the White Pages® (or similar) product and note the discrepancies. Where a difference is found, the CSP responsible for the record should be notified, the subscriber contacted by the CSP for any update, and a correction made to the IPND record if necessary. If there is no subsequent change in an IPND record, the ACMA would be able to use this information to then conduct targeted compliance and enforcement action against CSPs that have not provided updated records. This process would not however assist with checking information about unlisted or 'silent' numbers which are not included in the White Pages®.

Existing databases could also be used to determine whether the telephone numbers listed in the IPND are valid. The ACMA operates an online, freely accessible database known as 'NUMB' that lists the blocks of telephone numbers that have been assigned under the numbering plan.[22] For a number to be valid it must fall within one of the blocks of numbers within NUMB. There are two possibilities:

- the IPND could be washed against NUMB to highlight numbers that are invalid for correction by the CSP and enforcement action by ACMA (if needed); and
- entries uploaded into the IPND by CSPs could be automatically checked against NUMB and only accepted if they are valid numbers. This would ensure that invalid numbers were not entered into the IPND, and would have a secondary benefit in enforcing parts of the Numbering Plan on an ongoing basis.

This option would impose significant additional costs on the IPND manager which would need to be recovered somehow, either from data users in the form of increased access fees or provided by Government. Neither of these options seems entirely practicable.

In comments on the draft recommendations, Telstra suggested that it could be empowered to undertake 'operational maintenance' of the IPND in certain circumstances. This might include, for instance, where it is clear particular numbers are no longer in use such as a particular CSP no longer offering services and the numbers allocated to it have not been reassigned or where changes to the numbering plan have made numbers obsolete. This solution is likely to be a lower cost option for improving the accuracy of data already in the IPND, but the circumstances in which such maintenance would occur need to be developed with care and the agreement of industry, including Telstra as the manager of the IPND.

[22] http://www.acma.gov.au/Industry/Telco/Numbering/Managing-numbers/online-numbering-system-managing-numbers-i-acma.

Enhanced feedback loops

Telstra, as the IPND manager, has implemented a data feedback loop into the IPND that provides a mechanism for data users to provide feedback on the quality of records. Data users can lodge a data user query file (DUQF) with the IPND manager that flags that particular IPND records are incorrect. Telstra noted that the process to lodge a DUQF is complex, which has contributed to its low level of usage. Those data users who acquire information from the IPND via encrypted disc do not appear to be able to lodge DUQFs. Once a DUQF has been received by the IPND manager, it is not clear to third party observers what the next step in the process is.

The Department understands that there are particular issues with updating information from emergency services agencies which do not use the DUQF form but instead send emails from the ECP to the IPND manager and the CSP. Telstra is currently investigating options for automating this process to improve the likelihood of updates being activated in a timely manner. In consultations, Telstra has suggested that this process could be improved by the development of a web-based interface for data users and providers.

The accuracy of the IPND would be improved if the update process was enhanced to simplify the process to lodge a query and ensure that the CSP took timely action, including advising the ACMA of any queries and corrections made.

Telstra has also proposed that statistics about the number of 'soft errors'[23] in the IPND uploads or quality issues identified by data users be published regularly. These statistics could assist the ACMA in targeting its compliance investigations. It could also assist data providers in identifying errors in their data quality so that they had incentive to investigate and resolve data quality issues rather than waiting for notification of errors through an audit. Other industry members supported strengthening the feedback loop between the data provider and the IPND manager. VHA and Optus suggested that more information about the type of error code should also be provided to data providers rather than simply the number of errors so the reasons for the error can be investigated.

Access to records by individual subscribers

If individuals could see and, if necessary, correct information about their own telecommunications services in the IPND, it is likely to be more accurate. However, there are currently legislative and operational barriers to this occurring.

As will be described in more detail in the Security and Privacy section of this report, Part 13 of the Telecommunications Act imposes limitations on the disclosure of information in the IPND. Section 289 of the Telecommunications Act provides that a disclosure of information about listed entries is not prohibited if it is done with the knowledge and consent of the person concerned (that is, the telecommunications subscriber).

[23] An example of a soft error is when a first name appears in a surname field. While this is technically an error (and could prove problematic for searches done to the database), this information is still available and arguably still usable for the purpose of dispatching emergency services.

Theoretically, subscribers can seek access to their own record held by their CSP or by the IPND manager through this provision. However, there is an important limitation on the use of the exception in Section 289. Section 289 (like all of division 3 of Part 13 to the Telecommunications Act) operates as an exception to the primary disclosure/use offences established in Division 2 of Part 13.[24] In other words, CSPs can rely on section 289 in providing access to a subscriber as an exception to the Division 2 offences, but they are not obliged to provide access.

There are also practical difficulties for subscribers seeking access to their own records. One submission to the IPND review discussion paper from an individual subscriber noted that they had sought their IPND record from their CSP and from the IPND manager, but had been refused on both counts.[25] The subscriber then approached the ACMA which was able to facilitate access. Another subscriber making a submission to the review was unable to gain access and update his IPND record, noting his concerns that the information provided to the CSP did not reflect the information provided to the IPND manager.[26]

One submission argued that CSP customer service representatives were generally unaware of the IPND, and were not aware of the role that carriage service providers play in providing customer data to the IPND.[27]

A subscriber may only discover a potential problem when a critical service is not able to locate them in an emergency or when they are alerted to an inaccuracy or the publication of an unlisted number in a public number directory. Many critical users supported access by a subscriber to their own record as 'read only' access would have a positive impact on accuracy.

A number of submissions argued that subscribers should be able to view and correct their own entry directly with the IPND manager. The Office of the Australian Information Commission (OAIC) considered that allowing subscribers access to their own records would be consistent with National Privacy Principle 6 in the *Privacy Act 1988*.[28] OAIC supported the use of identity verification measures to ensure that the person seeking access was the actual subscriber. ACCAN and the Australian Privacy Foundation (APF) also supported access by subscribers subject to strong identity verification processes.[29] VHA suggested that subscribers have access to their own IPND record to allow validation, and should contact their CSP if there was an error.[30] Optus argued that allowing subscribers to access their own records has the potential to increase accuracy, and allowing a user to update it would potentially improve the speed to update a record. Optus also noted that alternatives exist, such as allowing the subscriber to provide data directly to the IPND manager.[31]

---

[24] Section 276, 277 and 278 prohibit primary disclosure of certain information by specified people (including CSPs)

[25] Confidential submission by individual subscriber

[26] Mr Arthur Marsh submission

[27] The Local Phone Books Company submission, p.4

[28] OAIC submission, p.11. On 12 March 2014, In the Privacy Act, the NPPs were replaced with the APPs. The APP12 relating to access to personal information is the equivalent of the repealed NPP 6.

[29] ACCAN submission p.12, APF submission, p.13

[30] VHA submission, p.17

[31] Optus submission, p.3

Telstra supported access by individual subscribers to their own records in principle, but also noted that the costs of the system would need to be assessed and appropriate identity verification procedures would need to be developed[32]. The Commonwealth Attorney-General's Department supported access by a subscriber to their own record, and noted that a system the Department was developing at the time called the Document Verification Service (DVS) could be a quick and cost-effective way to verify common identity documents[33]. The DVS was launched in May 2014.

One critical user group was concerned that allowing access by subscribers to their own records (and especially giving subscribers 'write' access) could facilitate fraud and identity theft[34]. Acceleon, a public number directory producer, also did not support access by subscribers[35], and Telstra argued that allowing subscribers to amend information directly could create risks of inappropriate and fraudulent data and raise data accuracy, security and data integrity issues.

In the medium term, a protocol could be developed by the IPND manager to allow access by a subscriber if sufficient levels of identity documents are submitted (for example 100 points of identification). In the longer term, an easy-to-use web portal could be developed. Subject to appropriate screening processes, subscribers could access the web portal to see and flag their records for update.

At present, there is no simple or effective way that a subscriber can access their own IPND record. On balance, it appears that allowing subscribers to see their own records, and request necessary updates through appropriate channels, could have a positive impact on the accuracy of the IPND. The medium- to long-term options would need further consideration.

Enhanced awareness raising measures

CSPs are currently obliged to alert their subscribers about the IPND's existence[36]. Industry participants have interpreted this obligation in a range of ways. In many cases, they provide information about the IPND in their standard form contracts.

The IPND accuracy study has shown that awareness does not generally have a positive impact on accuracy. It is suggested that this is because, even if a subscriber is aware of the importance of accurate IPND information, the mechanisms for them to update their information are not effective.

Generally speaking, CSPs have an interest in ensuring that their customers provide accurate information. Current industry communication practices could be used fairly readily to inform subscribers of the information that their CSP holds about them, and provide a timely prompt for subscribers to update their information regularly. For example:

- CSPs could include the customers' IPND-related information on any invoices issued and suggest it be updated if necessary.
- CSPs could include information at the time of contact on the reasons why it is in a subscribers' best interest to provide accurate and up-to-date information.

[32] Telstra submission, p.20
[33] Attorney General's Department submission, p.2
[34] NECWG-A/NZ submission (duplicated in the NSW Police submission)
[35] Acceleon submission, p 10; Telstra submission, p.20
[36] Communications Alliance Integrated Public Number Database (IPND) Industry code ACIF C555:2008, p.15

Industry members also suggested that there is a role for Government, including the ACMA and the emergency services in raising public awareness of the IPND.

The Department makes the following recommendations in relation to the Quality and Accuracy of the IPND:

Recommendation 1

The quality and accuracy of data in the IPND should be improved by:

- enhancing the existing feedback processes between the IPND manager, data providers and data users, including by exploring improved automated processes and ensuring changes are made in a timely way, and
- industry working to improve the quality of information in the next review of the IPND code, such as by requiring that all data providers use validation software.

Recommendation 2

The regulatory arrangements should be amended to ensure subscribers can:

- be provided with the information in the IPND relating to themselves, and
- flag incorrect information for action by CSPs in a specified timeframe.

Recommendation 3

In order to raise awareness of the IPND, CSPs should:

- alert their subscribers of their IPND information, and
- advise subscribers regularly of the importance of providing correct information.

Security and Privacy

This section discusses the privacy implications of the IPND, including the appropriate protection of personal information and the circumstances in which information should be used and disclosed.

Why protect information?

Under the Privacy Act, information about an identified individual or an individual who is reasonably identifiable, is defined as 'personal information'.[37] This includes the type of information in an IPND entry such as name, telephone number and address information of an individual.

Most government agencies, businesses with an annual turnover of $3,000,000 or more and some small businesses are subject to the Privacy Act and are obliged to collect, protect, use and disclose such information in accordance with guiding principles set out in that Act which include:

- ensuring personal information is only collected if necessary and that individuals are advised it has been collected and the uses to which it will be put[38]
- ensuring that personal information which is unsolicited is afforded the same protection as solicited information[39]
- limiting how individuals' personal information may be used and disclosed - if certain conditions are met, an organisation does not always need an individual's consent to use and disclose personal information[40]
- requiring an organisation to take steps to ensure the personal information it holds is accurate and up-to-date, and is kept secure from unauthorised use or access[41]
- giving individuals a general right of access to their personal information, and the right to have that information corrected if it is inaccurate, incomplete or out-of-date.[42]

The IPND affects the privacy of individuals because information about individual telecommunications subscribers is acquired compulsorily. Subscribers do not have a choice as to whether the information they provide to their CSPs is stored in the IPND. They do, however, have some control over its disclosure. By choosing to have an unlisted or 'silent number', they are able to prevent the disclosure of their information to non-critical users.

As shown in the IPND accuracy study, consumer awareness of the IPND is relatively low, despite current awareness-raising activities. Even if a consumer was aware that their information was stored in the IPND, they would not necessarily be aware of which organisations have access or consent to access of that information.

[37] Section 6 *Privacy Act 1988*

[38] Australian Privacy Principle 3 (APP3) and APP 5).

[39] APP 4

[40] APP6 and APP7

[41] APP 10 and APP 11

[42] APP12 and APP13

As the information in the IPND covers the entire telecommunications industry and contains personal information in tens of millions of individual records, there is a need to ensure that there are appropriate privacy protections in place.

Use and disclosure

The ALRC review of privacy laws recommended that the Telecommunications Act be amended to clarify when a use or disclosure of information or a document held on the IPND is permitted.[43]

Use and disclosure of information in the IPND occurs through Part 13 of the Telecommunications Act and a range of legislative mechanisms. One important difference between the Telecommunications Act and the Privacy Act is that the Telecommunications Act covers all Carriers and CSPs (and telecommunications contractors), not just those with a turnover of $3,000,000 or more.

Division 2 of Part 13 of the Telecommunications Act sets out broad prohibitions on the primary disclosure or use of information that CSPs might provide to the IPND manager and that the IPND manager provides to IPND users.[44] Division 3 of Part 13 to the Telecommunications Act then provides a broad range of exceptions to the prohibitions, of which the following are relevant to the IPND:

- As part of performance of one's duties (such as when CSPs pass information to other CSPs and carriers to route communications or to operate the emergency call service) (s279).
- Where a law enforcement agency has a warrant for its use or disclosure, or as authorised by or under law (s280).
- To assist the ACMA, the Telecommunications Industry Ombudsman (TIO), the Australian Competition and Consumer Commission (ACCC) or the Telecommunications Universal Service Management Agency (TUSMA) (s284).
- The exemptions specifically provided in relation to IPND (s285), which include:
    - to provide directory assistance services by or on behalf of a CSP
    - to maintain and publish a public number directory (if also authorised under the IPND Scheme by the ACMA) which contains the names of people and bodies and their telephone numbers
    - to conduct research of a kind specified by the Minister (if also authorised under the IPND Scheme). To date, three kinds of research have been specified:
        - public health (including epidemiological) research, where the research is not conducted for a primarily commercial purpose

[43] ALRC Review Recommendation 72-11, p.2459

[44] Sections 276-278 of the Telecommunications Act

- electoral research (not conducted for a primarily commercial purpose) by a registered political party, a candidate in a Parliament or local government authority, or a person on behalf of such a party, representative or candidate

- government research which will contribute to the development of public policy, (not conducted for a primarily commercial purpose) by or on behalf of the Commonwealth, a Commonwealth Authority or a prescribed agency for the purposes of the *Public Governance, Performance and Accountability Act 2013.* [45]

- To provide telephone-based emergency warnings (s285A).
- To allow the Emergency Call Person to disclose information to the emergency service organisations (s286).
- To prevent an imminent threat to human life or safety (to enable information about unlisted numbers to be provided to the emergency call service) (s287).
- disclosure with the knowledge and consent of the person concerned (s289).
- To enable the supply of carriage services (s291).
- To provide LDCS (s291A).
- In circumstances to be prescribed in regulations (s292).

Division 4 of Part 13 to the Telecommunications Act regulates the secondary use and disclosure of protected information. That is, persons permitted to receive information under Part 13 are prohibited from using the information they have received for purposes other than those for which the information was given.

Part 14 of the Telecommunications Act sets certain conditions and obligations on the disclosure of information to enforce the criminal law, impose pecuniary penalties, protect public revenue and safeguard national security.

Law enforcement and national security agencies must also meet the broader requirements of the *Telecommunications (Interception and Access) Act 1979* (TIA Act). The requirements of the TIA Act are outside the scope of this review.

[45] Telecommunications (Integrated Public Number Database – Permitted Research Purposes) Instrument 2007 (No 1)

ALRC review

The ALRC review of privacy law considered whether the IPND should be regulated under the Privacy Act rather than the Telecommunications Act. The Department argued, as part of that review, that a number of disclosures of information to allow the operation of the telecommunications industry and for public safety would no longer be possible if the Privacy Act applied. Conversely, if the APPs in the Privacy Act were applicable to the IPND, disclosure of information for direct marketing purposes would be possible in certain circumstances. The ALRC concluded that the IPND should continue to be regulated under the Telecommunications Act rather than the Privacy Act, as this provided an appropriate level of protection of IPND information.[46]

However, the ALRC noted that it was unclear which of the exceptions in Part 13 (other than section 285) applied to the IPND data. In particular, the ALRC expressed concern about the broad-ranging power to disclose under the exception in subsection 289(b)(i), which specifies that disclosure could occur if a person 'is reasonably likely to have been aware or made aware that information or a document of that kind is usually disclosed, or used, as the case requires, in the circumstances concerned'.[47]

Telstra's carrier licence limits the purposes for which information in the IPND can be used and disclosed. The ALRC also noted it was unclear how the exceptions in Part 13 interact with Telstra's carrier licence conditions.

The ALRC recommended that the Telecommunications Act be amended to clarify when the use or disclosure of information or a document held on the IPND is permitted.[48]

Views of stakeholders

A number of submitters to the IPND review discussion paper suggested that the legislative access controls for the IPND should be clarified. For example, the OAIC argued that the exceptions under Part 13 of the Telecommunications Act should be removed and that access to IPND information should either be governed more generally under former NPP 2 (new APP6 and APP7) of the Privacy Act, or that the exceptions be aligned with the Privacy Act.[49] ACCAN suggested that all of the regulatory instruments should be aligned so that they are consistent.[50]

Who should have access?

Key questions about the disclosure of data from the IPND include which types of user should have access to which data and who should determine this.

---

[46] ALRC Review p.2457. Note that from March 2014, the new APPs replaced the NPPs.

[47] *ibid* p.2458

[48] *ibid*, Recommendation 72-11, p.2459

[49] OAIC submission, p.5. Note that from 12 March 2014, NPPs were replaced by the APPs, and the equivalent of NPP2 is APP6 and APP7

[50] ACCAN submission p.8

Currently, different categories of users of IPND information have access to different levels of information.[51] Critical users have higher levels of access than non-critical users and researchers have the least. No non-critical user has access to unlisted numbers under the current arrangements and, as the ALRC noted, it is not clear that unlisted numbers can be disclosed to another person to deal with matters raised by a call to an emergency service number.[52]

The chief 'cost' in allowing access for non-critical uses is the potential impact on the privacy of subscribers. It is recognised that the public interest in allowing access must be balanced against the public interest in protecting the privacy of subscribers. In many cases, allowing non-critical users to access aggregated or depersonalised information may have no practical privacy impact at all. In other cases, the privacy impact of access could be offset by providing an effective option for subscribers to 'opt-out' of their information being provided to non-critical users (by, for example, choosing to have an unlisted entry).

Ideally, the rules for access should be consistent, both at the macro level (in terms of deciding which categories of non-critical users should be allowed) and at the micro level (in terms of deciding in a practical sense which particular non-critical user can access which data elements).

Views of stakeholders

Submissions to the IPND Review discussion paper generally agreed that organisations accessing the IPND should only have access to the information that they require to offer their services effectively.

During the 2012 stakeholder Workshop, participants supported the continued access to IPND data by critical users but considered that there should still be some form of scrutiny on access by those organisations. Many submissions supported the current access arrangements for critical users. However, the APF argued that critical users should only gain access to the data elements they 'proportionally' require to provide their services:

> [w]e recognise that some information which may not be necessary for one of the critical purposes … may however be necessary for another critical purpose…. 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.[53]

Access for critical users

The IPND was developed to support the continued operation of critical users in a competitive telecommunications environment. The following table outlines the data elements accessible by each category of critical user and the policy rationale permitting access.

[51] *IPND Review Discussion Paper*, p.8

[52] ALRC Review recommendation 72-13, p.2461

[53] APF submission, p.6

Table 4 - Requirements of types of critical user for particular IPND data elements

Data Element/ Category of critical user	Law Enforcement and National Security Agencies	Emergency Call Services	Emergency Warning Systems
Telephone number	Required. Enables agencies to connect a telephone number to a subscriber or location to facilitate an investigation.	Required. Enables the ECS to connect the Calling Line Identification (CLI) for an incoming call to other subscriber details (most notably location information).	Required. Enables the EWS to determine which telephone numbers are likely to be in a location affected by an emergency.
Identity information (e.g. name)	Required. Identity information is a key data element used by agencies to progress an investigation.	Required. Identity information is useful to ECS to enable the appropriate service to be dispatched and also enables the investigation of non-emergency calls.	Not required.
Service address of telephone subscriber	Required. Used as a proxy for the actual location of a subscriber/caller, facilitate investigations and enables an emergency response if required.	Required. Used as a proxy for the actual location of a subscriber/caller and enables efficient dispatch of emergency services.	Required. Used as a proxy for the actual location of a subscriber/caller and is used to determine which telephone numbers are likely to be a location affected by an emergency.
Directory address of telephone subscriber	Required. Provides useful information to agencies about the reported address of a subscriber.	Not required. Service address is used instead.	Not required. Service address is used instead.
Receives information about unlisted numbers	Required. Critical users need to provide services to all users on the telecommunications network.	Required. Critical users need to provide services to all users on the telecommunications network.	Required. Critical users need to provide services to all users on the telecommunications network.
Information about the type of subscriber (e.g. business etc.). This is an optional data element.	Required. Provides useful information about how a service is reported to be used.	Required. Provides useful information to the ECS when dispatching services.	Required. Provides useful information to the EWS about the kind of messaging to send.
Prior public number	Required. Enables agencies to connect a subscriber to a prior service address or number.	Not required.	Not required.
Name of CSP	Required. Enables the agency to contact the CSP for further assistance.	Required. Enables the ECS to contact the CSP for further assistance.	Required. Enables the EWS to contact the CSP for further assistance.
Information about whether the service is fixed or mobile/nomadic	Required. Enables agencies to determine the type of service, and the limitations of the information they have about the service (e.g.	Required. Enables the ECS to query nomadic callers about their actual location.	Required. Enables the EWS to determine the limitations of the service and determine appropriate messaging

	a mobile service may not be at the service address).		(i.e. to send SMS to mobile services etc.).

The critical users that can access various data elements is currently determined by Telstra's Technical standard and the IPND code. While this has been an effective mechanism to date, these documents are determined by industry in consultation with critical users. There has been no formal consideration of the privacy impact of allowing access to a particular data element, and this information is not widely available to the public. It may be more appropriate for the rules about which data elements can be accessed by which critical users to be more generally known.

Access for non-critical users

In certain circumstances, it is appropriate for information collected for critical users to be disclosed to non-critical users. This section discusses the key questions of the process for gaining access, whether access to unlisted numbers should be available to non-critical users and whether the rules for public number directories remain appropriate.

Who should decide?

Certain types of non-critical user of IPND data seek access directly from the IPND manager but researchers and public number directory producers must first seek an authorisation from the ACMA under the IPND Scheme.

Telstra questioned whether the arrangement of having multiple decision-makers for access to the IPND was effective and considered that it would be more appropriate if the ACMA had a comprehensive role in assessing access by all organisations. It argued:

> it would be more appropriate for the ACMA (as an independent industry regulator) to authorise all IPND users' access to the IPND. This would help ensure that the operational aspects of the IPND management can be left to the IPND Manager and remove any potential perceptions of conflicts.[54]

Telstra suggested that this could be resolved if all types of access for non-critical users was sought from the ACMA.

However, as the types on non-critical users able to seek access to the IPND are CSPs performing Directory Assistance and LDCS, these services are well-established and clearly defined. Telstra's proposal would add a regulatory hurdle to the entry of new service providers which seems to offer limited benefit.

Unlisted numbers

Non-critical users currently do not have access to information about unlisted numbers in the IPND. Having an unlisted number is therefore an important tool that allows subscribers to protect their information.

[54] Telstra submission p.7

An 'unlisted number' is defined in Telstra's carrier licence conditions as a public number that is one of the following:

a) a mobile number, unless the customer and the carriage service provider that provides the mobile service to the customer agree that the number will be listed;
b) a geographic number that the customer and the carriage service provider that provides services for originating or terminating carriage services to the customer agree will not be included in the directory;
c) the number of a public payphone;
d) a number that when dialled, gives access to a private telephone exchange extension that the customer has requested not be included in the directory.[55]

In practical terms, an unlisted number has three effects:

1. Unlisted numbers are not permitted to be listed in the White Pages®.[56]
2. Calling Line Identification (CLI) must not be passed on to call recipients.[57]
3. Unlisted numbers are not permitted to be passed on to the following IPND users when accessing the IPND:
   a. researchers.
   b. LDCS providers.
   c. public number directory producers, or
   d. directory assistance providers.[58]

Subscribers with unlisted numbers cannot select which non-critical services to opt out of; rather, by obtaining an unlisted number, they opt out of them all.

Unlisted on category by category basis

The IPND review discussion paper sought views from stakeholders on whether subscribers should be allowed to opt out of having their IPND information accessed by non-critical IPND users on a category by category basis.[59] For example, a customer might not want researchers to gain access but might see a practical benefit in LDCS providers having access.

In responding to this question, most submitters commented on the cost of communicating a listing preference with their CSP. The ALRC Review recommended that the Telecommunications Act be amended to prohibit the charging of a fee for an unlisted number in a public number directory.[60] This recommendation relates to a listing in the White Pages® for which there is a charge, rather than in the IPND for which no CSP currently makes a charge.

[55] Clause 3 of Telstra's CLCs

[56] Sub-clause 9(7) of Telstra's CLC

[57] ACIF Code C522:2007, Calling Number Display

[58] Subsections 285(1) and 285(1A) of the Telecommunications Act. Note that information relating to an unlisted number arguably may not be disclosed to the emergency call service under clause 285(1A)(c)(iii)

[59] IPND review discussion paper q.18, p.13

[60] ALRC Report Recommendation 72-17, p.2475

In practice, the ability for a customer to alter their listing preference for IPND purposes rather than for the White Pages® is quite limited because of the relatively low level of awareness of the role of the IPND. It is unlikely that most subscribers would have sufficient awareness to know that an unlisted entry in the IPND protected their information from certain categories of IPND data users, and that they could request an unlisted IPND entry from their CSP for no cost.

Given that providing information to the IPND is mandatory, an unlisted entry is one of the most important ways that a subscriber can protect their information from disclosure to non-critical users. It is noted that not all CSPs have the business processes for a subscriber to express their choice of whether their IPND entry should be considered listed or unlisted as opposed to a listing in the White Pages® directory.

Privacy and consumer stakeholders generally argued that subscribers should have an effective option to 'opt-out' of their IPND records being accessed by non-critical data users. For example the APF argued 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.[61]

Similarly, ACCAN stated:

> The IPND is essentially 'marketed' to the public as an emergency database – consumers are encouraged to provide correct and current information to their CSP specifically so that they can be found in an emergency…. Consumers should be able to opt out of having their IPND information accessed by non-critical users on a category by category basis.[62]

All of these submitters agreed that subscribers should be able to opt out of having their IPND information accessed by non-critical IPND users on a category by category basis. On the other hand, Acceleon suggested that the default position for mobile phone numbers should be that they are listed, with an option to make them unlisted.[63]

Telstra was strongly opposed to altering the approach to unlisted numbers. Its submission stated that there is no demand for a functionality in the IPND to allow subscribers to opt out on a category by category basis. Telstra noted that the inclusion of additional data fields for this purpose could create confusion given the limited public awareness of the functions of the IPND. Telstra agreed that subscribers should be able to change their listing preference in the IPND for free, independently from requests for unlisted numbers for the purposes of the White Pages® or CLI.

However, it is noted that not all CSPs have the business processes for a subscriber to express their choice of whether their IPND entry should be considered listed or unlisted. It is likely that it would add a significant level of complexity to the current data collection arrangements to require CSPs to

[61] Australian Privacy Foundation submission, p.14

[62] ACCAN submission p.13

[63] Acceleon submission, p.5

collect additional information about whether a subscriber would choose to provide information to several different categories of non-critical user.

LDCS access to unlisted numbers

LDCS are services that route calls based on the location of the callers. They are used by commercial services (for example, pizza or taxi services) to direct a call to the closest retail point, and are also used by a range of public interest services (such the State Emergency Service) to direct calls to the closest office.

Telstra noted that LDCS utilise 'full Caller Line Identification' routing to ensure that a call is connected to the correct location.[64] Where a caller uses an unlisted number to make a call through an LDCS, the call can only be routed as far as the exchange level (or 'standard zone unit'), which can be very large areas. This means that callers with unlisted numbers can experience a delay in being connected to the correct office or, in some rare cases, cannot be connected at all.[65]

Industry participants in the 2012 stakeholder workshop suggested that access to high-level location information for unlisted numbers be allowed for LDCS, to enable consumers with unlisted numbers to take advantage of these services. Such information would only be used within networks and would not be released to end-users. This would enable all subscribers to utilise LDCS services without unduly impacting on their privacy. This view was supported by the APF submission which noted that:

> [t]here is however a case for LDCS providers to have access to limited location information even for unlisted numbers…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.[66]

Likewise, ACCAN argued that:

> holders of unlisted (silent) numbers may be (unwittingly) disadvantaged in attempting to call numbers which require routing [through LDCS]… ACCAN 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.[67]

However, in subsequent discussions in 2014, ACCAN and the APF expressed concern about extending LDCS to unlisted numbers. Nevertheless, on balance, access to high level location information, rather than complete addresses, for unlisted numbers for the purpose of routing calls does appear to be in the public interest.

[64] Telstra submission, p.14
[65] INMS submission, p.2
[66] APF submission, p.7
[67] ACCAN submission, p.9

Public Number Directories

The ALRC report recommended that the Telecommunications Act be amended to provide that directory products produced from sources other than the IPND should be subject to the same rules under Part 13 of the Telecommunications Act as directory products which are produced from data sourced from the IPND.[68]

The Department understands that IPND information was utilised for identity verification purposes by some public number directory producers. In 2006, the Telecommunications Act was amended in order to prevent the use of IPND information for 'skip tracing' and identity verification. The Explanatory Statement to the amending Act noted that it inserted a definition of 'public number directory' into the Telecommunications Act:

> to prevent IPND information being used directly to produce records or databases which are used for such purposes as marketing, data cleansing and appending, debt collection, identity verification and credit checking and to limit the extent to which records which are public number directories (within the meaning of the definition in the Bill) are readily able to be used for such purposes.[69]

Rules for IPND Public Number Directories

Public number directories produced from the IPND (IPND PNDs) are subject to a range of special rules under the Telecommunications (Integrated Public Number Database - Public Number Directory Requirements) Instrument 2007 (No. 1) (the PND Instrument). These rules do not apply to public number directories that do not use the IPND as a data source (non-IPND PNDs).[70] Local Directories, a public number directory producer, made a detailed submission on the IPND Scheme and the regulatory instruments that support it. In summary, Local Directories argued:

- The electronic display requirements set out in the PND Instrument (that no more than twenty entries are transferred with a single action and that no more than 100 entries are generated from a single search) should be rationalised given the advances in anti-scraping technology.
- Electronic PNDs should not be required to be encrypted.
- PND Instrument should be clarified to indicate that any electronic display requirements only apply to IPND information in a PND, and not additional non-IPND information.
- The requirement that IPND data be kept in a database separate to the non-IPND data be removed.[71]

Acceleon also considered some of the restrictions did not suit electronic directories, noting that the requirement for the directory to be alphabetical could only apply to printed directories.[72]

---

[68] ALRC report recommendation 72-16, p. 2469

[69] Explanatory Statement to *Telecommunications Amendment (Integrated Public Number Database) Act 2007*

[70] See sub-clause 4(e), (f) and (g) of the Telecommunications (Integrated Public Number Database - Public Number Directory Requirements) Instrument 2007 (No. 1).

[71] Local Directories submission, pp.2-5. Other public number directories held similar views e.g. Acceleon submission, pp.8-9

[72] Acceleon submission, p.8.

The policy rationale for these obligations was to prevent the scraping of data from a public number directory produced using IPND data.[73] That is, these requirements are intended to prevent the large scale electronic copying of IPND data by third parties. This policy rationale is, by and large, still relevant.

However, these obligations are somewhat dated and do not recognise the advances that have been made in anti-scraping technology. Indeed, artificially limiting the number of entries which can be displayed at one time or retrieved in a single search does not, by itself, prevent scraping because multiple searches can be performed very easily. An electronic public number directory producer must also have a process to identify and ban multiple searchers from the same source.

In addition, these requirements can have unintended side-effects, such as by reducing the exposure that some businesses have to legitimate searchers and it is generally out of step with current industry practices for searches of non-IPND data. It is noted that public number directory producers utilising IPND information appear to have a strong commercial incentive to prevent scraping, and have implemented technical measures to prevent scraping as far as possible.

The PND Instrument could be amended to allow anti-scraping technology to be used instead of artificially limiting the number of entries which can be displayed at one time or retrieved in a single search. The ACMA could then determine to its satisfaction that the anti-scraping technology used by authorisation holders is providing an effective solution as a condition of approval under the Scheme. In the absence of effective anti-scraping technology, the requirements artificially limiting the number of entries which can be displayed at one time or retrieved in a single search should remain.

On the other hand, there are no compelling reasons to remove the requirement to encrypt IPND data as encryption is efficient and cost-effective as compared to the wholesale copying of an entire PND.

Sources for Public Number Directories.

There are a number of other sources of information and directories that are not subject to the same rules. For example, Telstra noted that it does not rely on the IPND to produce its White Pages® product because it has bilateral arrangements with CSPs to provide information directly to it. CSPs are under no obligation to provide information to Telstra, and Telstra has advised that CSPs are recompensed for providing this information.[74]

A number of submitters to the IPND review discussion paper agreed with the ALRC recommendation that all public number directory producers should be bound by the same rules. For example, ACCAN stated that '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.'[75] The APF suggested that there are four reasons to require this:

---

[73] Explanatory statement of the *Telecommunications (Integrated Public Number Database - Public Number Directory Requirements) Instrument 2007 (No. 1)*

[74] Telstra submission, p.11

[75] ACCAN submission, p.4

- to ensure that all [Public Number Directory Product] 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.[76]

PND producers that use the IPND had differing views. The Local Phonebook Company considered that all public number directories should be bound by the same rules and that the definition of public number directory in the Telecommunications Act should be refined to apply to the White Pages®.[77] Likewise, Acceleon argued that all public number directory producers should be required to use the IPND and that this would produce a level playing field.[78]

On the other hand, Local Directories thought that requiring all public number databases to be bound by the same rules as the IPND would needlessly inhibit innovation.[79] Telstra argued similarly:

> [C]ompetition in the market for directory services is best served by providing the choice of access to the IPND for directory producers, while also encouraging market players to innovate and provide incentives to differentiate their products.[80]

The ALRC found that the voluntary nature of non-IPND PNDs did not justify different rules to IPND PNDs. The ALRC noted that there is a lack of certainty as to which rules regulate non-IPND PNDs. In making its arguments, the ALRC focused on the White Pages® and did not consider other non-IPND PNDs, including other information products that service much the same purpose as public number directories (such as internet search engines or social networking websites).

There are three key arguments in support of the position of not requiring PND producers to derive their information from the IPND:

a) Competition is unlikely to be increased:

There is no evidence that requiring traditional public number directories to source their information from the IPND will increase competition in the directories market. In fact, the contrary could be true: requiring all directory producers to use the same data source is likely to reduce opportunity for innovation and reduce the ability of competitors to differentiate themselves.

The comparative accuracy of the IPND and White Pages® was advanced by some stakeholders as a reason to require Telstra to utilise the IPND for its White Pages® product.

---

[76] APF submission, p.9

[77] The Local Phonebook Company submission, p.6

[78] Acceleon submission, p.9

[79] Local Directories submission, p.6

[80] Telstra submission, p.12

The argument is that, if Telstra utilised the IPND, it would have greater incentives to improve the accuracy of the IPND. However, this argument confuses Telstra's role as a CSP with its role as the IPND manager. As IPND manager, Telstra has no role in promoting the accuracy of IPND information.

It may be that CSPs and consumers confuse updates of White Pages® information with updates of the IPND but this is a problem that should be addressed through enhanced enforcement measures and public awareness-raising.

The special rules regarding IPND PNDs have been seen as a barrier to competition but, as noted above, IPND data warrants special protection because it covers every subscriber, and subscribers do not necessarily consent to their information being disclosed. It is acknowledged that IPND protections should not apply to non-IPND data. Therefore, rather than apply the requirements of the instrument to all PND publishers, the protections should be limited to ensure that it only applies to IPND information.

b) Appropriate rules already apply to non-IPND information provided by CSPs:

All information disclosed or used by CSPs that relate to the personal particulars (e.g. name, address) is already protected by Part 13 of the Telecommunications Act (as well as the Privacy Act). For example, the information that CSPs disclose to Sensis to produce the White Pages® is protected information under section 276 of the Telecommunications Act. Unless an exception applies to allow disclosure, the disclosure is illegal. Section 289 of the Telecommunications Act allows disclosure where the relevant person has consented to the disclosure. It is understood that CSPs obtain consent from relevant subscribers via their standard services contracts.

c) Appropriate rules already apply to non-IPND information used for non-traditional PNDs:

A number of services are increasingly competing with traditional PNDs. For example, internet search engines and social networking sites ('non-traditional PNDs') are increasingly the means by which consumers are finding information about people and businesses. The information used and disclosed by non-traditional PNDs is not generally covered by Part 13 of the Telecommunications Act because the providers are not CSPs, carriers or other entities specified in Division 1 of Part 13 of this Act. This information may however fall under the broader privacy regime in the Privacy Act. Often information re online users is provided voluntarily and consent for disclosure is sought through a site's terms and conditions.

On balance, it does not seem to be in the public interest to require public number directory producers to source their information from the IPND.

Other ALRC recommendations about IPND

Unauthorised alteration of records

The Department understands that some CSPs may have mistakenly altered IPND records for services for which they are not responsible. This could potentially lead to inaccurate IPND information being entered on that system. While there should be technical barriers to prevent this kind of issue arising, it could be appropriate to have a regulatory solution such as provisions in an industry code or even an amendment to Part 13 of the Telecommunications Act to clarify that alteration of an IPND record by a CSP is a breach if the record does not relate to a service for which that CSP is responsible. Where a customer is moving from one provider to another there should be sufficient leeway (for

example, 24 hours) to ensure that the CSP losing the customer can still provide an update to IPND records, if necessary.

Notification of data breaches

Clause 7 of the Telecommunications (Integrated Public Number Database Scheme - Conditions for Authorisations) Determination 2007 (No. 1) requires the holder of the authorisation to notify ACMA and the IPND Manager as soon as practicable after becoming aware that a person to whom the authorisation holder has disclosed IPND information had contravened any legal restrictions on the use or disclosure of IPND information.[81]

The ALRC review recommended that this declaration be amended to provide an additional condition of a requirement to notify the Privacy Commissioner, as soon as practicable after becoming aware:

a) of a substantive or systemic breach of security that reasonably could be regarded as having an adverse impact on the integrity and confidentiality of protected information; and

b) that a person to whom the holder has disclosed protected information has contravened any legal restrictions governing the person's ability to use or disclose protected information.[82]

Given the importance of privacy matters, it seems that there would be merit in extending this requirement to all IPND data users, not just producers of public number directories and researchers.

Civil penalties

The ALRC review recommended that unauthorised disclosures under Part 13 of the Act should be subject to civil penalties as well as to criminal penalties.[83] This would enable flexibility in enforcement action as civil actions are better suited to pursuing corporate offenders than criminal penalties in some cases. The IPND review discussion paper sought views on this question as this would apply to offences for unauthorised disclosure of IPND information but, as Part 13 also covers a broader range of information than that in the IPND, this recommendation will not be addressed in this report.

Research

In Recommendation 72-14, the ALRC recommended that, before the Minister for Communications specified the types of research permissible under the IPND, the Minister must be satisfied that that the public interest in the research outweighed the public interest in maintaining the level of protection provided by the Telecommunications Act. This recommendation will be considered in the Additional Data Users section of this report.

---

[81] Telecommunications (Integrated Public Number Database Scheme— Conditions for Authorisations) Determination 2007 (No 1) clause 6

[82] ALRC report recommendation 72-15, p.2466

[83] ALRC report Recommendation 71-3, p.2401

Definition of 'enforcement agency'

The ALRC report recommended that Telstra's carrier licence conditions be amended to provide that 'enforcement agency' has the same meaning as that provided for in the TIA Act.[84] Telstra is required to provide information for purposes connected with a number of activities including assisting 'enforcement agencies'. Clause 3 of Telstra's carrier licence conditions states that *enforcement agency* has the meaning given by section 282 of the Telecommunications Act, but in 2007 this section was repealed and the relevant part was replaced by the operation of chapter 4 of the TIA Act.

The TIA Act's definition extends the definition of 'enforcement agency' to include four additional state based anti-corruption agencies which were not created at the time of the Telecommunications Act. These are:

- NSW Police Integrity Commission
- IBAC – the Victorian Independent Broad-based Anticorruption Commission
- Tasmanian Corruption and Crime Commission and
- South Australian Independent Commissioner against Corruption.[85]

As a consequence of this inconsistency, there is a risk that Telstra cannot rely on its carrier licence conditions as empowering it to provide assistance to the newer state-based anti-corruption agencies. No submissions to the IPND review commented on this ALRC recommendation but it would be consistent with the intent of the list for this recommendation to be adopted and for Telstra's carrier licence conditions to be amended to refer to section 5 of the TIA Act.

Disclosure of unlisted number for emergency services

The ALRC report recommended that section 285 of the Telecommunications Act be amended to provide that a disclosure of an unlisted number is permitted if the disclosure is made to another person for purposes connected with dealing with the matter or matters raised by a call to an emergency service number.[86]

Currently section 285 restricts the permitted use and disclosure of IPND information for the purposes of emergency calls to 'listed' numbers only. There is a general exception within Part 13 (section 287)of the Telecommunications Act which enables disclosure of information to prevent a threat to a person's life or health. However, as mentioned earlier, the ALRC has noted there is some uncertainty whether the general exceptions in Part 13 apply to the IPND. This recommendation would make clear that information relating to an unlisted number in the IPND may be used or disclosed when dealing with a matter raised by a call to an emergency service number. This recommendation received widespread support from stakeholders with no objections raised.

Finding

The IPND arrangements have not kept pace with developments in privacy legislation and changing community expectations. Review consultations suggest a public interest case for allowing some IPND

[84] ALRC Report Recommendation 72-12, p.2460

[85] TIA Act section 5

[86] ALRC report Recommendation 72-13, pp. 2460-2461

information collected to meet the needs of critical users to be available to non-critical users. Conversely, there is limited public information about which data users have access to IPND data and the processes for determining who should have that access. The Review found non-critical users are allowed access to some IPND information, however this may be limited by restrictions available to subscribers concerning whether their information is accessed or not. Options available to subscribers may however be impacted as not all CSPs have processes in place to allow a subscriber to alter their listing preference in the IPND, at no charge.

Additional data users

The IPND must innovate and keep pace with technological and market changes if it is going to continue to be a valuable data source that serves the public interest.

Likely changes in future demand

As a consolidated source of customer and location information, it is anticipated that the IPND will continue to be seen as a valuable data source by many potential users.

As most mobile phone services are categorised as 'unlisted' in the IPND, information about these subscribers is not available from the IPND to non-critical users. As noted in the Security and Privacy section of this report, there is increasing interest from current IPND users in seeing information about unlisted numbers to deliver LDCS to mobile numbers. Access to unlisted information would also help the ABS complete its surveys more cost-effectively by enabling initial contact with survey participants to be made by phone rather than in person.[87]

The research industry argued that access to de-identified mobile phone numbers with high level location information (such as postcodes) would enable the increasing proportion of households without landlines to participate in randomised telephone surveys. Among other things, this would provide higher quality information about the impact of public policies at a lower cost than is currently possible.[88]

The company responsible for delivering the National Broadband Network (NBN Co) has also requested access to the IPND to improve its ability to identify current connections to telecommunications networks.

As part of this review, the Department has been asked to consider whether the IPND data could be used to compare to the Do Not Call Register (DNCR) in order to determine whether numbers in the register are currently connected. In addition, because numbers stay on the DNCR for eight years, a significant proportion of them may no longer be in use by the individuals who requested their inclusion in the register, and the new subscribers may not know the numbers are included. The IPND could be used to determine whether numbers were still connected and associated with the subscriber requesting inclusion in the DNCR.

Additional non-critical users

Some of these potential new users would fit within the current category of 'research' although their projects are not necessarily within the types of research currently defined in the ministerial determination, which refers to research relating to:

- public health (not conducted for a primarily commercial purpose)
- electoral research (not conducted for a primarily commercial purpose)

[87] ABS submission

[88] RICA submission, Social Research Centre Submission

- government research which will contribute to the development of public policy.[89]

In other cases, researchers are seeking access to information not currently available to non-critical users of IPND information.

For other types of non-critical user, legislative or regulatory change would be required to enable access.

New types of researchers

With developments in telecommunications leading to an increasing number of households without a landline and changes to accessibility of the electronic White Pages®, the research industry has found it increasingly difficult to obtain representative samples of telephone numbers to conduct geographically-based surveys. This reduces the reliability and increases the cost of research.

Very few authorisations for research have been made under the IPND Scheme and at June 2014 there was only one current authorisation.[90]

In its review of privacy legislation, the ALRC expressed concern about the lack of transparency in the Minister for Communications' power under the Telecommunications Act to specify which kinds of research project should be eligible to use IPND data. The Act provides that the Minister must be 'satisfied that the kind of research is in the public interest' but provides no further detail.[91]

In relation to the current categories, the ALRC argued that these are not appropriate because:

- It may not always be clear whether or not research is primarily for a commercial purpose and some research for commercial purposes may be in the public interest.
- The test for conducting health research is significantly stronger for health research proposals under the Privacy Act where a Human Research and Ethics Committee must determine that the public interest in the research *substantially* outweighs the level of public interest in protecting the privacy of individuals.
- It was particularly concerning that the electoral research category could lead to IPND information being used for political canvassing.[92]

The ALRC recommended that the Telecommunications Act should be amended:

> to provide that before the Minister specifies a kind of research for the purpose of the use or disclosure of information or a document contained in the Integrated Public Number Database, the Minister must be satisfied that the public interest in the relevant research

[89] Clause 4 Telecommunications (Integrated Public Number Database – Permitted Research Purposes) Instrument 2007 (No1)

[90] ACMA *Annual Report 2013-14* p.120

[91] Section 285(3) of the Telecommunications Act

[92] ALRC review, pp.2462-2464

> outweighs the public interest in maintaining the level of protection provided by the *Telecommunications Act* to the information in the Integrated Public Number Database.[93]

Stakeholder views

Submissions from the research industry supported expanding the categories of research, including into the area of market research.[94] Other sectors were more cautious. ACCAN proposed a range of specific rules for research projects including. This included requiring researchers to explain why the data could not be obtained from other non-IPND sources and to allow people contacted by researchers the opportunity not to participate and to have their information flagged as not to be further used, immediately.[95]

In relation to the research categories, ACCAN noted that there was less likelihood that electoral research projects would have undergone an ethics review compared to other types of research. For this reason, the ACMA must have the ability to determine whether research was conducted ethically and appropriately including by having access to the questions.[96]

The APF was also opposed to the category of electoral research and considered that the other two categories were too broad to ensure adequate public interest justification for using IPND information. However, the APF also considered that the public policy research category should not be limited to Commonwealth agencies but include State and local government bodies.[97]

The OAIC recommended that research with any commercial purpose not have access to the IPND and was opposed to any proposal that the ACMA authorise ongoing access for particular organisations because it would create serious privacy risks.[98]

RICA proposal

The Research Industry Council of Australia (RICA) consists of the Association of Market and Social Research Organisations (AMSRO) and the Australian Market and Social Research Society (AMSRS).[99] RICA argued that the provisions relating to research should be broadened to include market and social research because:

> in the absence of accurate market and social research information, private and not-for-profit sector decisions would be sub-optimal, reducing economic efficiency and the ability of organisations in these sectors to provide services and products that meet the needs of their customers.[100]

---

[93] ALRC review recommendation 72-14, p.2464

[94] Sample Pages Submission, RICA submission, Social Research Centre

[95] ACCAN submission, p.12

[96] *ibid* p.11

[97] APF Submission, pp.11-12

[98] OAIC submission, pp.8-9

[99] AMSRO and AMSRS are industry bodies representing market and social research businesses and individual research professionals respectively.

[100] RICA submission, p.4.

RICA proposed a new framework to allow the research industry to conduct geographically-based telephone surveys by gaining access to depersonalised number and geographic information from the IPND. Under this model:

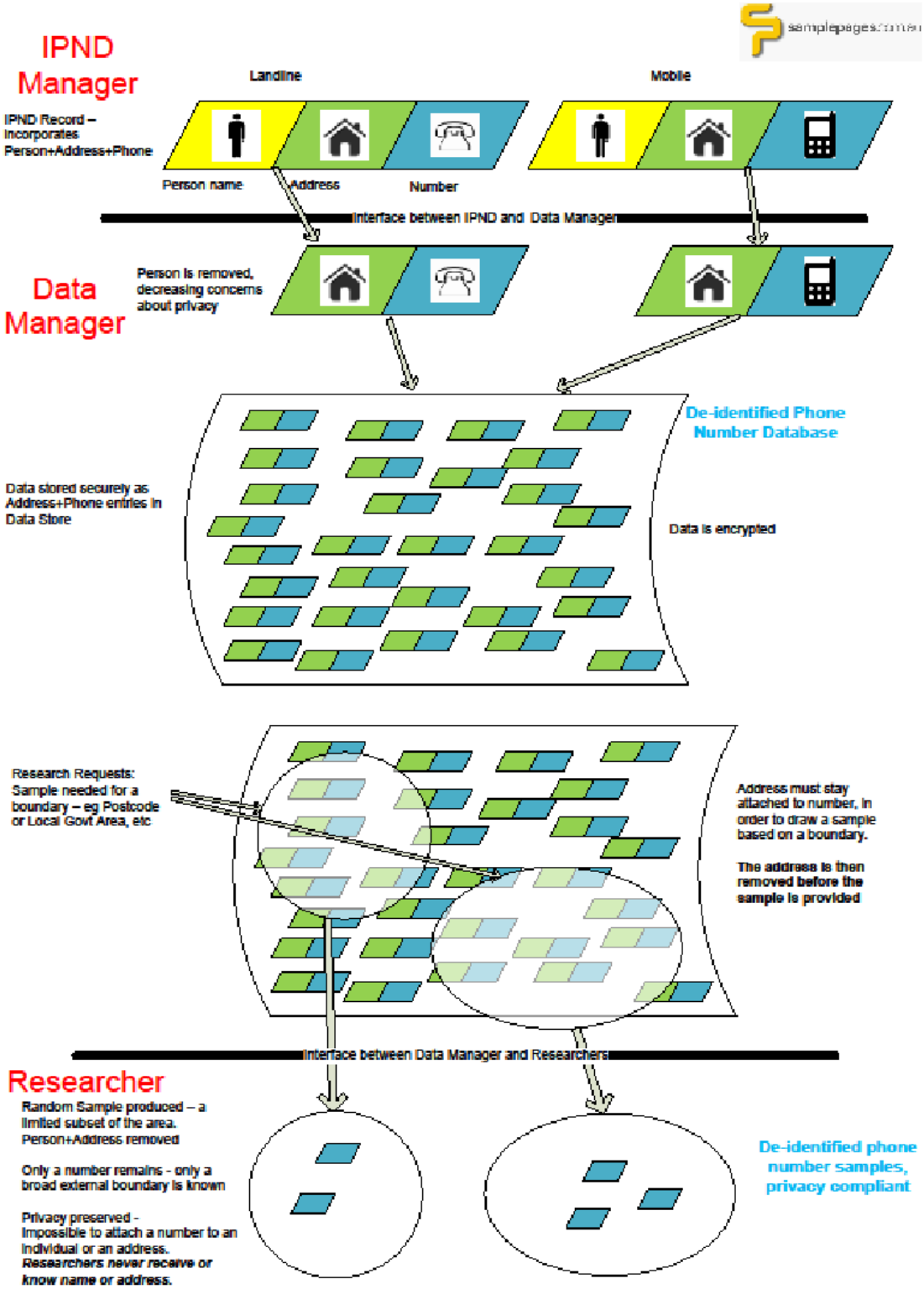
- RICA's two member organisations would apply for a joint authorisation for access to the IPND on an ongoing basis. The authorisation would not be for a particular research project, but for more general use of the IPND as a standing database for research.
- They would acquire quarterly updates of IPND information consisting of telephone number, postcode, type of service and type of subscriber.
- They would disclose some information to their members on request, where the proposed research complied with the various research industry standards.

RICA argued that its proposed model provides privacy protections because no personal information would be disclosed and because RICA members (and AMSRO and AMSRS members) are bound by strict research codes of conduct for ethics and privacy.

The main areas in which this proposal differs from current arrangements are:

- gaining access to unlisted numbers
- enabling a 'standing' authorisation rather than a project by project assessment
- including a broader range of research projects
- delegating to a non-government body the power to determine whether a particular project should have access.

Figure 3. RICA's proposed model for de-identified information for research purposes



Source: Research Industry Council of Australia IPND - proposed industry access model (5 July 2012)

Sample Pages

Sample Pages, a business providing samples to the market research industry, made a similar proposal in its submission. It noted that one benefit of a standing authorisation for certain organisations would be to increase the timeliness of access to data and that this would suit the needs of the research industry.[101]

Social Research Centre

The Social Research Centre submission proposed that the research community gain access to:

- A biannual update of all connected listed and unlisted fixed-line residential telephone numbers on the IPND, containing just the eight digit prefixes of all listed and unlisted fixed-line telephone numbers, along with a postcode for each prefix. This could then be used as a starting point for the generation of a 'list-assisted' sampling frame for fixed-line telephone surveys.
- Mobile phone number information in order to undertake geographically targeted mobile phone surveys either:
    - to provide a sample frame of all listed and unlisted residential mobile phone numbers along with available postcode, or
    - to provide a 'list matching' service whereby the IPND data could be used to append available postcode information to a randomly generated mobile phone number.[102]

Principles for approving research

The proposals put by RICA, Sample Pages and the Social Research Centre all advocate for providing depersonalised information about unlisted numbers to researchers. Some of these researchers would be undertaking projects in categories other than the three currently approved.

As noted in the Security and Privacy section of this report, in relation to access to unlisted number information for LDCS, there may be a public interest in the disclosure of information about such numbers in some cases, such as:

- where no personal information is disclosed
- disclosure would improve the utility of services or statutory authorities
- data users would not be able to discover new unlisted numbers.

In relation to extending the types of research project eligible to use data, there may be merit in this approach where researchers can show a significant public benefit.

Other new non-critical users

Requests have been made for access to some information in the IPND by the ABS, the ACMA as administrator of the Do Not call Register (DNCR) and NBN Co.

[101] Sample Pages submission, pp.2-3

[102] The Social Research Centre submission, pp.1-2

Australian Bureau of Statistics

The ABS is a statutory authority established by the *Australian Bureau of Statistics Act 1975*. The ABS is charged with collecting, compiling, analysing and disseminating statistics which are used by decision-makers to assess and create new policies. The ABS has powers under the *Census and Statistics Act 1905* to gain access to dwellings and direct people to provide information on prescribed issues. The ABS has requested power to use IPND information in order to ensure better statistics are collected for use by policy makers and assist in the efficient allocation of resources and creation of public policy. [103]

At present, the ABS contacts individuals notifying them that they are required to participate in national surveys. First contact is generally by mail and then a suitable appointment time is established. Appointments to conduct the surveys are generally face to face, but are increasingly by telephone. The ABS does not currently have access to the IPND to assist in this work but uses publicly available information.

Access to unlisted numbers in the IPND by the ABS would enable the ABS to establish suitable appointment times more efficiently and conduct telephone surveys. Importantly, access to unlisted numbers in the IPND by the ABS would not increase the chance that a person would be required to participate in a survey; it would simply make the appointment and survey process more efficient and less costly for taxpayers. The ABS has advised that access to the IPND for this purpose will have a significant impact on the cost of conducting some of its work. Under this proposal, the ABS would contact each individual by post prior to accessing his or her IPND record.

When consulted, many stakeholders agreed that access by the ABS for statistical purpose was in the public interest, but on the condition that the ABS access the IPND on the same grounds as other access seekers.

There may be merit in extending limited access to the IPND information to the ABS as a way to fulfil its statutory obligations more cost-effectively and if relevant individuals have been notified prior to accessing their records.

Do Not Call Register operator

The DNCR was established in 2007. It allows people to register their telephone or fax numbers so that they do not receive certain unsolicited telemarketing and fax marketing calls. Currently numbers can only be registered for a limited period of time.[104] This period was originally three years but has been extended, and is currently eight years.[105] By February 2015, the DCNR contained ten million numbers.[106]

[103] Australian Bureau of Statistics submission, p.2.

[104] Section 17 Do *Not Call Register Act 2006.*

[105] Do Not Call Register (Duration of Registration)Specification (No. 1) 2010 as amended

[106] ACMA Media release of 5 February 2015

In order to avoid calling the registered numbers, marketing organisations regularly submit their lists of numbers to the ACMA to be checked or 'washed' against the DNCR. In 2013-2014, 1.11 billion numbers were washed against the DNCR.[107]

There is growing concern in industry that an increasing proportion of registered numbers are no longer used by the original subscribers and the current subscribers may not be not aware of the listing of their numbers or wish the listing to continue. This is because, under the regulatory arrangements governing telephone numbering, once a subscriber stops a service, a number can be reallocated after six months in most cases.[108] As CSPs do not know if a subscriber's number is in the DNCR, there is no straightforward process for a subscriber to remove a number from the register when cancelling a service or changing numbers. Based on a disconnection rate of five per cent each year, the Data-driven Marketing and Advertising estimated that around 2.5 million numbers on the register no longer belong to the subscriber who registered them.[109]

It has been proposed that the numbers in the DNCR be tested to verify that they are retained by the original subscriber. Previous consultation with the industry found that the simplest and most cost-effective solution would be to utilise information already provided in the IPND. Other options (such as CSPs providing information directly to the DNCR operator) were not supported at that stage because any solution involving individual CSPs:

- would involve significant cost for each CSP, which would ultimately be passed onto their customers
- would involve significant cost for the Register operator, which would be passed on to the taxpayer and the telemarketing industry
- has privacy implications because CSPs could discover whether their customers are on the DNCR and the DNCR operator would necessarily discover which numbers were associated with which CSPs.

If a cleansing mechanism for the DNCR is considered necessary and using the IPND for this purpose is found to be in the public interest, a change to the IPND rules would be required to enable this.

NBN Co

The Department has been asked to consider amending the IPND access arrangement to enable NBN Co, the company rolling out the National Broadband Network, to use IPND data to identify the location and service status of all premises across Australia.[110] Access to the relevant fields has the potential to expedite the rollout including by assisting in confirming the geographic locations of premises in an industry-standard environment and the nature and provider of telecommunications services to those locations.

NBN Co suggested that outcomes for IPND stakeholders and the community would be improved by allowing access to NBN Co to only the minimum amount of data necessary to assist the company in its identification and confirmation of the nature and location of premises and the services provided to them. This information could include subscriber address and type, current CSP name and whether

[107] ACMA *Communications Report 2011-2012,* p.89

[108] Clause 10.12 Telecommunications Numbering Plan 1997

[109] Correspondence from ADMA 27 January 2012, p.5

[110] Correspondence to the Department from Mr Duncan Giles, Senior Regulatory Adviser to NBN Co, 11 April 2013

it was a fixed, mobile or nomadic service. NBN Co noted that its rollout could help identify inaccuracies with the IPND and it could use information generated in the rollout to improve the quality of the data in the IPND.

Access for NBN Co would not be a permitted disclosure under the current arrangements and would require legislative change. Where a privacy impact process can demonstrate that the public interest would be served by such a change, there might be merit in extending access to a limited range of data.

Standing authorisations

There is no statutory time limit on the length of time an authorisation through the IPND Scheme lasts, although the Scheme already allows for multi-year authorisations. Based on the Department's experience in accessing the IPND through the Scheme (discussed in Management of the IPND section of this report), the administrative burden for obtaining access is not high. The assessment process developed by the ACMA is not onerous on applicants. Rather, it is the technical and contractual process of obtaining access to the IPND that raises the greatest administrative barriers to access. There is an administrative burden on the ACMA in assessing applications, but again it is noted that the ACMA has capacity to charge application fees to recoup its costs.

Nonetheless, periodic or ongoing authorisations could be an efficient way for some organisations to access the IPND. This may be a mechanism to reduce the technical and contractual burden on applicants, and could reduce the burden on the ACMA.

For these reasons the Scheme could be amended to include periodic or ongoing authorisations, with regular checks to ensure that there have been no changes to the use or disclosure of the data. In particular, ongoing authorisations would be useful to LDCS providers and other commercial access seekers that require ongoing access to low sensitivity data (such as high level location information).

Finding

The Review finds possible opportunities exist to expand the range of non-critical users of IPND data if it can be demonstrated that use of IPND data is in the public interest, and that the public benefit in providing access to data (either at the aggregate or individual level) significantly outweighs the public benefit in protecting the privacy of individuals.

Recommendation 4

The range of users able to apply for access to IPND information (including anonymised information about unlisted numbers) should be broadened, including for a wider range of researchers, the Australian Bureau of Statistics, NBN Co and others subject to a case by case privacy impact assessment and public interest test.

Additional data fields

The IPND review discussion paper asked stakeholders to consider which data elements should be in the IPND and what principles should guide the addition or removal of data elements.[111] This section discusses these factors and then considers policy issues of adapting the system to expand the type of information included in the IPND while minimising the additional compliance costs for industry.

Stakeholder views

Most of the responses related to information that would help critical services. One exception was the submission from Acceleon which requested that a commencement date for the establishment of connections be included because this would be helpful in establishing a transaction history for credit checks and for undertaking identity verification under the *Anti-Money Laundering and Counter Terrorism Financing Act 2006*.[112]

Critical users have requested new data elements to support various functions, including:

- dynamic internet based information for use by the ECS and law enforcement and national security agencies
- real time information provided through the enhanced Mobile Location Information program (MoLI)
- geographic coordinates for landline location to assist in locating an address
- update 'type of service' field to include a wider range of technologies such as mobile broadband
- date of birth of subscribers, to enable law enforcement and national security agencies to distinguish between two subscribers of the same name
- International Mobile Subscriber Identity information, to enable law enforcement and national security agencies to identify which physical network a non-roaming mobile phone is utilising without having to seek the assistance of carriers when required.

A number of submissions considered that new data elements should be included in the IPND only after comprehensive analysis of public interest and privacy impacts. For example, the APF stated that:

> the starting point should be that only information proportionally necessary for the critical uses of the 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).[113]

The qualitative section of the Department's Triple Zero research study found that there was significant support amongst survey participants for the Triple Zero operator to have access to a

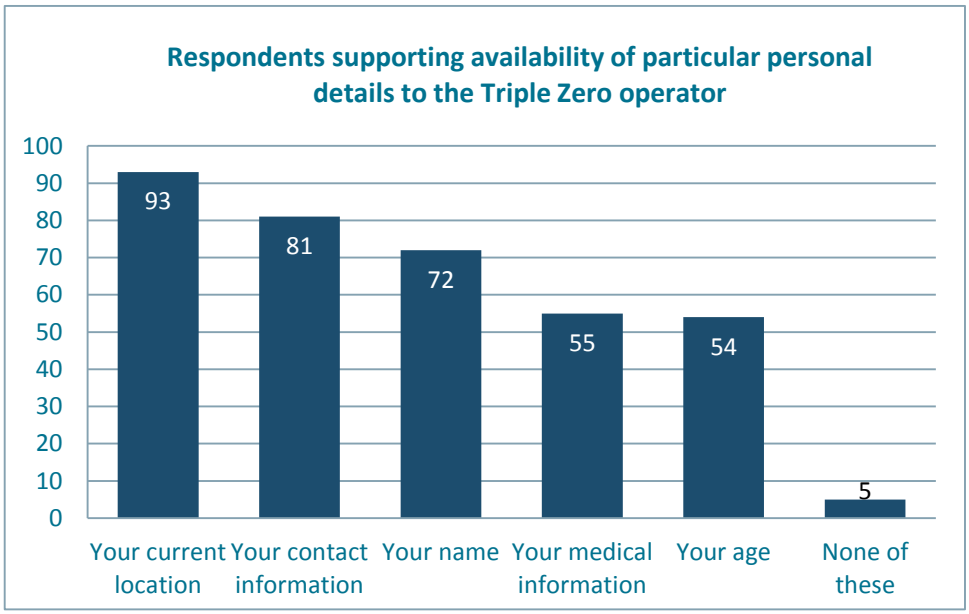
[111] *Review of the Integrated Public Number Database Discussion paper*, discussion question 7, p.8

[112] Acceleon submission, pp.8-9

[113] APF Submission, p.6.

broad range of personal information, although some participants felt that 'others' may be uncomfortable with the availability of medical records.[114] The quantitative part of the study about these findings can be seen in the chart below.

Figure 4. Respondents supporting availability of particular personal details to the Triple Zero operator.



Source DBCDE Triple Zero study p.29

Industry submitters to the IPND review discussion paper argued that the data in the IPND should be as limited as possible. For example, Optus noted that '[a]ny consideration to add data elements collected from CSPs must only relate to data that is ordinarily collected in the course of supplying telecommunications services'.[115] This view was supported by other industry participants who were concerned that, even if information is collected, there can be a large cost in making that information available to the IPND because of the need to adjust different databases inside an organisation.

Some submissions cited the arrangements used internationally by emergency services to locate mobile handsets and incorporate VOIP services and provided examples where social media had been used to contact emergency services.[116] In the United States of America, access to location information for mobile handsets and for VOIP services connected to the Public Switched Telephone Network (PSTN) is mandated. In the USA, Government and industry are also working towards protocols for using internet services to transmit text voice or images to emergency call services.[117] In

[114] Former Department of Broadband Communications and the Digital Economy 'Triple Zero Research Study' June 2012, p.31

[115] Optus submission, p.2

[116] e.g. VON Europe Submission p.3, VHA submission pp.4-5

[117] National Emergency Number Association 'Next Generation 9-1-1' http://www.nena.org/?NG911_Project#bottom

Canada, a system has been developed for the transmission of caller locations to emergency services. This system does not yet work for nomadic VOIP services.[118]

Critical users

While there remains a need for critical users to have access to personal and locational information, there are concerns that the IPND is becoming less relevant due to changing technologies. Table 5 lists the specific information problems as identified by each critical user that are not currently being met by the IPND. This table was developed with the assistance of critical users and through responses to question 21 of the IPND review discussion paper.

It should be noted that it is not feasible to provide some of these types of information within the current IPND. It also raises issues as to how this may work with other regulatory schemes, the compliance burden to industry, and privacy implications of the collection of information.

Table 5 - Information gaps for critical users

	Emergency Call Service	National security and law enforcement	Emergency Warning System
Internet based			
Linking a location with the CSPs providing telecommunications services to the location	Not needed	Current need	Not needed
Linking a subscriber with the CSPs providing telecommunications services to the subscriber	Not needed	Current need	Not needed
Dynamic data			
Linking a location with the mobile/nomadic VoIP telephone numbers at that location	Not needed	Expected need	Current need
Linking a mobile number with the location of the handset	Current need	Current need	Not needed
Both dynamic and Internet based			
Linking a nomadic VoIP telephone number with the location of a handset	Current need	Current need	Not needed

[118] Canadian Radio-television and Telecommunications Commission at www.crtc.gc.ca/eng/info_sht/t1035.htm

Linking a VoIP telephone number with the internet identifiers used to access the service	Expected need	Current need	Not needed
Linking an internet identifier with a subscriber in real time	Expected need	Current need	Not needed
Linking a subscriber with an internet identifier in real time	Expected need	Current need	Not needed
Linking a location with an internet identifier in real time	Expected need	Current need	Not needed

Dynamic internet based information

Information about internet services is not captured by the current regulatory scheme. While consumers are increasingly substituting internet services for traditional telephony. At present, there is no IPND equivalent that enables critical users to link an internet service to a subscriber or service address. This places pressure on critical users to adapt their processes to these new services.

In many cases, the IPND already enables critical users to have a reasonable idea of the relevant internet service provider, given that there is a strong correlation between the internet service provider and the CSP that assigned the telephone number (for example, many CSPs offer an ADSL service, but require the customer to also purchase a voice telephone service associated with a telephone number). However, the current system does not provide complete coverage, is expensive in terms of administrative effort, and there is no indication within the IPND about which telephone services have internet services associated with them.

Critical users have noted that a system to provide information about Internet Protocol (IP) addresses is required to perform their functions efficiently. On the internet, each end node must be assigned an IP address. Due to exhaustion of the number of addresses under the older IP standard, IPv4, end nodes are also sometimes assigned port numbers to differentiate different end nodes from the same network. At any one point in time, there can be only one end node anywhere in the world using a particular IP address and port number combination on the internet. Port numbers are not a requirement for more recent IPv6 addresses. IP addresses/port numbers are assigned by the end-user's internet service provider. Critical users have identified that they face two linked, but distinguishable needs in terms of internet services:

1. linking IP address information to a subscriber or location
2. linking a subscriber or location with an IP address.

Views about including dynamic information varied among privacy stakeholders. For example, the APF argued 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 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.[119]

In contrast, ACCAN noted that:

> Clearly, the delivery of dynamic location information to Emergency Service Organisations (ESOs) is essential … [t]he 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.[120]

Information provided through the MoLI program

The ACMA has been working with the Communications Alliance and the three Australian mobile carriers to enable automatic delivery to state/territory Emergency Service Organisations of location information when a mobile phone is used to contact Triple Zero (known as enhanced MoLI). This capability has been implemented and tested by all three carriers and the Triple Zero operator. A number of States/Territories have updated their systems to accept this location information as part of their dispatch systems, with full implementation across all jurisdictions expected before the end of 2015. Enhanced MoLI provides estimated location details when a mobile handset is used to contact Triple Zero. The accuracy of this information will vary, and the system does not provide precise coordinates of the mobile handset. MoLI will provide emergency service organisations with the estimated area where a Triple Zero caller is most likely located, based on the coverage area of the mobile tower used to make the emergency call.

National geo-coded addressing

One of the Government's public policy objectives is to make quality geo-coded national address data available to all Australians under open data terms (that is, at no charge to end users and with minimal license restrictions). The Department of Communications continues to work with industry and government stakeholders in the spatial sector to realise this objective.

Geo-coded addressing is the process of associating an address with coordinates such as latitude and longitude to enable it to be readily mapped and related to other data. Geo-coded national address data can be used in almost any business or operation. Examples include: effective government service delivery and policy development, national, state and local infrastructure planning; private business planning and analysis; data verification and accuracy; emergency response; personal navigation and mapping; fraud prevention; and address validation at the point of entry for business and government. In regard to the IPND, geo-coded address data provides an authoritative reference against which existing IPND data can be washed so as to improve its accuracy.

An authoritative geo-coded national address dataset is currently maintained by PSMA Australia Limited (PSMA), an unlisted public company owned in equal shares by the nine governments of Australia. The Geocoded National Address File (G-NAF) contains more than 13 million physical address records. Each record includes the state, suburb, street, number and coordinate reference (or geocode) for each street address. G-NAF does not contain personal information. PSMA uses data

[119] APF submission, p.15

[120] ACCAN submission, p.15

from a range of sources and contributors, including state and territory land records, Australia Post and the Australian Electoral Commission. PSMA funds these activities through licensing fees.

Making geo-coded national address data available under open data terms would result in public sector efficiencies driven by data sharing, productivity improvements for large and small business generating profits and growth, and the stimulation of research, innovation and competition in the applications and software markets.

Date of birth

A number of law enforcement and national security agencies have suggested that the date of birth of the subscriber should be included in the information provided to the IPND because:

- Date of birth, name and address information are the data keys that are commonly used in other public and private databases. The inclusion of date of birth information would assist agencies in being able to cross-reference IPND information with information in other databases managed by those agencies.
- Date of birth information could also be used to distinguish between two subscribers of the same name, which would enhance the privacy of subscribers, reduce the costs of IPND access and enhance the efficiency of law enforcement and national security agencies.

In addition, there is a benefit in ECS knowing the age of a subscriber before dispatching emergency services (for example, in identifying that a caller could be elderly). As noted above, 54 per cent of respondents to the Department's Triple Zero research study expected that the Triple Zero operator would have age information available.

Bilateral consultations with industry indicated that date of birth information is typically collected by CSPs for the purposes of checking credit-worthiness. This is confirmed by the privacy policies of CSPs.[121] Also of note, Mobile Number Portability industry code arrangements already require CSPs to validate a ported service against date of birth information unless the two carriage service providers have a bilateral agreement in place.[122]

Requiring the provision of date of birth information will impose a compliance cost on CSPs. This cost will be elevated because CSPs have a range of products across their business, and there is no system currently in place that allows all of the databases behind those products to report date of birth information.

International Mobile Subscriber Identity

An International Mobile Subscriber Identity (IMSI) is a 64 bit data field that is associated with GSM mobile telephone handset. Critical users have suggested that IMSI information should be included in the IPND to enable law enforcement and national security agencies to identify which physical

[121] e.g. VHA <http://www.vodafone.com.au/aboutvodafone/legal/privacypolicy> , Optus <http://www.optus.com.au/aboutoptus/About+Optus/Legal+%26+Regulatory/Privacy/Privacy+Collection+Statement>, Telstra <https://register.telstra.com.au/global/collection_statement/privacy_statement.htm?SMSESSION=NO>,

[122] Communications Alliance *Industry Code Mobile Number Portability C570:2009*, p.27

network a non-roaming mobile phone is utilising without having to seek the assistance of carriers. This would allow an investigation to progress without requiring the active assistance of the carrier. This would promote greater security during an investigation, reduce compliance costs for carriers and enhance the efficiency of law enforcement and national security agencies.

A subscriber's IMSI is necessarily known by their CSP, because it is assigned to Subscriber Identity Modules (SIMs) as they are issued. It is not expected that there would be a large compliance cost associated with the provision of IMSIs to the IPND.

Update to the type of service field

In addition to new data elements, it was also suggested that the existing 'type of service' field be updated because the 'type of service' information provided is out of date, and had not kept pace with the introduction of new services. While the 'type of service' information allows the identification of data and facsimile services, this is not the case for mobile broadband services. A mobile broadband service is a wireless internet service that commonly utilises a mobile phone number and a 3G or 4G mobile network to provide internet access. Where a law enforcement or national security agency identifies a subscriber through the IPND and wishes to request call charge records from the relevant CSP, they have no way of knowing whether the relevant mobile number is for a voice mobile service or for a data only mobile broadband service. CSPs cannot provide call charge records for mobile broadband services, and so the inclusion of this kind of information in the IPND would enable law enforcement and national security agencies to only make requests for call charge records where the request has a chance of being fulfilled. This would reduce the number of call charge requests that CSPs receive.

Submitters to the discussion paper also argued that the 'type of service' field should also be mandatory rather than optional. In principle, this would ensure that there was some information available to critical users about the service associated with a particular number. However, CSPs are not always aware of the use to which a number is being put. For example, under the current classification system, a CSP cannot be sure that a number that it issues is not being used for data or fax purposes.

Finding

The Review identifies additional data fields could be added to the IPND to meet the changing needs of IPND users. It is important to evaluate any potential compliance burden and privacy implications of collection of information.

Management of the IPND

The review considered the current management arrangements for the IPND and whether the IPND meets the needs of data providers and users by examining how easy it is to meet the technical and regulatory requirements associated with the IPND, including in relation to the compliance cost for data providers and the direct charges for data users.

Transparency of role of IPND manager

Current management of the IPND

Telstra is the manager of the IPND as part of its carrier licence conditions.[123] Under section 272 of the Telecommunications Act, the responsible Minister has power to make a written determination specifying that a different person or organisation must manage the IPND. This power has never been exercised.

Whilst the basic functionality of the IPND has not changed since its creation, Telstra has advised that it has made a number of upgrades to the IPND to implement changes in the level of access for different types of IPND user, to upgrade hardware and software and to improve security.[124] Telstra advised in its submission that these upgrades had led to having a current availability of at least 99.98 per cent.

Stakeholder views

Critical users noted that Telstra had generally managed the IPND well but, nonetheless, argued that the management of the IPND should be more transparent. There was a perception that Telstra operated the IPND on a commercial basis and makes a profit from the fees charged for access to the IPND without any independent oversight.

Public number directory producers considered there was a perceived conflict of interest in having Telstra as the manager of the IPND and the owner of Sensis, the publisher of the White Pages®. For example, the Acceleon submission stated:

> One of the primary purposes for the establishment of the IPND was to introduce competition into the provision of telephone directory services … [i]t is therefore ironic that Telstra should have the role of being IPND Manager.[125]

This view was also supported by the APF which recommended that:

[123] Clause 10 of *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*

[124] Telstra submission pp.24-25

[125] Acceleon submission p. 4. It is noted Telstra announced it sale of the majority of Sensis in January 2014 and is now only a part owner.

> 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.[126]

As noted in Quality and Accuracy of the IPND section of this report, some submissions considered that the current management arrangements do not contain incentives to upgrade technology or improve data quality. The Local Phonebook Company argued that the role of database manager should be given to the ACMA because it was the best organisation to ensure the integrity of the IPND.[127]

ACCAN noted that the key attributes in managing the IPND are the robustness and reliability of the system. ACCAN suggested that, if any transition was made away from Telstra, then this process would need to be carefully managed.[128]

Telstra questioned whether it was appropriate to alter management arrangements in the medium term. Telstra pointed out that under its management, the IPND had been subject to no major service faults, and argued that it had made a number of investments to improve the technical operation of the IPND. Telstra also noted that there are synergies between its role as IPND manager and as the Emergency Call Person.[129] In bilateral discussions, Telstra argued that it had no commercial interest in managing the IPND and stressed that administrative and operation procedures currently in place prevent any conflict of interest in having Telstra manage the IPND and own Sensis.

Accountability and transparency of the IPND manager

The fact that Telstra is both the current IPND manager and part owner of Sensis, the leading telephone directory publisher in Australia, has led to the perception of a potential conflict of interest. This potential conflict could be mitigated if there was more transparency about the measures that Telstra takes to manage its potential conflict of interest.

Telstra has advised that there are operational firewalls that it has put in place to ensure that any potential conflict of interest is managed. However, these measures are not well known, even to stakeholders that deal with the IPND on a daily basis. The standard form of agreement (the access deed) that IPND access seekers must agree to before accessing the IPND is not a public document. In fact, access seekers must sign a confidentially agreement before having an opportunity to view the access deed. Telstra's carrier licence conditions specify that for CSPs, terms of access to IPND information, including costs, are contestable and can be determined by the ACCC if the parties are unable to agree. These provisions do not apply to other IPND users.[130]

Other performance metrics are more difficult to assess. There does not seem to be any natural incentive for Telstra to reduce costs, given there is no public scrutiny of the cost recovery arrangements and costs are recoverable from IPND users. It would be expected that the costs should

[126] APF submission, p.16

[127] Acceleon submission, p.8; The Local Phonebook Company submission, p.8

[128] ACCAN submission, p.16

[129] Telstra submission, p.6

[130] Subclauses 10(7), 10(9) and 10(10) of Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997.

vary depending on the number of users the system has in any given period but the charges have only been adjusted once.

Finding

The transparency of the IPND manager is lowThe Review found no publicly available information on how the costs of the IPND are determined, or how access fees are calculated. While Taxpayers fund the majority of access charges to the IPND, little available information exists as to how efficiently the IPND is run. Stakeholders and the public at large may have greater confidence in the IPND manager if there was more publicly available governance information regarding the IPND.

Technical requirements

In order to provide data to the IPND, data providers must comply with technical requirements set by Telstra. These:

- set out the high level design of the IPND data structure and physical database
- set out the format that data must be provided
- require that data provided to the IPND must be over a secure link and can only occur via a frame relay[131] or Integrated Services Digital Network (ISDN) link
- set out other operational constraints (such as availability of the database).[132]

Data users can access the IPND through frame relay, ISDN link or encrypted disc.

Views of stakeholders

There was concern expressed about the technical requirement to use an ISDN link, as this is an older and quite expensive technology. For instance the Local Phonebook Company submission noted:

> network infrastructure should use the fastest current technology available – broadband internet – not one of the slowest and costliest – ISDN. Access could be provided through an RDC [Remote Desktop Connection], or even better a browser connection.[133]

Acceleon also considered that the technical requirements were difficult to establish and stated that:

> it required Acceleon up to 10 calls to Telstra, over 5 hours on the phone, and many internal transfers to set up [an ISDN] connection. Further to this, it is an extremely expensive technology, and skills to correctly configure the hardware to communicate via an ISDN connection are rare because the technology is out-dated.[134]

The Communications Alliance submission argued that the use of dedicated ISDN links has contributed to the high level of security of the IPND since it was established.[135]

---

[131] 'Frame relay' is an older packet-switching technology for sending data used primarily for Wide Area Network links.

[132] Telstra *Integrated Public Number Database (IPND) Data Users and Data Providers Technical Requirements for IPND*

[133] The Local Phonebook Company submission, p.7

[134] Acceleon submission, p.4

[135] Communications Alliance submission, pp.8-9

Impact on stakeholders

It is not clear how many CSPs would be affected by the requirement to establish an ISDN link because, although all CSPs are required to provide information to the IPND, the vast majority of them send it via data aggregators, which are the direct data providers. There are only about 85 data providers and more than 500 CSPs.[136] Whether particular CSPs need to comply with the technical requirements for the IPND would depend on their contractual arrangements with their data aggregator.

There are only a small number of data users receiving information via an ISDN link. However, the use of ISDN technology to connect the IPND is imposing an ongoing compliance cost on users and raises a significant 'red tape' barrier to the use of the IPND. While this arrangement may have some privacy benefits because it is extremely difficult for unauthorised people to access the system remotely, in principle, the privacy of subscribers should be protected through strict administrative rules, rather than through a technology. Furthermore, higher compliance costs in uploading information to the IPND may have a detrimental impact on the accuracy of information.

Cost of access and management of the IPND

The Government does not directly fund the operation of the IPND. Rather, the obligation to provide data in a particular form is a cost to the telecommunications industry. The costs of managing the IPND are recovered from data users.

Views of stakeholders

Few submissions expressed concern about the compliance costs and data access costs. The Communications Alliance stated that '[i]ndustry does not have any significant concerns about the costs to data providers and data users of accessing the IPND'.[137] Other submissions from CSPs did not raise the cost of providing data as a significant issue. In contrast, industry submitters to the discussion paper have noted that changes to the existing IPND (and the CSP systems that feed into the IPND) could impose a high compliance cost.

Similarly, the cost of access for data users does not appear to be a major issue. While some users indicated that costs seemed high, they did not present any alternative funding proposals. The AGD submission suggested that the cost of critical users gaining access should be reviewed and should be on a cost recovery basis only.[138]

Telstra proposed that an alternative charging mechanism could be to charge data providers when making entries.[139] However, this option would be a disincentive for CSPs to provide updates and might reduce data quality and accuracy.

---

[136] ACMA *Communications Report 2011-12* p. 19 lists 212 providers of PSTN (landline) telephony, 212 providers of VOIP services and 156 mobile service providers and Telstra has advised there are 85 data providers as at June 2013.

[137] Communications Alliance submission, p.2

[138] Attorney-General's Department submission, p.3

[139] Bilateral discussions with Telstra.

Current compliance costs

The costs to comply with the current IPND requirement will vary for each individual provider, depending on their mix of services, the number of customers that they have and their efficiency in complying. The set-up costs of providing IPND information are understood to be in the order of $50,000-$100,000 but, as noted above, CSPs typically contract with a data aggregator to offset some of these costs. An encrypted ISDN link is estimated to cost up to $15,000 per quarter. Ongoing costs for each provider would include labour costs for data verification.

Compliance costs would increase for CSPs as their systems become more complex and product offerings become more diverse. For some large CSPs, it is estimated that the cost of compliance with IPND obligations could approach $100,000 per year.[140]

Across the industry as a whole, the compliance costs are likely to be in the order of several million dollars each year.

Cost of access for data users

Access fees to the IPND are set by Telstra. There is currently no additional charge set by the ACMA to apply to the ACMA for access under the IPND Scheme.

Telstra advises that it sets fees on a cost recovery basis and last reviewed them in 2007. Currently the standard fees are almost $4,000 per quarter and $0.01 per IPND record per year. There is also an initial application fee of $3,000 and a charge for an encryption device.

If IPND users choose to use an ISDN link there would be additional establishment and ongoing data costs.

Telstra's carriage licence conditions set some price controls for CSPs accessing the IPND, but there are no price controls on other types of user accessing the IPND.[141]

The cost of managing the system varies from year to year depending on whether there are any upgrades to hardware and software, and the number of records accessed by data users. Telstra has advised that, over time, it tends to recover its costs from users, making the system effectively cost-neutral.

IPND access seekers pay for access on a unit basis, which provides a natural incentive to seek the minimum amount of information necessary. Payment by access seekers is considered to be an efficient allocation of costs, because the stakeholders that pay are the stakeholders who receive the benefits of the services provided by the IPND. For example, NSW taxpayers are the beneficiaries of access by the NSW police force, and are ultimately the stakeholders that fund this access.

[140] Informal advice from a large CSP, with many legacy systems and a diverse product offering.

[141] Subclauses 10(7) and 10(9) of Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997.

Regulatory issues to gaining access

Another consideration is whether the regulatory barriers designed to ensure that access to IPND data is only granted in accordance with the public interest remain appropriate.

The decision-maker on access to the IPND depends on which provision in Part 13 of the Telecommunications Act is relied on to obtain access. Generally speaking, critical users are able to access IPND information under various provisions of Part 13 of the Telecommunications Act. In those circumstances, it is for Telstra (as a carrier and CSP) to satisfy itself that any disclosure is permitted under Part 13 and its carrier licence conditions.

However, in relation to two types of non-critical users (public number directory publishers and researchers) there is a two-step process for accessing IPND information. This process is set out in paragraph 285(1A)(d) of the Telecommunications Act and the Telecommunications Integrated Public Number Database Scheme 2007 (the IPND Scheme). First, these entities must apply to the ACMA for authorisation. If ACMA provides this authorisation, then Telstra (as the IPND Manager) establishes a contract with these entities, which gives Telstra control over how IPND information is used. The contract sets access terms, and generally is designed to enable Telstra to recover IPND access fees. It is not known whether any IPND user has not proceeded to obtain access to the IPND because of the terms of the contract.

Access to the IPND for research purposes has only occurred rarely, and one of those cases was the Department of Communications seeking access to conduct the IPND accuracy study. It is possible that the complexity of the regulatory requirements is a factor in the low usage rate.

Case study: Process of acquiring access to the IPND

In 2012, Woolcott sought access to the IPND through the IPND Scheme to conduct an accuracy study of IPND information as consultants to the Department of Communications.

Woolcott's role was to:

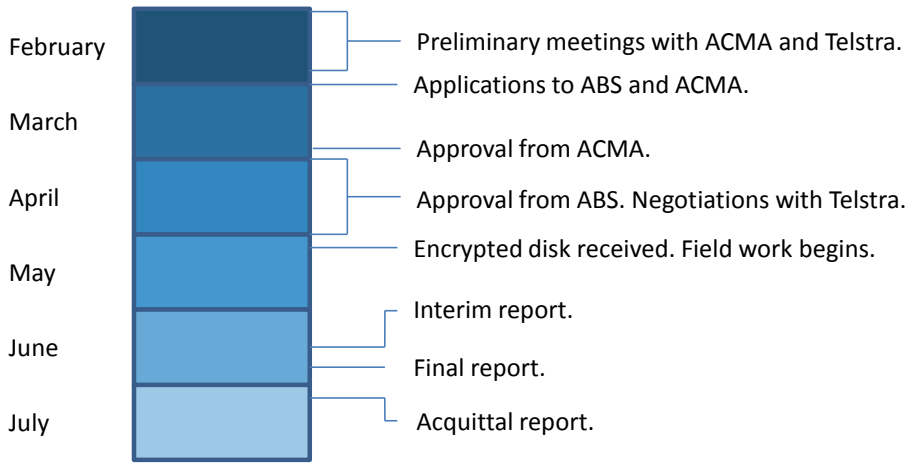
- develop a sampling methodology and script for conducting telephone surveys
- develop and submit the:
    - IPND Scheme application documentation
    - ABS statistical clearing house application (government surveys contacting 50 businesses or more must be approved by the ABS statistical clearing house)
- conduct the survey and prepare statistical analysis on the results
- prepare a report for the Department.

In general terms, a significant amount of preparatory work was conducted before field work commenced. Much of this work related to the development of a suitable methodology with the desired cross-tabulations and the development of a script.

The development of the IPND Scheme applications and their examination by the ACMA proceeded faster than expected. However, the actual exchange of contracts with Telstra took longer than expected. This was because contracts needed to be exchanged physically and because of the number of agreements that needed to be finalised (Telstra's process requires the completion of an 'Application of Intent', a 'Confidentiality Agreement' and the access agreement). Once received, Woolcott did not experience any problems with accessing and formatting of the data.

The fieldwork component of the study proceeded smoothly and no complaints were received by the Department of Communications or Woolcott about the study. The following timeline shows how the study progressed.

Figure 5. Progression of Woolcott's study of the accuracy of the IPND



In summary, the researchers found little difficulty with complying with the regulatory requirements, but the operational and contractual requirements were quite complex.

Many of the delays in the current process experienced by Woolcott could be removed or offset by improving the transparency of the management of the IPND, including through the publication of standard form contracts for accessing the IPND. This would allow access seekers to determine whether the terms are acceptable prior to making an application through the IPND Scheme.

Finding

There is little information available concerning the technical requirements for connecting to the IPND using ISDN connections, and information that is available appears to be out-dated.

The Review found that while Telstra has managed the IPND in a reliable and secure manner, greater transparency regarding its management would benefit users. This includes issues such as the methodology for establishing user charges and how it manages its potential conflicts of interest between its roles as a CSP and IPND manager, and as part owner of the publisher of the White Pages®.

The level of compliance costs for data providers was identified by the review as not being of concern to industry, however the costs of transitioning to any new system would need to be considered carefully.

The review identified that recovery of costs for IPND management from data users may be an efficient method, particularly as it recovers costs from those benefiting from the system and sends appropriate price signals to data users by linking fees to the level of use.

Recommendation 5

The ACMA should be enabled to approve ongoing or periodic access for an applicant, provided that the ACMA regularly reviews access and that a privacy impact assessment is completed.

Recommendation 6

The ACMA should be able to approve electronic public number directories to display unlimited numbers of entries from the IPND if appropriate 'anti-scraping' measures are in place.

Recommendation 7

The ACMA should publish information about applications and decisions made under the IPND Scheme.

Recommendation 8

In order to improve the transparency of the management of the IPND, Telstra should make available:

- the measures it takes to separate its role as part-owner of the publisher of the White Pages® and the manager of the IPND
- its standard form of agreement with data users
- annual audited financial reports for the IPND.

The regulatory process for gaining access to the IPND is complicated, since non-critical users need to demonstrate that the proposed use will be in accordance with the requirements of the IPND Scheme, and that they will comply with security requirements. The Review finds potential opportunities to make the process more transparent.

Future of the IPND

The Review considered whether the current static database meets the needs of users and evaluates the need for change.

There are opportunities to improve the IPND by developing a replacement (or modified) system that enables access to more dynamic information and information about web-based services. If these deficiencies are not addressed, there are likely to be higher compliance costs on industry, higher costs on emergency services and law enforcement agencies and lower public confidence in their operations.

To overcome the deficiencies of the IPND, information from a greater range of industry participants is required, including Internet Service Providers (ISPs). The Review has identified that this would be a significant challenge. Multiple systems to access information from the telecommunications industry duplicate costs and raises privacy and consistency questions. To the extent possible, any possible successor to the IPND should take into account existing data sources and minimise duplication.

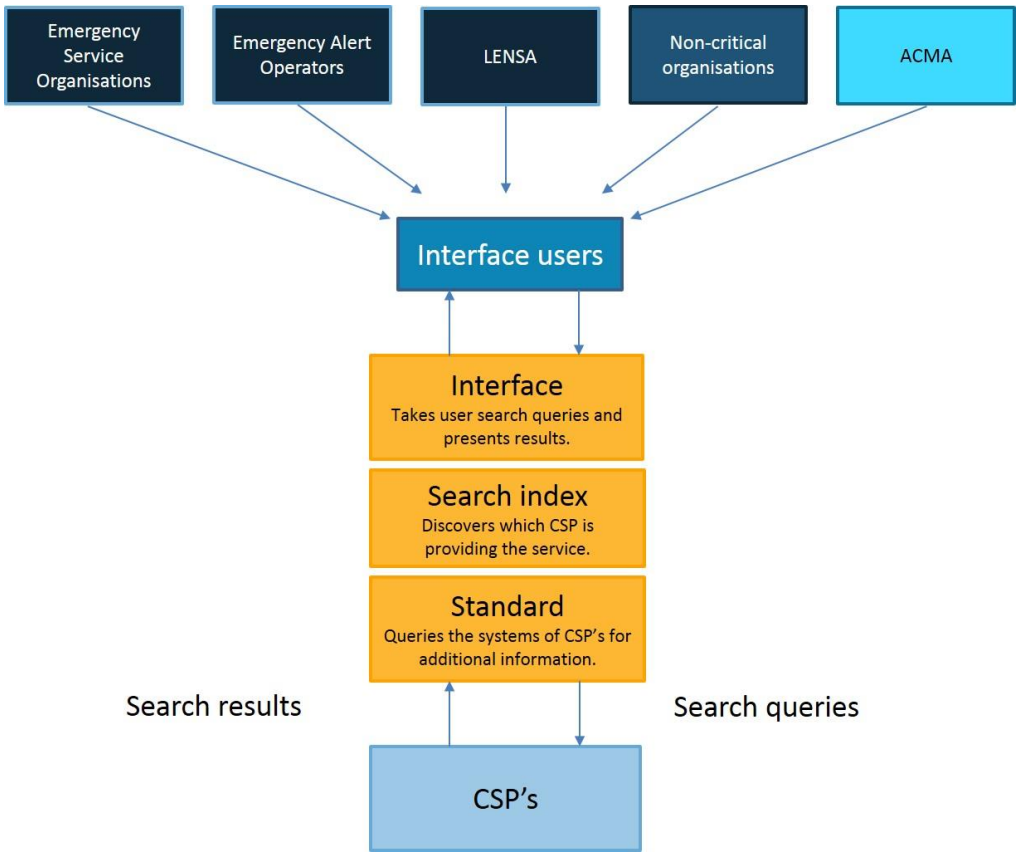
A single, centralised system of providing information to critical users may be more efficient and have lower compliance costs than multiple systems. The privacy of subscribers should be protected through robust and well enforced access rules.

A new system would not be intended to impose data retention obligations on CSPs, or require CSPs to collect or store data that they would not have existing capacity to collect or store. Likewise, a new system interface should have technical limitations built into it to ensure that all data users have proper authorisations, and would be unable to utilise the system to conduct activities outside their authorisations. It would replace the current 'push' system with a 'pull' system.

Over time, it could transition to a more dynamic system that would make particular information available to the categories of users which have demonstrated a substantial net public benefit in gaining access to it.

As this system would no longer be a single database but rather an interface through which users would gain subscriber and location information, a more appropriate name than the IPND could be 'Subscriber and Location Information Interface' or 'SALII'. A diagram of how such a system would work is below.

Figure 6. Model of subscriber and location information interface.



The Review found that should IP address information be provided through the proposed system, potential compliance costs may be imposed on CSPs. The precise cost would depend on the standard and particular systems of respective CSPs. The Review identified that further work with CSPs (particularly smaller CSPs) would assist in the development of a standard to ensure compliance costs are minimised.

Development process

The development process would involve the development of a system that preserves the strengths of the current IPND while enabling enhanced functionality. Key principles to consider when developing a new system include that it would be:

- consistent with community expectations in terms of the protection of personal information
- scalable to new data providers, data users and data elements
- secure, reliable and robust with inbuilt redundancy
- easy to use
- as accurate and up to date as possible
- cost-effective.

Ongoing dialogue with industry would be needed to ensure that the successor to the IPND could be integrated with companies' systems to the extent possible and to trace the changing use of telecommunications by consumers. The new system would be developed in a way that addresses the regulatory and policy issues raised in previous sections of this report.

Incremental change

The telecommunications industry is in a state of constant and (potentially) disruptive change. Large changes to regulatory obligations can lead to significant compliance costs. It is preferable from a regulatory point of view for change to be incremental. This approach should lead to lower compliance costs and enable the system to remain viable and adaptable and to maximise the chance to ensure that the quality of public safety is maintained.

The transition from the existing IPND to a new system would need to be managed carefully to ensure the continued availability of information to critical users and to improve public safety outcomes for agencies, maintain the privacy of customer information, and minimise any transition costs to industry and data users.

There is opportunity to encourage competition and innovation in the construction and management of the system. If there is a transition to a new system (including technical specifications and standards), the building and management could be subject to a periodic tender. The first of those tender processes could focus on building and managing the new system, with subsequent tenders focusing on management and any necessary refinements to the system, for instance. Periodic market testing would allow the new system to operate more efficiently and potentially at less cost both to users and to the CSPs who provide the information.

Under this option, the costs associated with establishing, running and managing the new system could be funded by charges paid by critical and non-critical users. These charges would be transparent, and developed and agreed in consultation with data users and providers in order to ensure that potential costs were understood by all parties.

To support these new arrangements, regulation would be reformed and streamlined with the objective of less regulation and lower costs for data providers and users in the long term.

The following principles could guide the development of a new system:

Principle	How the differs from current arrangements/ Why change?
It would provide dynamic information from CSPs on demand from critical users.	Only static information is available. Critical users supported the inclusion of dynamic information to improve the utility of the system.
It would incorporate IPND-like information about internet services from a broad range of CSPs, including Internet Service Providers.	It only includes information about public numbers. Critical users supported the availability of information about internet services such as the name of an ISP and a customer's IP address in order to find a subscriber's location.
Primarily, the new system would not operate as a relatively static database (like the current IPND)	Currently, the IPND is a central database.

but use an interface to query the databases of CSPs.	This change was supported by industry to reduce the cost of interfacing with a central database using legacy technologies.
It would not duplicate existing information systems and, where possible and necessary, it would integrate data from all relevant sources.	This is a new principle, intended to minimise the compliance cost of providing additional data to the new system while maximising its effectiveness. While there were few concerns about the costs of complying with the current system, this would address industry concerns about the cost of providing additional data.
It would not impose new data retention obligations on CSPs.	This is a new principle, intended to clarify (and limit) the intended scope of the new system.
It would only contain new data elements where the benefits substantially outweigh the cost of collection and where they can be shown to be in the public interest.	This is a new principle, to provide a public policy framework for the assessment of new data elements.
It would provide appropriate levels of technical security to ensure that the privacy of subscribers is maximised.	The current system is very secure but uses outdated technology. All stakeholders considered security of any replacement system to be of paramount importance.

While a new system might bring with it a range of benefits, it would be prudent to await the Department's Review of the Triple Zero operator and the implementation of the Triple Zero contract arrangements from 2016. This is because in conducting this review, issues and options that have not yet been adequately explored might be identified which could be of greater benefit to the development, operation and management of a future IPND-type system.

Recommendation 9

The current IPND should be retained for the medium term and the need for a new system should be investigated again after the completion of the Department's Review of the Triple Zero operator and the implementation of the Triple Zero contract arrangements from 2016.

Appendix 1 – List of public submissions and submission process.

Organisation/ Name
Acceleon
Anonymous submission 1
Association of Public-Safety Communications Officials Australasia
Attorney General's Department
Australian Bureau of Statistics
Australian Communications Consumer Action Network (ACCAN)
Australian Privacy Foundation (APF)
Communications Alliance
Industry Number Management Services
Liberty Victoria
Local Directories
Mr Arthur Marsh
National Emergency Communications Working Group - Australia & New Zealand (NECWG- A&NZ)
NBN Co
NSW Police
Office of the Australian Information Commissioner
Optus
Research Industry Council of Australia (RICA)
Samplepages
Social Research Centre
Telstra
The Local Phonebook Company (Green and Gold)
Vodafone Hutchison Australia
Victorian Police
Victorian Spatial Council
Voice on the Net Coalition Europe

The Department also received a number of confidential submissions which are not listed in this table.

The submission process

The following information was made available about how submissions could be made to the IPND Review:

Closing date for submissions: **16 December 2011**

Submissions were to be lodged in the following ways:

Email: IPND.review@communciations.gov.au

Post: IPND Review

Department of Communications

GPO Box 2154

Canberra ACT 2601

Enquiries about this report may be directed to the email addressed specified above.

Publication

Submissions will be made publicly available, including on the Department's website. The Department reserves the right not to publish any submission, or part of a submission, which in its view, breaches applicable laws, promotes a product or a service, contains offensive language, or that may offend or vilify sections of the community. Publication of a submission is not an indication that the Department endorses the content of that submission.

In making a submission, you provide the Department with a permanent, irrevocable, royalty-free, worldwide, non-exclusive licence (including a right of sublicense) to use, reproduce, adapt, communicate and exploit your submission both online and in any other related documents (for example, in a future discussion paper or report).

Confidentiality

Submissions will be treated as non-confidential unless the respondent specifically requests otherwise. Email disclaimers will not be considered sufficient. Submitters of material marked as confidential must do so on the understanding that submissions may be released where authorised or required by law or for the purpose of parliamentary processes. The Department will strive to consult submitters of confidential information before that information is provided to another body or agency. The Department cannot guarantee the confidentiality of information released through these or other legal means.

Privacy

The Department is committed to protecting your privacy. The Department has obligations under the *Privacy Act 1988* (the Privacy Act). In particular, the Privacy Act contains the Australian Privacy Principles (the APPs) which govern how the Department collects, uses and discloses personal and sensitive information, and how individuals can access and correct records containing their personal or sensitive information.

You may make a submission to the Department anonymously or by using a pseudonym. If you include any personal information and/or sensitive information in your submission, this information will be collected by the Department. By providing the Department with your personal information and/or sensitive information, you consent to the Department collecting, using and disclosing that information in accordance with this Collection Notice.

As part of considering your submission, the Department may use your personal and/or sensitive information for the purpose of developing policies in relation to the subject of this Report. Further, the Department may also disclose your personal information to the Minister, other government agencies and by placing your submission on the Department's website (see above).

If you do not consent to the Department's collection, use and disclosure of your personal information in accordance with this Collection Notice, please do not provide your personal information to the Department. If you have already provided your information to the Department, please notify us immediately (see contact details above).

The Department will use the personal information collected from you for the primary purpose it was collected. The Department's may use or disclose this personal information for another purpose (i.e. secondary purposes) if:

- you reasonably expect the information to be used for the secondary purpose;
- it is required or authorised by law or a permitted general situation exist under the Privacy Act;
- you give the Department permission; or
- the Department reasonably believes the use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

For further information, please see the Department's APP Privacy Policy here: http://www.communications.gov.au/about_us

Appendix 2 – Summary of 2012 workshop

On 6 March 2012, the former Department of Broadband, Communications and the Digital Economy hosted a workshop to discuss potential reform to the IPND. The following organisations participated:

Telstra	Attorney-General's Department
Optus	ACMA
Vodafone Hutchison Australia	OAIC
Communications Alliance	National Emergency Communications Working Group
ACCAN	NSW Police Force
Social Research Centre	Ambulance Service of NSW
Research Industry Council of Australia	Australian Privacy Foundation
Acceleon	

History of the IPND: successes, failures and missed opportunities

Workshop participants noted that the IPND had served the community well to date. Over 6.2 million records were processed per month, and it had 99.98 per cent availability—24 hours daily, seven days a week. However, participants agreed that the rapid evolution of telecommunications technology services (especially VoIP and IP-based services) are placing pressure on IPND arrangements, which were designed with traditional fixed telephone services in mind.

Privacy advocates at the workshop were concerned with function creep that had seen the IPND's uses grow beyond its core objectives. Privacy advocates also argued that access to the IPND by law enforcement agencies should be subject to strict administrative controls. Consumer advocates expressed the view that the public interest in allowing access to the IPND for critical users outweighed privacy concerns. Consumers expect an ambulance or the police or the fire service to arrive.

The workshop agreed that there was a lack of awareness about the IPND by consumers. Workshop participants considered that raising consumer awareness of the IPND would have a positive impact on its accuracy.

Privacy advocates at the workshop noted that any public awareness campaign should also provide justification for the use of subscriber data held in the IPND. It should also educate subscribers on how to take advantage of the services which use IPND data, as well as making them aware of the limitations of the system.

Some participants noted that the IPND was particularly inaccurate for business listings, and questioned the difference between the data that CSPs provide to the IPND and that which they provide to Sensis. However, it was contended that the data provided to the IPND and to Sensis was

identical and that the difference in data quality is because of the additional checks carried out on business data by Sensis.

Non-critical users of IPND data noted that some of the controls around IPND access were impractical. It was felt that greater access could be facilitated, without lowering the privacy protections for subscribers (for example, by allowing access to de-identified information for limited research purposes). Many participants argued that even this access would need to be determined by an independent third party, such as the ACMA, on a case-by-case basis.

It was also noted by some IPND users that the IPND had missed the opportunity to have other secondary data available—for example, next-of-kin information. Participants argued that any additional secondary data should only be included on a voluntary basis.

Practical changes to the IPND

It was generally agreed by participants that IPND accuracy could be improved if subscribers were allowed to view their own IPND details online, although the practicalities and security of access would need careful consideration.

It was also considered that better auditing processes would assist in improving the accuracy of the database and may also provide stronger incentives for CSPs to keep information in the IPND up-to-date.

Participants argued that IPND data should be used to update the DNCR. Participants suggested that access to high-level location information for unlisted numbers be allowed for LDCS, to enable consumers with unlisted numbers to take advantage of these services. Such information would only be used within networks and would not be released to end-users.

The workshop discussed other ways that the emergency services might get information—for example, by developing mobile applications for smartphones to automatically deliver location information, finding a way to link IP addresses with subscribers and utilising social media platforms. It was noted that if smartphone applications were introduced to provide caller information directly to the emergency call service, then data sources such as the IPND would have less relevance. The workshop agreed that irrespective of what telecommunications technology is used, the information needs of critical IPND users remain, and there must be a system, database or process to provide this information.

Workshop participants agreed that, from a technical point of view, Telstra had managed the IPND effectively for the last 15 years. Over this time the IPND had very little down time, which is a fundamental quality needed by many critical users, such as the Triple Zero emergency call service.

There were complaints that access by non-critical users was slow and expensive. Some participants noted that there was a least a perceived conflict of interest in having Telstra as the IPND manager and the owner of Sensis, publisher of the White Pages®. It was suggested that the IPND manager should have more responsibility for the accuracy and integrity of IPND data.

It was also suggested that the management of the IPND could be split between the provision of the IPND infrastructure, and the actual operation of the database. If implemented, then the operation of the database could be put to tender by government while maintaining the availability of the underlying infrastructure.

New and ongoing needs of IPND users

As the telecommunications industry has evolved, the IPND has become less capable of meeting some of the information needs of critical users.

There were a range of qualities about the IPND that were considered successes—for example, that the IPND is largely automated, updated regularly, is reliable, is accessible and does not impose a cumbersome compliance burden on industry. Any new solution that incorporates a broader range of telecommunications services should use these characteristics as a benchmark.

It was agreed by workshop participants that IPND information is sensitive and needs access control to protect the privacy of subscribers. Privacy stakeholders asserted that the principles guiding any proposed reform to the IPND must include data integrity, subscriber choice and subscriber privacy. The principles must work out where to draw the line on use of the IPND and disclosure of data, plus measures to ameliorate negative privacy impacts.

The privacy stakeholders at the workshop agreed that the existing privacy protections under the Telecommunications Act and the TIA were good security protections for the IPND in its current form and should be retained.

Appendix 3 – Summary of 2014 Stakeholder meeting

On 18 June 2014, the Department of Communications held a stakeholder meeting to discuss proposed recommendations to the review and next steps. Attendees were from the following organisations.

Acceleon	Newspoll
Association of Market and Social Research Organisations	Office of the Australian Information Commissioner
Attorney-General's Department	Optus
Australian Communications and Media Authority	Samplepages
Australian Communications Consumer Action Network	Telecommunications Universal Services Management Agency
Australian Federal Police	Telstra
Australian Privacy Foundation	The Social Research Centre
Communications Alliance	Vodafone Hutchison Australia
Industry Number Management Services	Voxbox
NBN Co	

Mr Arthur Marsh, an individual who had previously made a submission to the review, also attended.

Meeting summary

The Department provided an overview of the IPND review process which had investigated the ongoing need for the current IPND and whether the current regulatory and management processes could be improved.

The initial result of the review was a proposal to transition of the IPND to a new system with increased functionality, including the ability to incorporate dynamic location information for critical users. This proposal was discussed with key stakeholders, but did not receive broad support, primarily because of concerns about the costs versus benefits of developing a new system. As a result of these consultations, the Department now considers that the current IPND should be retained for the medium term, and that measured improvements should be made to the current system. These improvements would be to:

- extend access to certain limited elements in the IPND to a broader range of data users, such as the ABS and market researchers where it could be shown that this was in the public interest
- adopt measures to improve the accuracy and quality of data

- streamline the rules for the production of public number directories from the IPND
- improve transparency of the management of the IPND by Telstra in its role as IPND Manager.

There was general agreement among stakeholders at the meeting that the above approach achieved an appropriate balance between the relevant considerations.

It was also agreed that the need to transition to a new system should be revisited once the current review of the Emergency Call Service has been completed.

In relation to particular proposals, the following points were made during the meeting:

It was noted that some users do not have access to the Data User Query Form (DUQF) which enables automated notification of problems with data. Acceleon noted that there is no clarity about what happens to the DUQF when submitted. Telstra suggested that the development of a web portal could address these issues. Telstra also noted that maintaining data security would be critical in making such a change. Optus noted that there was a need to consider data providers as part of the customer-CSP-Manager loop in terms of improving accuracy. VHA questioned the claims about data accuracy noting that the fact that data is not what a particular data user thought it should be does not necessarily reflect an inaccuracy.

The research community noted that there was no validation of address information at the point of collection and that customers should be made aware of the benefits of maintaining accurate information. The Communications Alliance stated that a project on customer information obligations is underway and could be coordinated with the IPND review outcomes.

It was noted that technological changes, such as the implementation of push soft errors and new applications enabling the use of GPS data by emergency services, could help to address the issue of mobile location.

There was discussion about discrepancies in information between White Pages® data and the IPND. One industry participant noted that the White Pages® and the IPND have different purposes and are fed independently. It was noted that it would be inappropriate to try and cross check them against each other and as such the data contained in each is often likely to differ. White Pages® information is provided by a person or business specifically for directory purposes and may often contain information that does not correlate with either the name of the telecommunications service account holder (for example, the end-user of a particular number may be a different person to the account holder, or - for companies, the account name is in a business name, not a trading name, which a business can have many of), or the address may be different for services which have no fixed location, such as nomadic VoIP and mobiles which rely on the address provided by the customer. Telstra also noted that customers may provide an address for aspirational purposes, or otherwise. VHA noted that IPND information is a reflection of the name and physical address of the account holder and should not be compared to a product such as White Pages® with a different purpose.

VHA also raised the issue of address validation software not necessarily reflecting information provided by customers due to it usually being updated quarterly. VHA noted that it uses a multitude of sources to try and validate address data quality, including specialised address validation software and online services such as Google maps and Whereis to ensure that a ‘valid’ address was captured.

It was suggested that the IPND Code could be amended to include an obligation that would require CSPs to alert subscribers of their IPND information. On this point, Communications Alliance indicated that industry had not had an opportunity to consider this change as yet, but noted that in line with the Government's deregulation agenda, it had undertaken to consider how the provision of information to customers could be streamlined. This option could be considered in this context.

More broadly, Telstra stated that it is has been considering improvements that could be made to the IPND after the review is complete, but that it needs certainty to progress these.

Action item

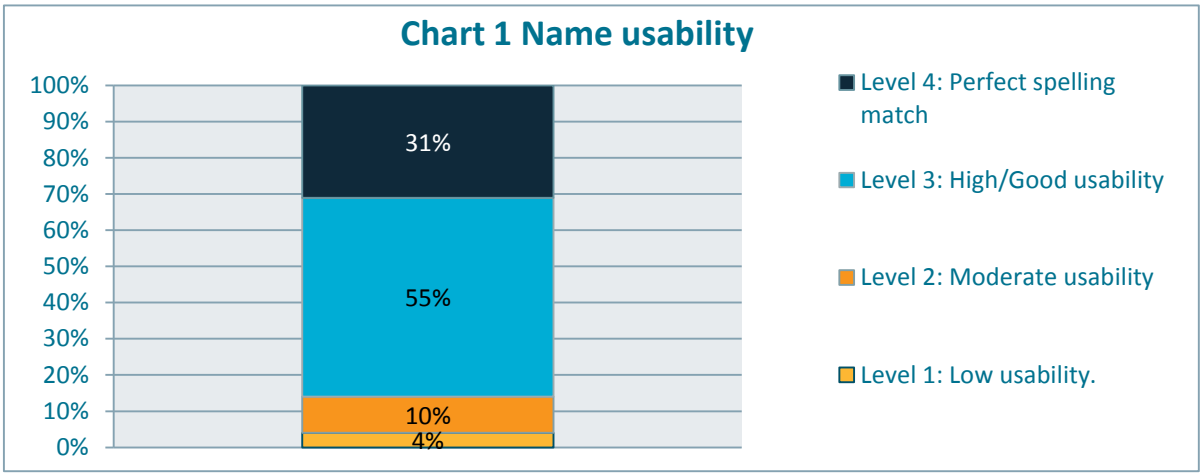
The Department sought any final comments and suggestions from stakeholders on the proposed recommendations, to assist in finalising advice to Government. All participants were invited to make comment on the draft recommendations in writing by **Tuesday 22 July 2014**.

Submission: Outcome post 22 July 2014.

Eleven written submissions were received from participants. These were broadly supportive of the proposed direction, and the draft report was updated to reflect comments received during this final round of consultation.

Appendix 4 – Results of IPND accuracy study

Chart 1 shows the usability of name information from the IPND. Name usability was measured as the likelihood that the information would be usable to an IPND user. The scale ranges from 1, meaning low usability to 4 meaning a perfect match.



The majority of entries rated at level 3 (with high usability) had first name information in the surname field. The information was correct, but it had been coded into the incorrect field by the CSP or data provider. While this would not impact the ECS, there could be an impact on law enforcement and national security agencies (who may wish to search by surname field).

Chart 2 shows the level of name usability by cohort. This shows that there was almost no difference in name usability of entries for metro/non-metro subscribers. Businesses and mobile entries were both found to have significantly higher percentage of entries at level 4 and level 1. That is, business and mobile entries were more likely to have accurate name information, but when it was incorrect, it was more likely to have more serious errors. Interestingly, taking levels 3 and 4 together, residential mobile entries had the *highest* accuracy out of all the tested cohorts.

Residential landline entries had significantly fewer entries at level 4 (15%) and level 1 (2%). This is the inverse of the business and mobile cohorts, and reflects that many residential and landline entries had first name information entered into the surname field.

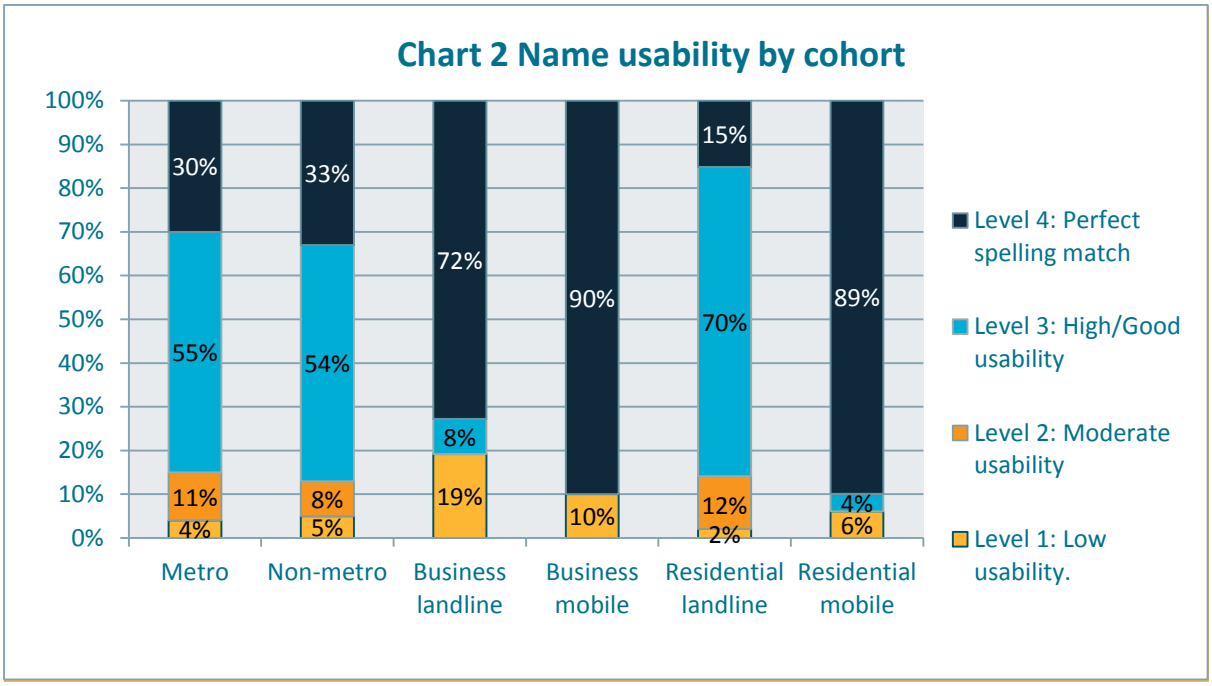


Chart 3 shows that a perfect match for name usability is highest for subscribers who moved into their current address 2-3 years ago. Name usability appears to have reduced since then – the percentage of level 1 and 2 entries combined is at 11% for subscribers who moved into their residence less than 1 year ago.

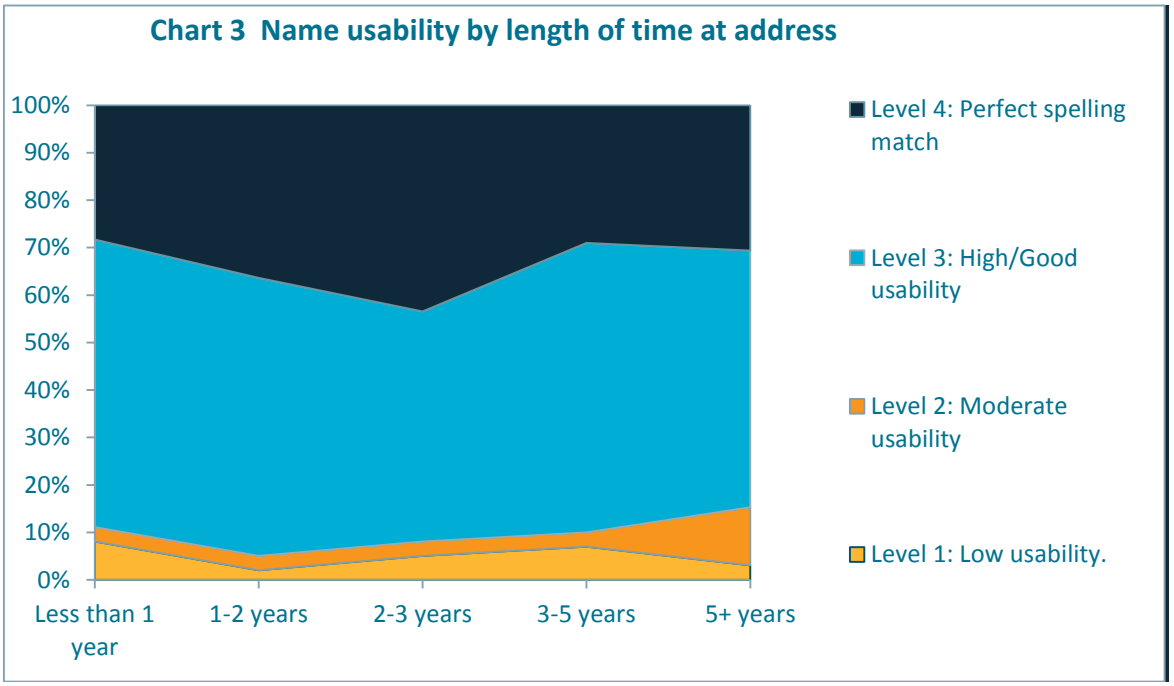


Chart 4 shows the impact that telephone payment method had on name usability. Interestingly, this data shows that online payment actually had a positive impact on name usability, although the difference between over the phone and online payments was not significant. Face to face payment had a significantly elevated percentage of level 2 entries.

Awareness had no statistically significant impact on the likelihood of accurate name information in the IPND.

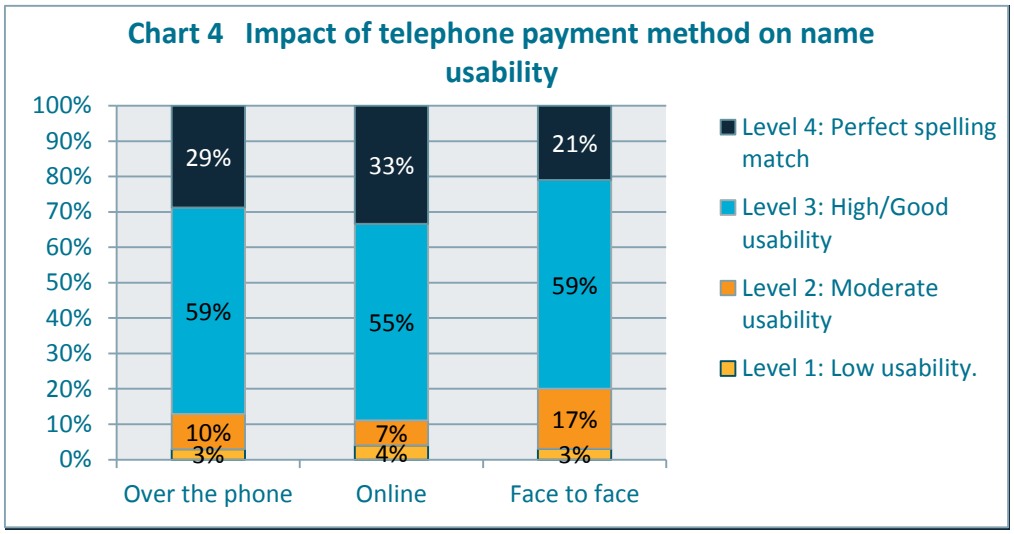
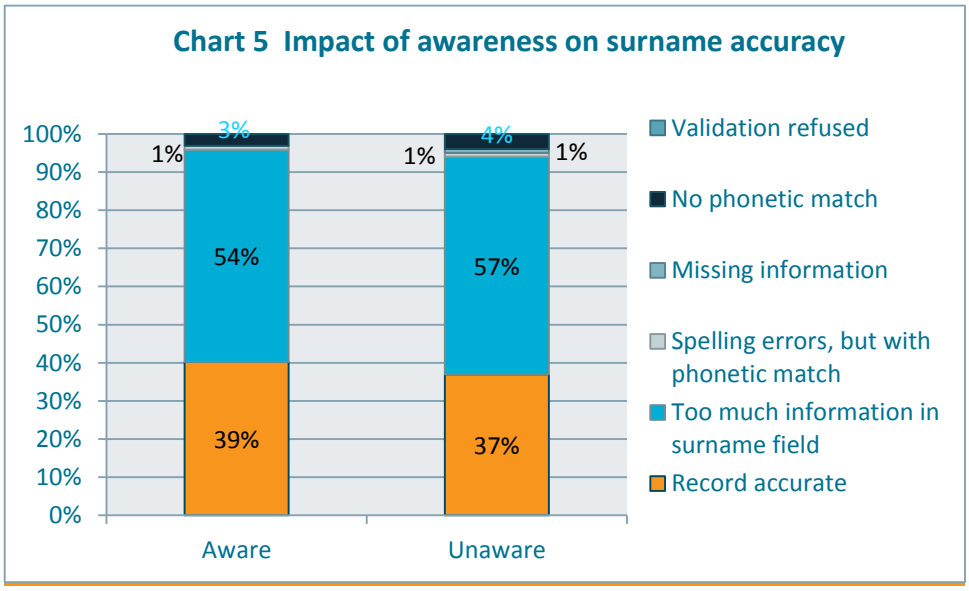


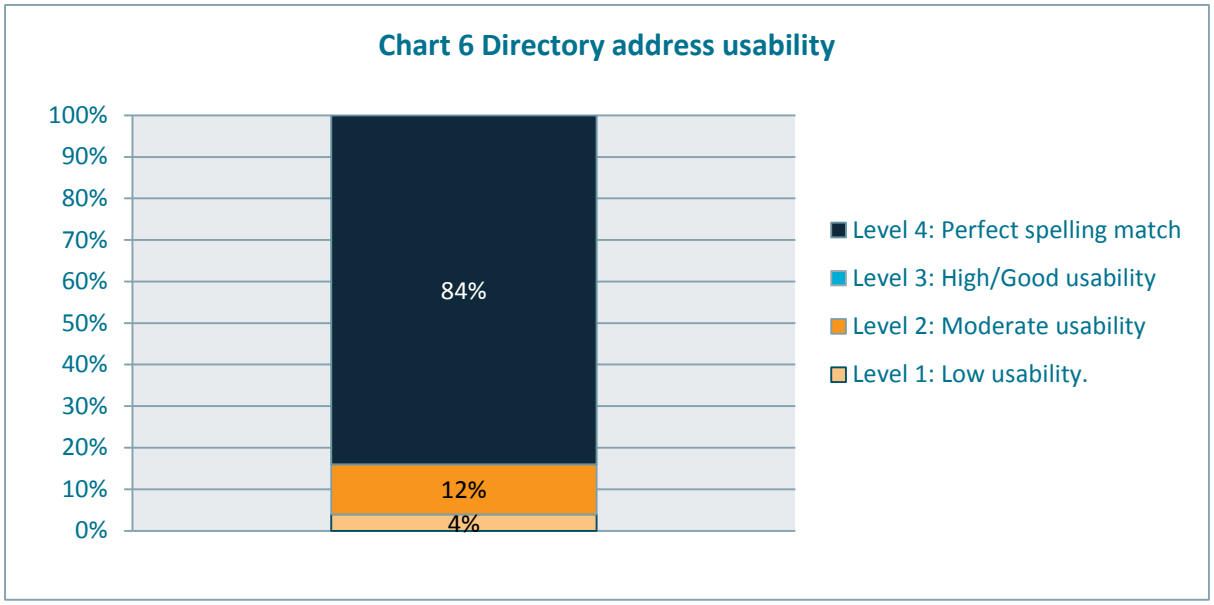
Chart 5 demonstrates the impact of awareness on surname/business name information

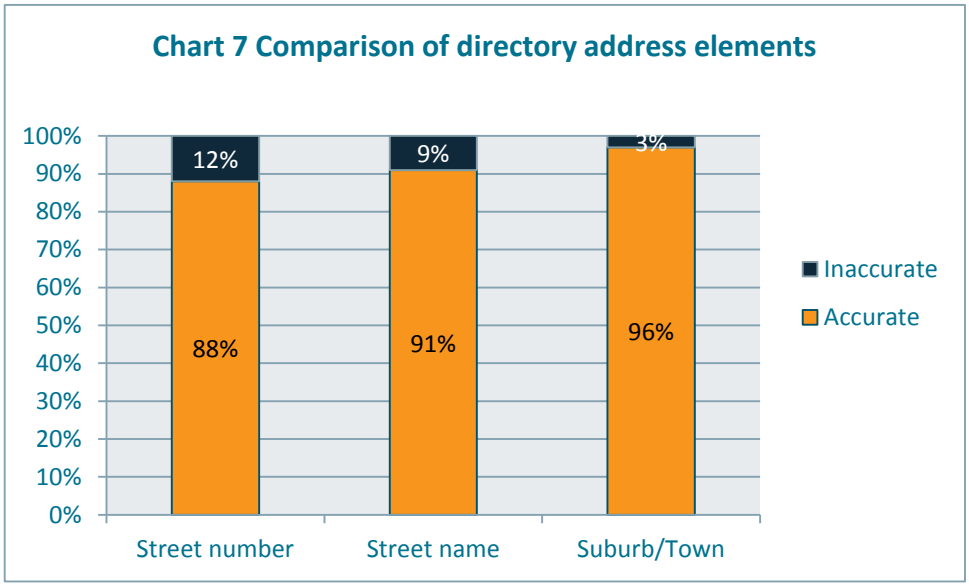


Directory address information

Chart 6 shows the usability of directory address information from the IPND. Directory address usability was measured as the likelihood that the information would be usable to an IPND user.

Overall, directory address was accurate for 84% of records. Approximately 1 in 6 records contained incorrect or missing information that would limit its usability for the production of directory products, the routing of calls for LDCS or research. The correlation between directory address and service address is not known, although a comparison between directory address, length of time at address and data from the ACMA's accuracy audits suggests that it is likely to be relatively high.





The accuracy of different directory address elements varied. Suburb information was more likely to be accurate than street name or street number (including sub-unit number). While Chart 7 demonstrates the differences between the different address elements, the table below provides a breakdown of the most common types of errors associated with street name and number.

Street number	
Error type	Prevalence
Incorrect street number	6%
Missing street number	3%
Missing/incorrect apartment number	2%
Incorrect street and apartment number	2%
Street name	
Error type	Prevalence
Spelling errors, but with phonetic match	1%
Suffix error	0[142]%
Missing street name	4%
No phonetic match	4%

Chart 8 shows directory address usability by cohort. These results are quite different to the Name usability results by cohort, presented above at Chart 2.

Metropolitan and residential landline subscribers had significantly more entries at level 4 (87% and 86% respectively) than other cohorts. Businesses landlines, business mobiles, residential mobiles and non-metro subscribers were significantly more likely to have less usable directory address information.

The errors in relation non-metro subscribes are potentially as a result of confusion about rural addressing, either by the relevant CSP or the subscriber.

[142] Rounded down. N=13.

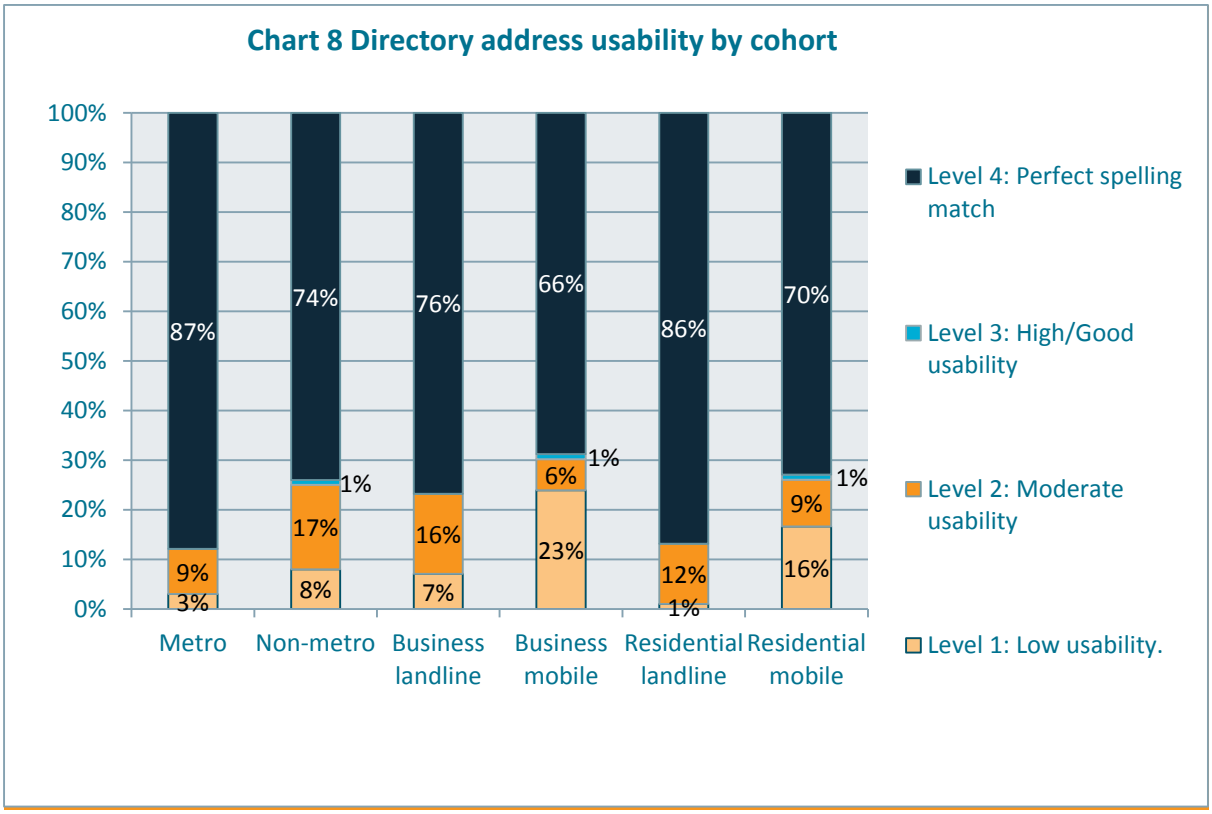


Chart 9 shows that directory address usability is at a low point for subscribers who moved into their current address 2-3 years ago. This result is almost the inverse of the result at Chart 3 above.

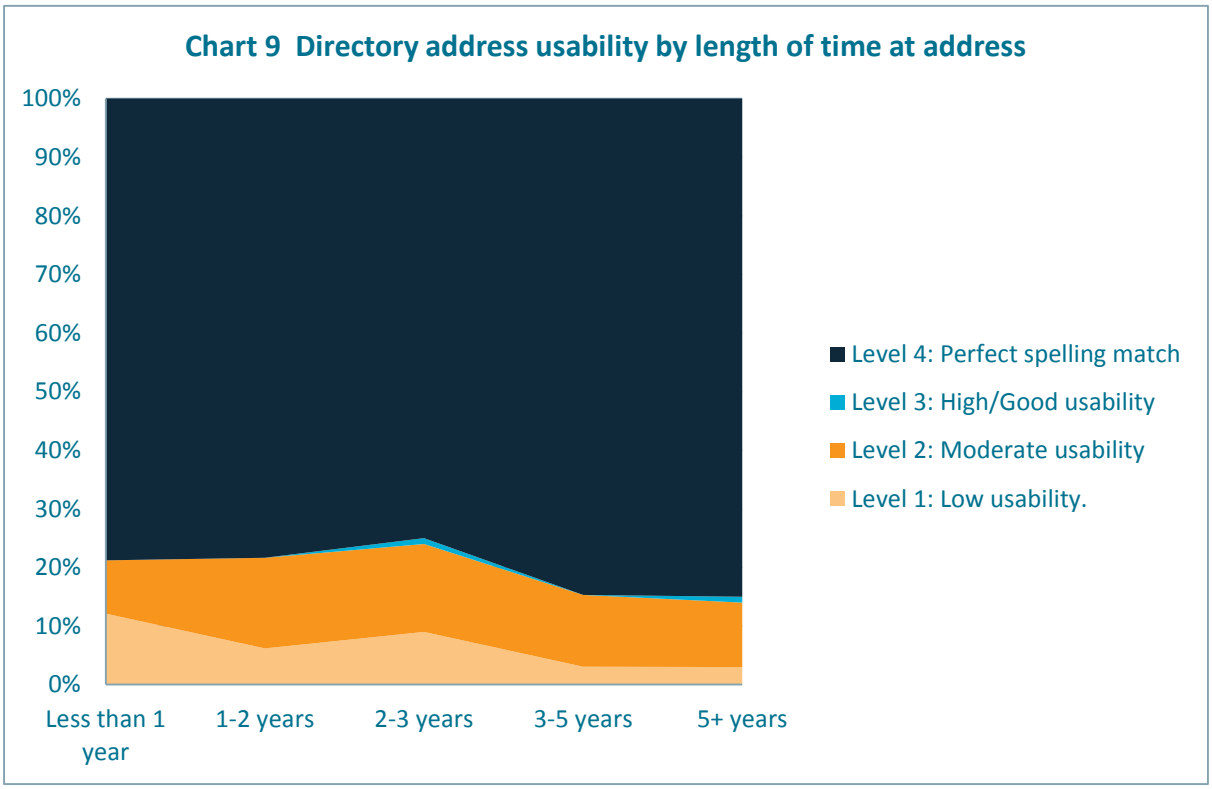


Chart 10 shows the impact that telephone payment method had on name usability. This shows that telephone payment method had almost no impact on directory address usability.

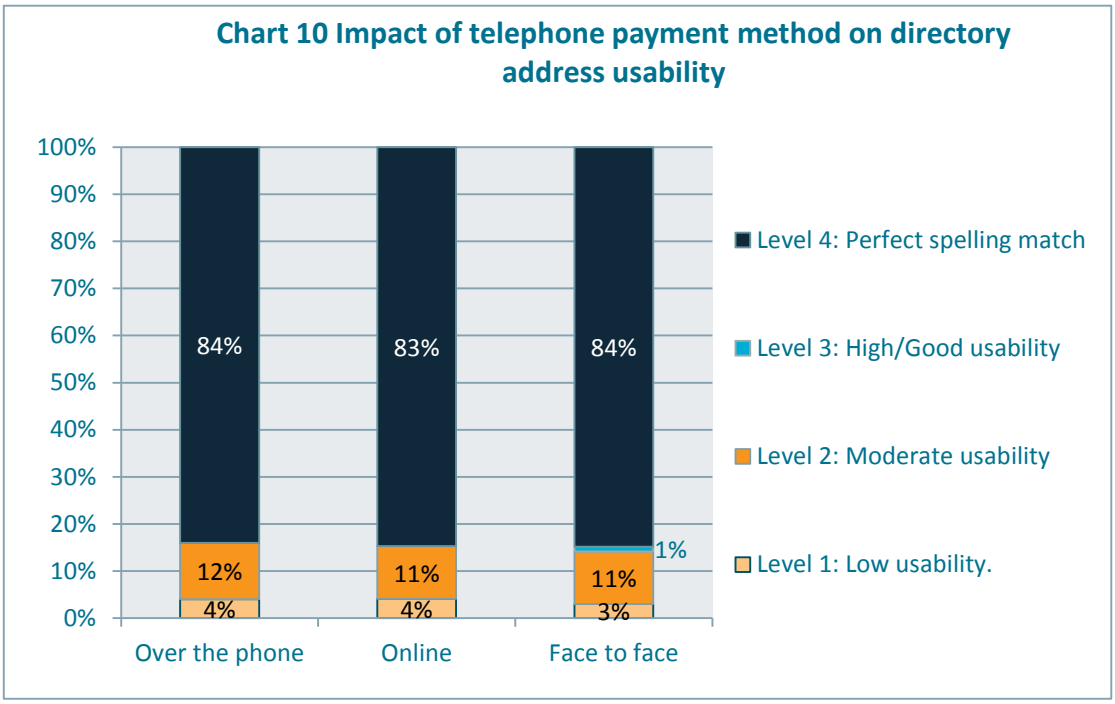
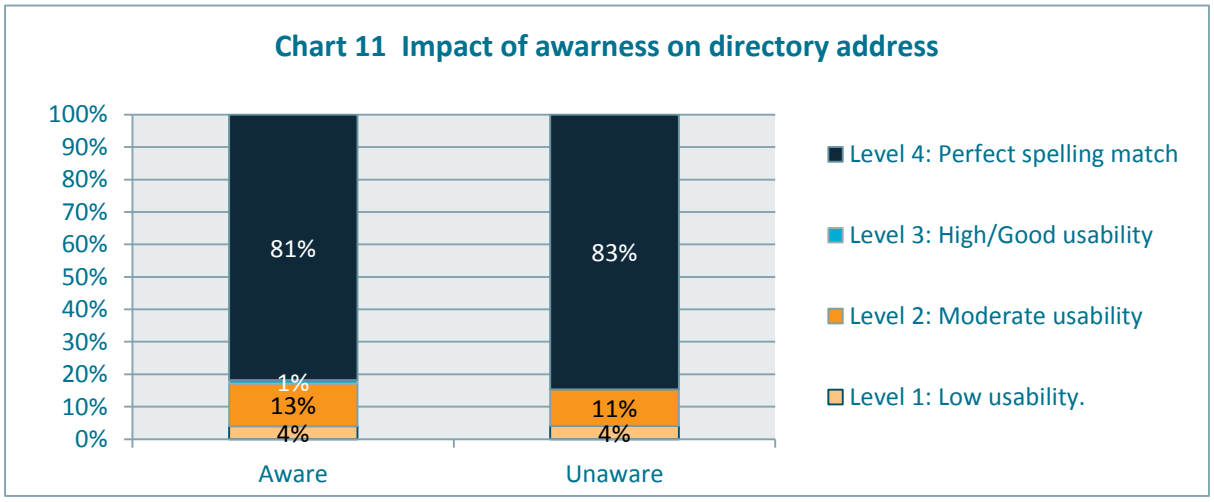


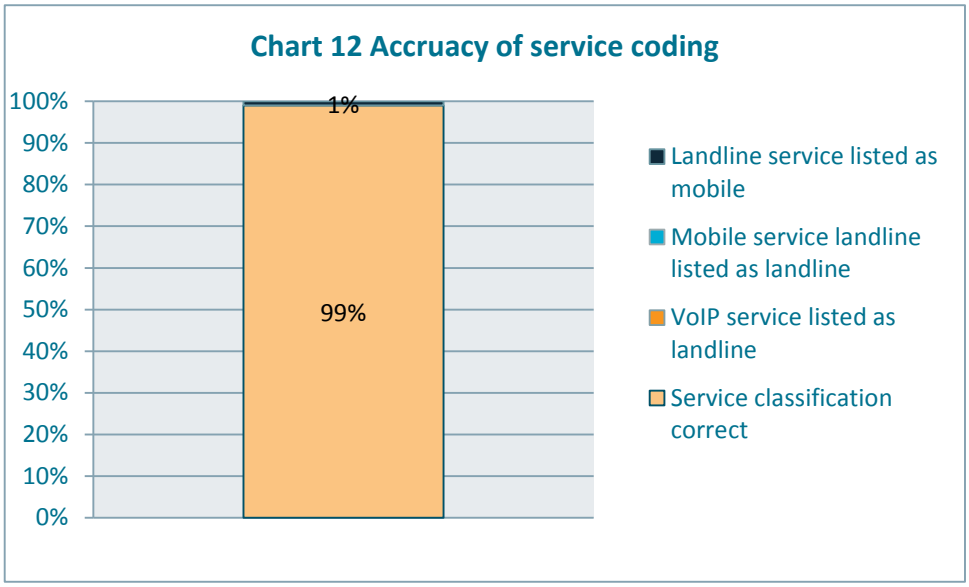
Chart 11 shows that (consistent with Chart 5 above) awareness had no perceptible impact on the likelihood of accuracy. Subscribers who were aware of the existence on the IPND were no more likely to have more usable directory address information than subscribers who were unaware of the IPND.

Given the very strong correlation between Charts 5 and 11, it is hypothesised that even where a subscriber is aware that of the importance of the IPND, there is no accessible way for them to improve the accuracy of their own records.



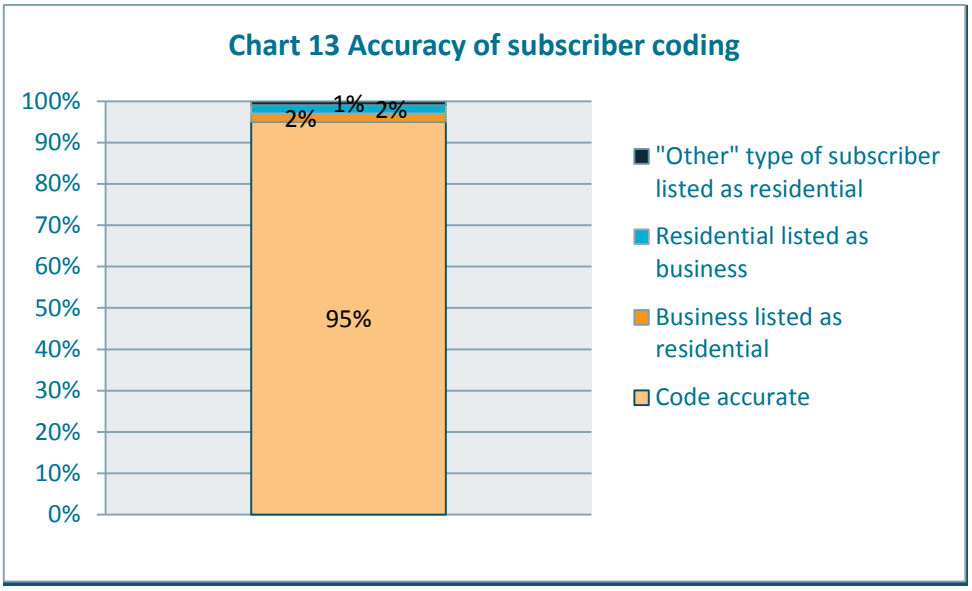
Accuracy of service coding

Chart 12 shows that, overwhelmingly, service coding appeared to be correct. 99% of respondents reported that their service had been correctly coded in the IPND. A very small number (n=11) of respondents reported that their VoIP number was incorrectly listed in the IPND as a traditional landline service. It is conjectured that this figure is under represented, on the basis that some subscribers may not have the expertise to identify whether their service is VoIP or not. It is not known whether the Alternative Address Flag (AAF) was correctly coded in these cases (this was one of the IPND data elements that the study was not able to access).



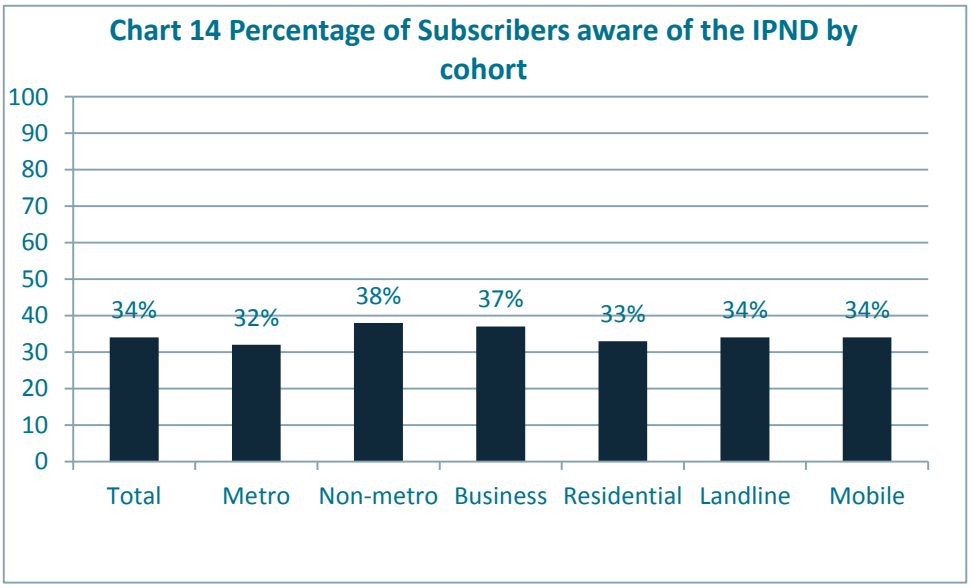
Accuracy of subscriber coding

Chart 13 shows that generally, subscribers were coded accurately. Business landlines and mobiles were at a significantly higher risk than other cohorts at having incorrect coding, either as being coded as a residential number or being coded as an 'other number' (i.e. coded as a charity or governmental organisation).



General level of awareness between cohorts

Chart 14 shows that 34% of respondents indicated that they were aware that their telephone company provided details to a government database that is used for the Triple Zero emergency call service and the EWS. This level of awareness was much higher than hypothesized prior to the IPND accuracy study. There was no significant variation between cohorts.



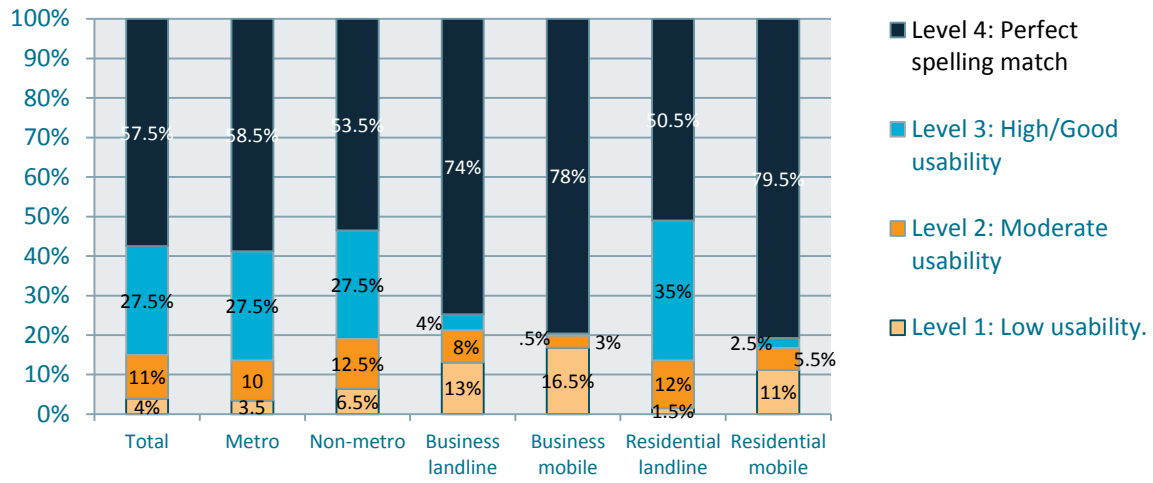
Results overall

Chart 15 shows the accuracy of the IPND overall, taking both name and directory address usability into account.

These results show that, overall, records for business and mobiles numbers were of significantly higher accuracy than those of other cohorts. It should be noted that only listed mobile numbers were included in the study and this result may not be representative of records for all mobile numbers, most of which as unlisted. The very low results of the residential/landline cohorts (which were the largest cohorts) strongly influenced the overall total of 57.5%, or 85% if levels 3 and 4 are

taken together.

Chart 15 Directory address and name usability by cohort



Appendix 5 – Sample IPND Entry

#	Field name	Description	Example
1	Record Type	There are three basic parts of the database, the header, the trailer and the actual data. This line identifies the header (or HDR).	HDR
2	File Type	Identifies the kind of file- i.e. IPND upload (IPNDUP) etc.	IPNDUP
3	File Source	Identifies the data provider's source system (five character code).	ABCDE
4	File Sequence No.	Identifies each record in relation to others from the source file.	0000001
5	File Creation Start	Date and time that file was created (in YYYYMMDDHHMMSS format).	20110901090101
6	Filler	Padding.	Blank
7	Record Delimiter	New line.	New line
1	Public Number	The public telephone number.	0262711000
2	Service Status Code	Whether the service is connected (C) or Disconnected (D)	C
3	Pending Flag	Identifies whether a change to the record is going to happen at a future time. Either True (T) or False (F).	F
4	Cancel Pending Flag	Identifies whether a pending flag is to be cancelled. Either True (T) or False (F).	F
5	Customer Name		
5.1	Customer Name 1	Company or Surname.	Department of Communications
5.2	Customer Name 2	Second company name or given name.	
5.3	Long Name	Characters that do not fit in Customer Name 2.	
5.4	Customer title	Customer title.	
6	Finding Name		

6.1	Finding Name 1	Name for directory purposes.	Department of Communications
6.2	Finding Name 2	Given name or initials/Company.	DoC
6.3	Finding Title	Title for directory purposes.	
7	Service Address		
7.1	Service Building subunit		
7.1.1	Service Building Type	Type of premises at service address.	
7.1.2	Service Building 1st Nr	First street number.	
7.1.3	Service Building 1st Suffix	First suffix.	
7.1.4	Service Building 2nd Nr	Second street number.	
7.1.5	Service Building 2nd Suffix	Second suffix.	
7.2	Service Building Floor		
7.2.1	Service Building Floor Type	Building floor type.	
7.2.2	Service Building Floor Nr	Floor number.	
7.2.3	Service Building Floor Suffix	Floor number suffix.	
7.3	Service Building Property	Building name.	
7.4	Service Building Location	Location of the building.	
7.5	Service Street House		
7.5.1	Service Street House Nr1	Building Number.	38
7.5.2	Service Street Nr 1 Suffix	Building number suffix.	
7.5.3	Service Street Nr 2	2nd number associated with the building.	

7.5.4	Service Street Nr 2 Suffix	2nd number suffix.	
7.6	Service Address Street		
7.6.1	Service Street Name 1	Name of street.	Sydney
7.6.2	Service Street Type 1	Abbreviation of street type.	Ave
7.6.3	Service Street Suffix 1	Suffix of street (i.e. North)	
7.6.4	Service Street Name 2	Name of street that does not fit at 7.6.1.	
7.6.5	Service Street Type 2	Abbreviation of street type.	
7.7	Service Address Locality	Suburb or town.	Forrest
7.8	Service Address State	State or territory.	ACT
7.9	Service Address Postcode	Postcode.	2603
8	Directory Address		
8.1	Directory Building subunit		
8.1.1	Directory Building Type	Type of premises for directory listing.	
8.1.2	Directory Building 1st Nr	First building number.	38
8.1.3	Directory Building 1st Suffix	First building suffix.	
8.1.4	Directory Building 2nd Nr	Second building number.	
8.1.5	Directory Building 2nd Suffix	Second building suffix.	
8.2	Directory Building Floor		
8.2.1	Directory Building Floor Type	Building floor type.	
8.2.2	Service Building Floor Nr	Floor number.	
8.2.3	Service Building Floor Suffix	Floor number with suffix.	

8.3	Directory Building Property	Building or property name.	
8.4	Directory Building Location	Building location for directory (i.e. rear etc.)	
8.5	Directory Street House		
8.5.1	Directory Street House Nr1	Building Number.	38
8.5.2	Directory Street Nr 1 Suffix	Building Number suffix.	
8.5.3	Directory Street Nr 2	2nd number associated with the building.	
8.5.4	Directory Street Nr 2 Suffix	2nd Building Number suffix.	
8.6	Directory Address Street		
8.6.1	Directory Street Name 1	Name of street.	Sydney
8.6.2	Directory Street Type 1	Street type abbreviation.	Ave
8.6.3	Directory Street Suffix 1	Suffix part of street.	
8.6.4	Directory Street Name 2	Name of part of street that does not fit into Directory street name 1.	
8.6.5	Directory Street Type 2	Suffix part of street.	
8.6.6	Directory Suffix 2	Suffix part of street.	
8.7	Directory Address Locality	Suburb or town for directory.	Forrest
8.8	Directory Address State	State or territory.	ACT
8.9	Directory Address Postcode	Postcode.	2603
9	List Code	Whether the customer has requested to be listed (LE), unlisted (UL) or has a suppressed address (SA).	LE

10	Usage Code	Information about the entity using the number (R-Residential, B-Business, G-Gov, C- Charity, N- Not Available).	G
11	Type of service	Information about the kind of service.	FIXED
12	Customer Contact		
12.1	Customer Contact Name 1	Surname.	Citizen
12.2	Customer Contact Name 2	Given name.	John
12.3	Customer Contact Nr	Telephone number of customer contact.	026271XXX
13	Carriage service Provider Code	Identifies the CSP. Provided by the IPND manager.	000001
14	Data Provider Code	Identifies the data provider. Provided by the IPND manager.	000001
15	Transaction date	Date of the transaction (in YYYYMMDDHHMMSS format).	20110901080101
16	Service Status Date	Date that the record was created on the data provider's system.	20110901080101
17	Alternative Address Flag	Indicates that the service address provided may not be where the service terminates.	
18	Prior Public Number	Customer's prior public number.	
19	Record Delimiter	New line.	
1	Record Type	There are three basic parts of the database, the header, the trailer and the actual data. This line identifies the trailer (or TRL).	TRL
2	File Sequence No.	Identifies each record in relation to others from the source file.	0000001
3	File Creation End	Date and time that the creation of the file was completed (in YYYYMMDDHHMMSS format).	20110901090110
4	File Record Count	A 7 digit number identifying the number of transaction records in the file.	0000000
5	Filler	Padding.	

6	Record Delimiter	New Line.	