Australian Government

Department of Broadband, Communications and the Digital Economy

The Integrated Public Number Database Review Workshop

Summary record

On 6 March 2012, the Department of Broadband, Communications and the Digital Economy hosted a workshop to discuss potential reform to the Integrated Public Number Database (IPND). The following organisations participated:

Telstra	Attorney-General's Department
Optus	Australian Communications and Media Authority (ACMA)
Vodafone Hutchison Australia	Office of the Australian Information Commissioner
Communications Alliance	National Emergency Communications Working Group
Australian Communications Consumer Action Network	NSW Police Force
The Social Research Centre	Ambulance Service of NSW
The Research Industry Council of Australia	The Australian Privacy Foundation
Acceleon	

The history of the Integrated Public Number Database (IPND)—its successes, failures and missed opportunities

Workshop participants noted that the IPND had served the community well to date. Over 6.2 million records are processed per month, and it has 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 carriage service providers (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 voluntarily.

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 to be carefully considered.

It was also considered that improved 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 Do Not Call Register. Participants suggested that access to high-level location information for unlisted numbers be allowed for location dependent carriage services (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 has 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

The IPND was designed for fixed lines. 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 and reasonably good privacy protections under the *Telecommunications Act 1997* and the *Telecommunications (Interception and Access) Act 1979* were good security protections that were inherent in the IPND in its current form and should be retained.