Draft of Telecommunications
Integrated Public Number
Database Legislative Instruments
2007

Submission to the Department of Communications, Information Technology and the Arts

March 2007
1. The Office of the Privacy Commissioner (the Office) is an independent statutory body whose purpose is to promote and protect privacy in Australia. The Office, established under the Privacy Act 1988 (Cth) (the Privacy Act) has responsibilities for the protection of individuals' personal information that is handled by Australian and ACT government agencies, and personal information held by all large private sector organisations, health service providers and some small businesses. The Office also has responsibilities under the Privacy Act in relation to credit worthiness information held by credit reporting agencies and credit providers, and personal tax file numbers used by individuals and organisations.

2. In addition, the Office has responsibilities under the Telecommunications Act 1997 (the Telecommunications Act) in relation to telecommunications industry Codes and Standards (Part 6) and monitoring compliance with the record-keeping requirements under that Act (Part 13 Division 5).

Contributions by this Office and general comments

3. The Office welcomes the opportunity to make a submission to the Department of Communications, Information Technology and the Arts (DCITA) on the draft legislative instruments relating to IPND access arrangements recently published for comment by DCITA under subsections 285(3), 285(4), 285(5), 295(N) and 295(P) of the Telecommunications Amendment (Integrated Public Number Database) Act 2006 (the IPND Amendment Act).

4. The Office has recently made a comment to the Australian Communications and Media Authority (ACMA) on the consultation draft of the Telecommunications Integrated Public Number Database Scheme 2007 (the ACMA IPND Scheme).

5. The Office has previously commented on the issue of access arrangements for the Integrated Public Number database (IPND) in its May 2004 submission to the (then) Australian Communications Authority’s Who’s Got Your Number? Regulating the Use of Telecommunications Customer Information Discussion Paper. The Office also made a submission to ACMA on the draft Telecommunications (Use of Integrated Public Number Database) Industry Standard 2005.

6. The use and disclosure of personal information held in the IPND is regulated by Part 13 of the Telecommunications Act. Currently, Part 13

allows use and disclosure for operator and directory assistance services, emergency service organisations and law enforcement agencies.

7. The new IPND access regime allows additional entities to gain access to the database for other public interest purposes as required by s 285(3) of the Telecommunications Act. In this submission the Office makes suggestions intended to assist in determining the ‘public interest’.

8. The Office is pleased that the IPND Amendment Act addresses the issue of unauthorised use of IPND information for commercial purposes, while retaining existing levels of access for essential services such as emergency services and law enforcement agencies. The Act achieves this outcome by defining what a Public Number Directory (PND) is and limiting how IPND information can be used and disclosed during the creation and publication of PNDs. Underpinning these provisions is the ACMA IPND Scheme, which places ACMA in a gatekeeper role. Drafting the Act in this way appears to provide a sound basis for protecting IPND information from misuse.

9. In respect of the legislative instruments, the Office notes that they include some privacy enhancing provisions, such as requiring access users to implement further protections where information will be sent outside Australia. However, the Office considers there are some areas where the legislative instruments could be further enhanced in terms of additional privacy protections.

10. In this submission, the Office has not commented on every legislative instrument, but has concentrated on those we consider may impact upon the privacy of the personal information held in the IPND, in particular those covering the Conditions for Authorisation; Criteria for Deciding Authorisation Applications; and Permitted Research Purposes.

11. The Office suggests that a review by DCITA, including public consultation, of the new IPND access regime would be beneficial in measuring the efficacy of the reforms. The Office suggests that this review be undertaken in two years. As part of this review, the Office suggests that DCITA should consider what regulatory mechanisms are available to deal with directory products produced from information sourced directly from telecommunications companies. The Office has commented previously about the need for consistent regulation of directory products5.

IPND data

12. The IPND is a comprehensive database of personal information of Australians which plays a number of critical roles for the Australian community. These roles include the provision of operator and directory assistance services and emergency and law enforcement purposes. The Office's view is that it is important that Australians maintain trust in the integrity and security of this important repository of personal information, making the need for adequate privacy protections particularly important.

5 Ibid pp9&11
Inclusion of customer data in the IPND

13. The initial circumstances in which individuals typically disclose their personal information to a telecommunications company is for the purpose of receiving a telephone service. Individuals’ expectations about the handling of their personal information will therefore, to a large extent, be set by this original transaction.

14. When an individual subscribes to a telephone service their personal information is automatically provided to the IPND Manager (Telstra) for inclusion in the IPND. This occurs because the carriage service providers (CSPs) are required by licence agreement to provide the information to the IPND Manager and the IPND Manager is required by the conditions of its carrier licence to enter the information in the IPND. These provisions ensure that the IPND is maintained in such a way as to achieve its public interest purposes.

15. Most individuals will understand and accept that their personal information may be published in a public number directory (PND), unless they request and, in most cases, pay for an unlisted number. Individuals may also understand that their personal information will be used for directory assistance, law enforcement and emergency services. However, individuals are less likely to appreciate that, due to the IPND access regime; the handling of their personal information does not end with their CSP providing it to the IPND manager, but may lead to their personal information being used in other contexts.

16. Recognising that many individuals in the community may not be aware of the way in which IPND data may be used under the IPND access regime, it is important that additional attention is given to ensuring the protection of individuals’ personal information in the IPND access regime.

Permitted research purposes

Primarily non-commercial

17. The draft instrument entitled *Telecommunications (Integrated Public Number Database – Permitted Research Purposes) Instrument 2007 (No.1)* (the Permitted Research Purposes instrument) is made under subsection 285(3) of the Telecommunications Act. It specifies the type of research that is in the public interest, and consequently, for which authorisation may be sought to access IPND data. The draft instrument specifies three types of permitted research, and specifies that they must not be conducted for a “primarily” commercial purpose.

18. The draft instrument entitled *Telecommunications (Integrated Public Number Database – Criteria for Deciding Authorisation Applications) Instrument 2007 (No.1)* (the Criteria for Deciding an Authorisation instrument) made under section 295N of the Telecommunications Act specifies that ACMA must be satisfied that proposed research is of the kind specified in the Permitted Research Purposes instrument.

19. The Office assumes that through the interaction of both of these instruments, ACMA must determine that proposed research is not of a primarily commercial nature. However, it is unclear to the Office how
ACMA will assess whether or not the research is for ‘primarily’ commercial purposes. The criteria or method of assessment does not appear to be dealt with either by the ACMA IPND Scheme or the legislative instruments.

20. The Office suggests that the term “primarily” could be removed from DCITA’s Permitted Research Purposes instrument at Item 4, Specification. Further, that an additional paragraph, excluding commercial research, be added to the Criteria for Deciding an Authorisation instrument.

21. More specifically, in relation to research regarding an electoral matter, the Office would suggest that the restriction placed on the use of other sources of personal information is taken into account by DCITA. An example of this is the Commonwealth Electoral Act 1918 (the Electoral Act), which allows research to be undertaken into electoral matters using information from the electoral roll that is provided by the Australian Electoral Commission. Section 91B of the Electoral Act includes a prohibition on using the information obtained from the electoral roll for “a commercial purpose”.

22. The Office would suggest that access to the electoral roll for research is a comparable circumstance to allowing access to the IPND data for research into electoral matters. The Office believes that consistent treatment should be applied to the use of the IPND for electoral research.

23. Accordingly, recognising the similarity of these two circumstances where researchers have access to a comprehensive data source, the Office suggests that amending the requirement at 4(b) to include that research “not be conducted for a commercial purpose” would be appropriate.

In the public interest

24. Subsection 285 (3) of the Telecommunications Act states that:

“The Minister may, by legislative instrument, specify kinds of research for the purposes of subparagraph (1A)(c)(iv). The Minister must not specify a kind of research unless the Minister is satisfied that the kind of research is in the public interest.”

25. Section 4(a) of DCITA’s Permitted Research Purposes instrument specifies “health or medical research” as one kind of research allowed for the purposes of subsection 285(1A)(c)(iv) of the Telecommunications Act.

26. The Office is concerned that there are no provisions within the legislative instruments to provide guidance so that the Minister may be satisfied that health and medical research carried out using IPND data is in the public interest. As mentioned above, the Criteria for Deciding an Authorisation instrument includes (at part 5(3) and 5(4)) specific criteria for ACMA to consider when deciding on an application for the permitted research purposes listed in sections 4(b) and 4(c) of the Permitted Research Purposes instrument. The criteria includes that ACMA must be satisfied that the researcher will use IPND data for the purposes listed in 285(1A)(c)(iv) of the Telecommunications Act.

27. The question of determining what is in the public interest in terms of health and medical research is often extremely complex. The Office notes that there are existing bodies who have determined standards for analysing
and approving medical and health research applications, such as, the Human Research Ethics Committee\(^6\) (HREC) which uses standards such as those in the *National Statement on Ethical Conduct in Research Involving Humans 1999*. The Office suggests that ACMA could investigate whether such a body could be included in their authorisation process.

28. In addition, the Office suggests that the phrase “in the public interest” is added to the health and medical research purpose at part 4(a) of the Permitted Research Purposed instrument. The Office also suggests that the term “health and medical research” be defined in this instrument. The Privacy Act, for example, defines medical research “to include epidemiological research”.

29. Alternatively, DCITA could add information about what the Minister would regard as in the public interest in relation to health and medical research in part 5 of the Criteria for Deciding Authorisations instrument.

**Privacy Act and the IPND access regime**

**Privacy regulation for the IPND access regime**

30. Ensuring that privacy protections apply to the personal information of individuals contained in the IPND is particularly important to assist in retaining community confidence in the integrity of the IPND.

31. The Office notes that, given the cross-jurisdictional nature of Australian privacy regulation, a number of agencies, organisations and individuals gaining access to the IPND under the new access regime, may have differing or no privacy obligations.

32. Australian Government agencies are covered by the Information Privacy Principles (IPPs) in the Privacy Act, as are ACT Government agencies. The information handling practices of many private sector organisations are regulated by the National Privacy Principles (NPPs). These organisations include businesses with a turnover greater than $3 million, as well as all businesses that provide a health service or trade in personal information.

**Exemptions in the Privacy Act**

33. In relation to the operation of the IPND access regime, two potentially relevant exemptions in the Privacy Act are the small business operator exemption in s 6C and the registered political parties and political acts and practices exemptions in s 7C.

34. Generally, a business with a turnover of $3 million or less (that is, a small business) would not fall within the jurisdiction of the Privacy Act and compliance with the NPPs unless, for example, that business trades in personal information.

35. The question arises as to whether or not an organisation that may be a small business as defined in the Privacy Act can continue to rely on that

exemption for personal information it has obtained through the IPND access regime.

36. The Office would suggest that as a result of some small businesses being granted authority to access IPND data they may not be able to rely on the small business exemption in the Privacy Act because they could be considered to be trading in personal information in accordance with s6D(4)(c) - (d).

37. Further, some small businesses may claim an exemption under s6D(7) of the Privacy Act. That section provides that an entity will not be prevented from being a small business operator due to the fact that they disclose personal information about another individual, if that disclosure is required or authorised by or under legislation. Section 303B of the Telecommunications Act allows for a disclosure or use of IPND information in accordance with Part 13 to be taken, for the purposes of the Privacy Act, as authorised by law.

38. The Office considers that the authorised disclosure provided for under s303B of the Telecommunications Act applies to the disclosure of personal information from the IPND by the IPND Manager and not the subsequent handling of that information by an authorised IPND data user.

39. On this basis, it would appear that authorised PND producers and researchers may need to comply with the Privacy Act in relation to their subsequent handling of the personal information they have received from the IPND Manager, regardless of the size of that business.

40. The Office also notes that authorised researchers undertaking research on electoral matters may believe they are exempt from coverage by the Privacy Act by the exemption in s 7C. However, organisations undertaking research of this type will need to carefully assess their activities against s7C as this exemption does not cover all political acts and practices by political parties.  

Proposed solution

41. The Office notes the privacy safeguards that have been incorporated into ACMA’s draft IPND Scheme and accompanying application forms as well as the ministerial instruments. These safeguards have in some cases provided additional privacy protections to those provided by the NPPs or IPPs, particularly in the areas of transborder data flows (in the Conditions of Authorisation determination) and the notice requirements in ACMA’s IPND Scheme.

42. However, though many authorised data users under the IPND access regime may fall within the coverage of the Privacy Act, the Office believes that there may be some potential gaps and uncertainty as set out above (at paragraphs 35-40) in relation to privacy protections for IPND data.

43. As well the type of information likely to be collected from individuals as part of the research permitted by the IPND access regime, particularly that specified at 4(a) and (b) of DCITA’s Permitted Research instrument could

---

7 See the Note at the end of s7C of the Privacy Act
be ‘sensitive information’ as defined in section 6 of the Privacy Act. This definition includes, for example, information about an individual’s political opinions or health information about an individual.

44. As a result of being able to collect this potentially sensitive personal information through using such a comprehensive data source as the IPND, the Office believes that there could be an argument to support the need to prescribe privacy provisions that will apply to all authorised IPND data users.

45. To that end, the Office suggests the following options:

   i. An amendment could be made to the Privacy Act such as the provision made in s 152 of the Anti-Money Laundering and Counter-Terrorism Financing (Transitional Provisions and Consequential Amendments) Act 2006. This section prescribes that the Privacy Act will apply to small businesses, which are reporting entities as defined in the Anti-Money Laundering and Counter Terrorism Financing Act 2006, to the extent of those activities.

   ii. Regulations could be made under section 6E of the Privacy Act to prescribe that small business operators, who are authorised IPND data users, will be treated as if they are an “organisation” under the Privacy Act.

   iii. The ‘Conditions for Authorisation’ determination could include that authorised users must comply with the provisions of the Privacy Act, or specifically the NPPs. For small businesses, this could be achieved by an authorised data user opting in, under s 6EA, under the Privacy Act.

   iv. The instruments could include a general requirement that all authorised data users must comply with the Privacy Act in relation to their information handling practices, except where the legislative instruments or ACMA IPND Scheme contains specific privacy provisions.

46. Some further examples of similar provisions that cover specific information handling activities can be found in relation to the handling Medicare and PBS claims information, and Tax File Numbers.8

47. The Office would welcome the opportunity to work with DCITA to create guidance material to inform and educate authorised IPND data users regarding their privacy requirements.

---

8 See, respectively, section 135AA of the National Health Act 1953 and Division 4 of the Privacy Act.
Key Recommendations

The Office believes it is important to protect individuals' information held in the IPND because individuals have limited control over how their personal information is used once it has been collected into the IPND. For this reason we suggest that the protections in the IPND access regime could be enhanced by implementing the following recommendations:

1. **Review**
   - The Office suggests DCITA review the efficacy of the IPND access reforms within two years and, as part of this review, whether consistent regulation of directory products has been achieved;

2. **Permitted research purposes**

   *Primarily non-commercial*
   - The Office suggests that the term “primarily” could be removed from DCITA’s Permitted Research Purposes instrument at Item 4, Specification. Further, that an additional paragraph, excluding commercial research, be added to the Criteria for Deciding an Authorisation instrument.

   *In the public interest*
   - The Office would suggest that DCITA could encourage ACMA to investigate whether a Human Research Ethics Committee (HREC) or equivalent body could assist them in relation to deciding authorisations for medical and health research applications.

   - The Office suggests that the phrase “in the public interest” is added to the health and medical research purpose at part 4(a) of the Permitted Research Purposed instrument.

   - The Office also suggests that the term “health and medical research” be defined in this instrument.

   - Alternatively, DCITA could add information about what the Minister would regard as in the public interest in relation to health and medical research in the part 5 of the Criteria for Deciding Authorisations instrument.

3. **Privacy Act and the IPND access regime**

   *Privacy regulation for the IPND access regime*
   - The Office submits that to address the problem of whether particular data users will be regulated by the Privacy Act, the IPND access regime could provide for
i. An amendment could be made to the Privacy Act such as the provision made in s 152 of the Anti-Money Laundering and Counter-Terrorism Financing (Transitional Provisions and Consequential Amendments) Act 2006.

ii. Regulations could be made under section 6E of the Privacy Act to prescribe that small business operators, who are authorised IPND data users, will be treated as if they are an “organisation” under the Privacy Act; or

iii. The ‘Conditions for Authorisation’ determination could include that authorised users must comply with the provisions of the Privacy Act, or specifically the NPPs. For small businesses, this could be achieved by an authorised data user opting in, under s 6EA, under the Privacy Act; or

iv. The instruments could include a general requirement that all authorised data users must comply with the Privacy Act in relation to their information handling practices, except where the legislative instruments or ACMA IPND Scheme contains specific privacy provisions.

1.