

2008-2009

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

**TELECOMMUNICATIONS AMENDMENT (INTEGRATED PUBLIC
NUMBER DATABASE) BILL 2009**

EXPLANATORY MEMORANDUM

(Circulated by authority of the Minister for Broadband, Communications
and the Digital Economy, Senator the Honourable Stephen Conroy)

TELECOMMUNICATIONS AMENDMENT (INTEGRATED PUBLIC NUMBER DATABASE) BILL 2009

OUTLINE

The Telecommunications Amendment (Integrated Public Number Database) Bill 2009 amends the *Telecommunications Act 1997* (Telecommunications Act) to allow information contained in the Integrated Public Number Database (IPND) to be disclosed and used in connection with the provision of telephony-based emergency warnings, and for the supply of Location Dependent Carriage Services (LDCSs).

The IPND is an industry-wide database of all residential and business phone numbers (both listed and unlisted) and associated subscriber information, including name and address information. The IPND was established and is maintained by Telstra as a condition of its carrier licence. All carriage service providers who supply carriage services to subscribers who have public numbers are obliged to provide to Telstra such information as it reasonably requires in connection with the fulfilment of its obligation to maintain the IPND.

Under its carrier licence conditions, Telstra is required to ensure that the IPND contains certain information about each telephone subscriber, including their name and address and whether the number is used for business, government, charitable or private purposes.

Section 276 of the Telecommunications Act effectively prohibits the disclosure or use of information released from the IPND in connection with the delivery of telecommunications services by carriers, carriage service providers or their contractors. However, a number of exceptions are specified in the legislation which allow disclosure for a number of reasons, including for the delivery of telecommunications services, the publishing of public number directories, emergency call purposes, and law enforcement purposes.

Emergency Warning System amendments

Under the Bill, Section 276 of the Telecommunications Act will be amended to allow data contained in the IPND to be disclosed to authorised persons to enable the provision of government initiated telephony-based emergency warnings.

The States and Territories have primary responsibility for emergency response measures. Arrangements for authorising and issuing warnings vary considerably between jurisdictions. Accordingly, the amendments will provide the Attorney-General, as the Minister with portfolio responsibility for emergency management issues, with powers to specify, by legislative instrument, who can use IPND information in the event of an emergency or disaster. This is likely to be primarily State and Territory Government officials, however, there is the flexibility for the Attorney to authorise other persons.

The Bill is drafted so that it allows for States and Territories to develop and operate jointly data management and emergency warning systems.

The amendments permit IPND information to be disclosed in the event of an emergency, or when an emergency is considered likely, according to the definition of emergency law as defined by the Minister with responsibility for emergency management. The term 'emergency law' will be defined through a legislative instrument which is likely to mirror or reference existing state and territory emergency laws.

Information obtained from the IPND may only be used for the purpose of providing warnings about specific emergency events. It is anticipated that these messages will generally be recorded voice messages providing appropriate advice to telephone subscribers about the nature of the emergency and any recommended actions.

Under the amendments, there is a requirement that reasonable steps be taken to ensure that the use or disclosure of IPND information does not adversely affect the normal operations of the telecommunications network. For instance, telephone subscribers in the geographic area affected must still be able to make outbound calls, especially to 000, while an emergency warning is being transmitted.

Division 3B contains a number of privacy protection provisions which are intended to ensure that subscriber data obtained from the IPND is not used or disclosed for any other purpose than to provide telephone-based emergency warnings in specific instances (including testing of systems to provide such warnings).

It will be an offence for an emergency management person to use or disclose any IPND information for any purpose not directly connected with the provision of telephone-based emergency warnings. Under the amendments an emergency management person will be permitted to use IPND information for the purpose of reasonable testing of whether, in the event of an emergency occurring, persons would be able to be alerted to that emergency.

Emergency management persons may either task their own agencies with issuing an emergency warning, or may delegate this task to a third party. In the event the task is delegated, it will also be an offence for the party to whom the task has been delegated to use or disclose any IPND information obtained for any purpose not directly connected with the provision of telephone-based emergency warnings.

In recognition of the sensitive personal information contained in the IPND and that both listed and unlisted numbers will be released, there are penalties of up to two years imprisonment for mis-use of the IPND data.

The amendments also contain accountability measures including a reporting requirement for any emergency management person who activates a telephony-based emergency warning. Emergency management persons will be required to report each disclosure of IPND information to the Minister administering the *Administrative Decisions (Judicial Review) Act 1977* and the Australian Communications and Media Authority (ACMA) as soon as practicable after each disclosure occurs.

Details of these reports will include the nature and location of the emergency, the number of telephone numbers that were disclosed, the date when the disclosure occurred, and the number of persons to whom the information was disclosed and for

what reason. The intention of these reporting requirements is to allow for any mis-use of IPND information by any person to be identified as soon as possible.

Emergency management persons will also be required to report annually to ACMA and to the Office of the Privacy Commissioner on each disclosure. The reports will include a description of the emergency, date and location, the volume of subscriber numbers disclosed and to whom for the purpose of issuing emergency warnings. This provision is similar to the current requirement in the Telecommunications Act for disclosures of IPND data, for example, in relation to law enforcement activities, to be reported on.

Location Dependent Carriage Service amendments

A Location Dependent Carriage Service (LDCS) is a carriage service that depends for its provision on the availability of information about the geographic location of the caller in order to route the call to a particular destination, normally the closest destination to the caller. Examples of these types of services include pizza delivery services and taxi services. They are generally services provided using 13 or 1300 numbers.

Generally, a carriage service provider (CSP) will only hold information about callers who are its own subscribers. The IPND provides access to the phone numbers and addresses of subscribers on all networks, thereby allowing a CSP providing an LDCS to route the call to the premises of the business nearest the location of the caller, regardless of whether or not that caller is one of its own subscribers.

In the provision of LDCS, location information from the IPND is geo-coded in order to allow the telephone number to be located geographically. The IPND and geo-code data is stored in a routing table, allowing providers to automatically route calls from these numbers to the relevant business premises closest to the location of the caller.

Current arrangements for callers with unlisted numbers, including silent numbers and mobiles will continue under the amendments. Calls to LDCS numbers from these subscribers are directed to an operator, who enquires about the caller's location and manually routes the call to the nearest relevant business.

Currently, the Telecommunications Act only permits access to the IPND for the provision of LDCSs by carriers and CSPs, and only where the IPND information relates to a current or former subscriber of that carrier or CSP. In effect, this means that use of the IPND to provide a LDCS on a large scale (i.e. to all subscribers) is not possible under the current arrangements.

The Bill seeks to clarify existing legislation to explicitly permit access to IPND data for the purpose of providing LDCSs. The Bill will insert a new section 291A after section 291 of the Telecommunications Act to allow disclosure of IPND data relating to listed telephone numbers (that is, not unlisted or silent numbers, or mobile numbers unless they have been included in the public number directory at the subscriber's request).

The disclosure will also be limited to only that information necessary to provide LDCSs. This typically consists of, but is not limited to, street addresses, telephone numbers and the name of the subscriber's CSP. The intention is to allow for the effective provision of LDCSs while not allowing any information which is not required to be released from the IPND.

The amendments will also extend the existing secondary disclosure provisions in Part 13 of the Telecommunications Act to prohibit the use or disclosure of IPND data obtained for the purpose of providing LDCSs, except for the purposes permitted under the Act. The prohibition against secondary disclosure will apply to either the carrier or CSP which initially requested the data and to any other party who may receive the information. The new secondary disclosure prohibition will prohibit disclosure of information received from the IPND as well as information contained in any routing table developed in order to provide an LDCS.

FINANCIAL IMPACT STATEMENT

The Bill is not expected to have any financial impact on Commonwealth expenditure or revenue.

REGULATION IMPACT STATEMENT

The Office of Best Practice Regulation has advised that a Regulation Impact Statement is not required for the amendments to the *Telecommunications Act 1997* to allow information contained in the IPND to be disclosed and used in connection with the provision of telephony-based emergency warnings, and for the supply of Location Dependent Carriage Services (LDCSs).

NOTES ON CLAUSES

Clause 1 - Short title

Clause 1 sets out how the Act is to be cited, that is, the *Telecommunications Amendment (Integrated Public Number Database) Act 2009*.

Clause 2 – Commencement

Clause 2 provides that the Act commences on the day after it receives the Royal Assent.

Clause 3 – Schedule(s)

Clause 3 provides that each Act that is specified in a Schedule is amended or repealed as set out in that Schedule.

Schedule 1 - Amendments to the *Telecommunications Act 1997*

Part 1 – Data for Emergency Warnings Amendments

Item 1 – At the end of Division 1 of Part 13

New subsection 275B(1) inserts a definition for ‘emergency management person’ by reference to new subsection 275B(2).

New subsection 275B(2) provides that the Minister administering the *Administrative Decisions (Judicial Review) Act 1977* may, by legislative instrument specify an office or a position for the purpose of the definition of ‘emergency management person’ in new subsection 275B(1). This power has been given to the Minister administering the *Administrative Decisions (Judicial Review) Act 1977* on the basis that this Minister, being the Attorney-General, currently has portfolio responsibility for emergency management issues. The emergency management person has powers and responsibilities in connection with alerting persons to a likely or actual emergency and for the reasonable testing of such alerts.

New subsection 275B(5) provides that before making an instrument under subsection 275B(2) the Minister administering the *Administrative Decisions (Judicial Review) Act 1977* must consult with the Minister administering the *Telecommunications Act 1997*. This consultation provision has been included given the close relationship between emergency management issues and telecommunications issues arising from the ability of specified emergency management persons to access information originally sourced from the integrated public number database.

New subsection 275C inserts a definition for ‘emergency’. It means an emergency is an emergency or disaster (however described) within the meaning of an ‘emergency law’.

New subsection 275D inserts a definition for ‘emergency law’ by reference to new subsection 275D(2).

New subsection 275D(2) provides that the Minister administering the *Administrative Decisions (Judicial Review) Act 1977* may, by legislative instrument specify a law of a State or a Territory for the purposes of the definition of emergency law. For a law to be considered as an ‘emergency law’ within the meaning of Part 13 of the Telecommunications Act, there must be an existing State or Territory law in relation to such an emergency and that existing State or Territory law must be specified by the Minister administering the *Administrative Decisions (Judicial Review) Act 1977* in a legislative instrument under new subsection 275D(2). This power has been given to the Minister administering the *Administrative Decisions (Judicial Review) Act 1977* on the basis that this Minister, being the Attorney-General, currently has portfolio responsibility for emergency management issues.

New section 275E provides a definition for ‘relevant information’ by reference to the additional exception to the primary use and disclosure offence provisions set out in sections 276 and 277 of the Telecommunications Act described in new section 285A

Item 2 – after section 285

New subsection 285A(1) provides an additional exception to the primary use and disclosure offence provisions set out in sections 276 and 277 of the Telecommunications Act. New subsection 285A(1) provides that disclosure is not prohibited under sections 276 and 277 if the information or document consists of information from the integrated public number database, the disclosure is made to an emergency management person and the disclosure is made for the purpose of the information or contents of documents being used and disclosed for the purpose of for alerting persons to to an emergency or likely emergency or the reasonable testing of such alerts. This exception to the primary disclosure and use offence provisions has been included to facilitate the access by specified emergency management persons to information originally sourced from the integrated public number database.

New subsection 285A(2) contains a definition for integrated public number database for the purpose of new section 285A.

Item 3 – After Division 3A of Part 13

New subsections 295V(1) and (2) describe the circumstances in which an emergency management person may use or disclose relevant information, being for alerting persons to likely or actual emergencies.

New subsection 295V(3) describes the circumstances in which an emergency management person may use or disclose relevant information for the reasonable testing of alerts for likely or actual emergencies.

New subsection 295V(4) describes the circumstances in which an emergency management person may disclose relevant information to another person where the information will be later used or disclosed for a purpose connected with alerting persons to likely or actual emergencies. This would permit an emergency management person to disclose information from the integrated public number

database to a person such as a contractor of systems or services to provide alerts for likely or actual emergencies.

New subsections 295W(1) and (2) describe the circumstances in which a person, to whom an emergency management person has disclosed relevant information, may use or disclose that information, being for alerting persons to likely or actual emergencies and for the reasonable testing of such alerts.

New subsection 295W(3) describes the circumstances in which a person, to whom information has been disclosed by an emergency management person, may use or disclose the information for a purpose connected with alerting persons to likely or actual emergencies.

New section 295X provides that a person using or disclosing information as provided by section 295X must take reasonable steps to ensure the use and disclosure does not adversely effect the operation of a telecommunications network.

New section 295Y confirms that disclosure of relevant information to a coronial inquiry, or to another inquiry specified by the Minister administering the *Administrative Decisions (Judicial Review) Act 1977* by legislative instrument, is permitted where the disclosure is in relation to an emergency or likely emergency.

New section 295Z provides that an emergency management person commits an offence with a maximum penalty of two years imprisonment if they access relevant information and that access is not permitted by section 295V.

New subsections 295ZA(1) and 295ZA(2) provide that it is an offence for an person to whom an emergency management person has disclosed information as permitted by subsection 295V(1) and (2) and 295W(1) and that person uses or discloses information not for the purposes expressly set out in those subsections respectively.

New subsection 295ZA(3) provides that it is an offence for an person to whom an emergency management person has disclosed information as permitted by subsections 295V(4) and 295W(3) and that person uses or discloses information not for the purposes expressly set out in those subsections respectively.

New subsection 295ZB(1) provides that each time an emergency management person discloses relevant information they must give a written report to the Minister administering the *Administrative Decisions (Judicial Review) Act 1977* and the Australian Communications and Media Authority (ACMA) which complies with the requirements set out in subparagraphs (a), (b) and (c) of that subsection.

New subsection 295ZB(2) provides that the aforementioned report must be provided to the Minister administering the *Administrative Decisions (Judicial Review) Act 1977* and the ACMA as soon as practicable after the access occurs.

New section 295ZC provides that an emergency management person who discloses relevant information during a financial year must, within two months of the end of that financial year, give a written report to the ACMA and the Privacy Commissioner that meets the requirements set out in subparagraphs (a), (b) and (c) of that section.

New subsection 295ZD(1) provides that the Minister administering the *Administrative Decisions (Judicial Review) Act* may make arrangements with a Minister of a State or Territory with respect to the performance of functions or duties, or the exercise of powers, by an emergency management person.

New subsection 295ZD(2) confirms that an instrument by which an arrangement is made under subsection 295ZD is not a legislative instrument. This provision is included to assist the reader.

New section 295ZE is an immunity provision, which aims to protect the Commonwealth from any action, suit or proceeding against it in relation to loss, damage or injury as a result of the use or disclosure of relevant information. Subparagraphs (a) and (b) indicate the circumstances under which the immunity is applicable. The immunity is included for two reasons. Firstly, the Commonwealth will not be in a position to ensure that the relevant information is accurate given that that information will be originally sourced from the integrated public number database, which is not Commonwealth managed. Secondly, the Commonwealth will not be responsible for the manner in which relevant information is disclosed and utilised given that this role may be exercised by State and Territory emergency management persons.

Item 4 – Subparagraph 306(1)(b)(i)

‘285A’ is inserted after ‘285’ in subparagraph 306(1)(b)(i) of the Act. This has the effect of exempting disclosures made pursuant to section 285A from the record keeping requirements set out in section 306 of the Act.

Part 2 – Location Dependant Carriage Service Amendments

Item 5 – After section 291

New subsections 291A(1) and 291A(2) provide additional exceptions to the primary use and disclosure offence provisions set out in sections 276 and 277 of the Telecommunications Act to expressly permit disclosure and use of information or documents relating to the integrated public number database (excluding information relating to unlisted telephone numbers) for the purpose of providing location dependant services.

New subsection 291A(1) provides that disclosure by a person is not prohibited under sections 276 and 277 if the information or document relates to information from the integrated public number database (excluding information relating to an unlisted telephone number), the disclosure is made to a CSP and the disclosure is made for a purpose of, or is connected with, the supply, or proposed supply, by a person of a location dependant carriage service.

New subsection 291A(2) provides that disclosure and use by a carrier or CSP is not prohibited under sections 276 and 277 if the information or document relates to information (excluding information relating to an unlisted telephone number) contained in an integrated public number database and the disclosure or use is made

for a purpose of, or is connected with, the supply, or proposed supply, by a person of a location dependent carriage service.

Information relating to unlisted telephone numbers is specifically excluded from the permitted disclosure provisions in subsections 291A(1) and 291A(2) to protect the privacy of all persons with unlisted telephone numbers.

New subsection 291A(3) provides a definition of integrated public number database for the purpose of section 291A.

Item 6 – After section 302

New subsection 302A(1) provides that if a disclosure is made to a person in accordance with subsection 291A, that person must not disclose or use that information or document, except for the purpose of, or in connection with, the supply, or proposed supply, by a person of a location dependent carriage service.

New subsection 302A(2) provides a definition for ‘location dependant carriage service’ for the purpose of section 302A.

Item 7 – Subparagraph 306(1)(b)(i)

‘291 or 291A’ is substituted in place of ‘291’ under subparagraph 306(1)(b)(i). This has the effect of exempting disclosures made pursuant to section 291A from the record keeping requirements set out in section 306 of the Act.