Further information on the operation of the Bill

Query

The following provides detailed advice as to the safeguards protecting information that may be used/disclosed under proposed subsection 285(1B) and proposed sections 287 and 300, including:

(a) to whom information may be disclosed;
(b) what kinds of information may be disclosed;
(c) the process by which information may be requested and disclosed; and
(d) what safeguards would operate in respect of information disclosed under these provisions and why these safeguards are considered sufficient.

Response

Subsection 285(1B) – Access to Information from the Integrated Public Number Database (IPND)

(a) To whom may information be disclosed?

The Bill facilitates the disclosure of information about unlisted numbers - including the name and residential address associated with the number - from the Manager of the IPND to the Emergency Call Person (ECP).

Disclosure of unlisted information through the proposed measure will be limited in practice to dispatching services (such as police, firetrucks or ambulances) and routing calls to either Triple Zero or the Australian 106 Text Emergency Relay Service for people who have a hearing or speech impairment. In law, disclosures are strictly limited to matters raised by a call to an emergency service number.

Further information about how disclosures occur from the IPND is set out under response (c).

(b) What kinds of information may be disclosed?

The proposed amendment to section 285 of the Act is mainly focused at promoting clarity in the legislative framework around the disclosure of unlisted number information. As set out in paragraph 13 of the *Notes on Clauses* in the Explanatory Memorandum for the Bill, the intention is to remove unnecessary complexity in the interpretation of the Act.

The exception in section 285, and the proposed amendment, applies only to information contained in the IPND, only to the Manager of the IPND, and only for purposes of dealing with a matter raised by a call to an emergency service number. In practice, this includes the name and service address associated with the number calling emergency services, as contained in the IPND. Further information about the kinds of information available on the IPND is set out under response (c).

Further detail about the IPND – including the kinds of information which is kept and can be disclosed under the proposed measure – will be set out in updates to explanatory materials for the Bill, and is summarised under response (d) below.

(c) What is the process by which information may be requested and disclosed?

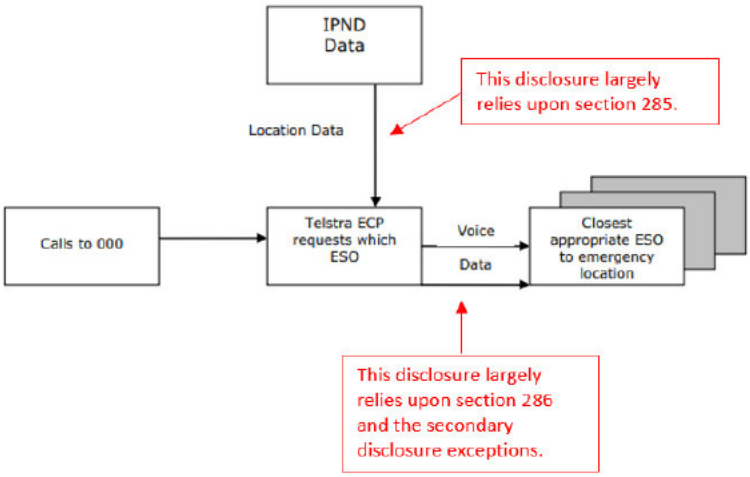
When a caller dials an emergency service number in need of emergency assistance, the call is first answered by the ECP (currently Telstra for 000/112, and the National Relay Service provider for 106). The ECP asks the caller which emergency service is required – police, fire, or ambulance – and then connects the caller to the relevant emergency service centre that services the caller's location[1].

When the call is transferred to the requested emergency service, the customer name and residential address of the caller is automatically transmitted from the IPND and displayed on the control screen of the emergency service operator handling the call. In most cases, the operator is able to confirm the appropriate dispatch location directly with the caller.

[1] Page 14 of the IPND Data G619:2017 Communications Alliance Industry Guideline outline the processes relating to emergency service calls, including how information derived from the IPND is used for the purpose of emergency call services.

However, if this location cannot be confirmed, in some cases, assistance is dispatched to the address associated with the phone number of the caller, as listed on the IPND. The IPND, which is managed by Telstra under clause 10 of its carrier license conditions,[2] contains a record of each telephone number issued by carriage service providers to their customers in Australia, including the customer's name and residential address. Access to information in the IPND – including storage, transfer, use, or disclosure of unlisted information – is strictly regulated through the Act, a number of legislative instruments, and enforceable industry standards. Further information is provided under response (d).

Figure 1: An overview of what happens on an emergency call (image courtesy of the Communications Alliance)



The proposed amendment merely seeks to clarify that disclosure about unlisted numbers from the IPND Manager to the ECP (for example, to allow the dispatch of an ambulance because the person on the call using an unlisted number is asphyxiating) is lawful.

(d) What safeguards would operate in respect of information disclosed under these provisions and why are these safeguards considered sufficient?

The amendment builds upon the existing Part 13 safeguards by introducing a requirement that it must be unreasonable or impracticable to seek the consent of the person to whom the disclosure relates. The use and disclosure of this data is restricted only to those necessary in providing an emergency service response. Through the interaction between several pieces of legislation which regulate either access to information in the IPND and/or the provision of emergency call services, information disclosure through the measure is restricted to police, fire and ambulance services.

Beyond this, the general safeguards that apply across Part 13 of the Act remain in place. For example, Division 2 of the Act sets out that use or disclosure of information received under these exceptions must be for the authorised purpose, contravention of which is an offence punishable on conviction by 2 years imprisonment, for example.

Telstra, as the IPND Manager and the ECP, has publicly available procedures in place to ensure that information disclosed between the IPND Manager and the ECP is handled appropriately.[3] Obligations on IPND access seekers are specified in an enforceable industry code[4] and in the data access agreements with Telstra.[5] These technical implementations limit the ability for disclosures to occur for purposes or to entities separate to those mentioned above.

The Government will issue an updated Explanatory Memorandum which comprehensively sets out the process by which disclosures under proposed subsection 285(1B) would occur, including the legislative instruments that regulate access to the IPND. Noting that there are several legislative and regulatory safeguards outside Part 13 of the Act for the handling, use, storage, and destruction of any information contained on the IPND, the updated Explanatory Memorandum will also draw out these specific provisions to provide assurance regarding the strictly limited scope of the exception and the proposed amendment.

[2] See: *Telecommunications (Carrier Licence Conditions - Telstra Corporation Limited) Declaration 2019*
[3] Part 8 of the *Telecommunications (Consumer Protection and Service Standards) Act 1999* and the *Telecommunications (Emergency Call Service) Determination 2019* set out obligations relating to the provision of emergency call services, including call information.
[4] See: Integrated Public Number Database C555:2020 *(industry code registered under Part 6 of the Act)*;
[5] For example, Data Users and Data Providers Technical Requirements for IPND outlines technical requirements of the IPND, including for file formatting and storage, data security, and reporting. IPND homepage link: https://www.telstra.com.au/consumer-advice/ipnd

Sections 287 and 300

(a) To whom may information be disclosed?

In practice, the provision generally only applies when a carrier or service provider is contacted by the police.

For the proposed exception in section 287 of the Act to apply, the carrier or carriage service provider must believe on reasonable grounds that the disclosure is reasonably necessary to prevent or lessen a serious threat to the life or health of a person. The Bill also introduces the safeguard that the carrier or carriage service provider must be satisfied that it would be unreasonable or impracticable to obtain the consent of the person to which the information disclosed relates to. The OAIC's Australian Privacy Principle Guidelines (C.5) on the equivalent use/disclosure principle in the *Privacy Act 1988* provides helpful interpretative guidance about the scope and appropriate meaning of these terms in relation to the circumstances where a use or disclosure is likely to be permitted.

As set out in the Explanatory Memorandum to the Bill, it is the intention of the proposed measure that regulated entities would be largely reliant on the representations made by law enforcement or emergency service organisations to determine whether a threat was 'serious'. This approach is consistent with the existing operational approach of law enforcement agencies, and recognises that police or emergency service organisations have access to information, systems and resources that telecommunications companies do not.

It is important to note that the amendments to the exception in section 287:

- do not compel the disclosure of information - even in cases where a request from police clearly satisfies the threshold for the exception to apply, disclosure remains at the discretion of the carrier;
- do not provide access to the contents or substance of a communication, or any other information which would ordinarily require a warrant; and
- do not allow for information received through the exception to be used for another purpose – the amendments to section 300 of the Act require that any secondary disclosure or use of information by police or emergency service organisations must relate back to the purpose of the original request. Failure to do so is an offence punishable on conviction by 2 years imprisonment.

Rather, the exception provides that a carrier or carriage service provider does not commit a criminal offence for disclosing information about the 'affairs or personal particulars' of a person where it has a reasonable belief that doing so is reasonably necessary for preventing or lessening a threat to the person's life or health. The secondary disclosure exception in section 300 of the Act can only be relied upon where doing so was for the purposes of preventing a serious threat, or if the disclosing entity believes on reasonable grounds that the disclosure is reasonably necessary to prevent or lessen a serious threat to life or health.

For example, if a carrier were to rely upon section 287 to disclose triangulation information to the NSW Police about a missing person, and the triangulation data showed that the approximate location of the missing person's phone was somewhere in Queensland, NSW Police would be able to rely on section 300 to disclose that triangulation data to Queensland Police if NSW Police believes on reasonable grounds that doing so was reasonably necessary to prevent a serious threat to the person's life.

In practice, secondary disclosures will be further limited through the proposed amendment as the section 300 exception will now require that it is unreasonable or impracticable to obtain the person's consent before the secondary disclosure exception can apply. This ensures that further disclosure of the information always requires consideration of whether the person's consent was able to be sought at that specific point in time.

(b) What kinds of information may be disclosed?

Section 287 of the Act reads:

> Division 2 does not prohibit a disclosure or use by a person (the ***first person***) of information or a document if:
>
> (a) the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and
>
> (b) the first person believes on reasonable grounds that the disclosure or use is reasonably necessary to prevent or lessen a serious and imminent threat to the life or health of a person.

Division 2 prohibits the primary use and disclosure of such information, and contravention is an offence punishable on conviction by 2 years imprisonment. For avoidance of doubt, the prohibition extends to the content or substance of the communication, including the content of voice calls, text messages, or voicemail, as well as any other information or document that relates to the communication, such as call logs. It also extends to any information that relates to a person's affairs or personal particulars, including numbers or addresses which are not publicly listed, or location information.

The exception in section 287 of the Act, and the proposed amendment, does not allow for the content or substance of a communication to be made available in any circumstance. The proposed measure in the Bill will not change or increase the type of information which can be requested and disclosed through the operation of the provision.

The exception only applies to information relating to the 'affairs or personal particulars of a person', a meaning which includes location information as clarified by section 275A of the Act. Carriers do not typically have access to GPS information, and triangulations do not use GPS technology. Instead, a triangulation provides an approximate area of where a handset might be located, based on the location of one or more nearby cell towers. While there can be an enormous variance in the accuracy of this information, triangulations remain a useful tool in missing persons investigations, assisting in locating high-risk missing persons in about 20% of occasions in NSW.

As set out in paragraph 177 of the *Inquest into the Disappearance of CD*, if deemed necessary and proportionate following the initial risk assessment of relevant factors in a missing persons case, consideration may also be given to the use of Live CAD – which provides the time and date of activation of a mobile phone to the network, whether those activations consist of incoming or outgoing calls, and cell tower location.

(c) What is the process by which information may be requested and disclosed?

In relation to missing persons, a formal request from law enforcement agencies to providers is required, but internal procedural requirements also apply for law enforcement to help establish that the thresholds for reasonable belief and reasonable necessity in the exception are met for section 300 of the Act.

This includes mandatory risk assessments, exhaustion of less intrusive methods, and internal authorisation requirements prior to initiating the process for a request. Broadly speaking, this also includes adherence to the Australia New Zealand Policing Advisory Agency *Missing Persons Policy (2020)* and *Guiding Principles*. In both the *Inquest into the death of Thomas Hunt*, and the *Inquest into the disappearance of CD*, a formal request to the provider was never made because NSW Police were not able to satisfy themselves that the threshold could be met by the circumstances.

The Government recognises the particular sensitivity that may attach to the personal information of individuals who have been reported missing. Such individuals may have exercised their free choice to disassociate themselves from friends and family for legitimate reasons, including removing themselves from harmful environments. Accordingly, a claim made by a member of the general public, without support or confirmation from emergency service organisations or law enforcement agencies, would not meet the threshold for the exception to apply. This is made plain in the explanatory memorandum to the Bill. However, the Government will clarify the process through which requests under the section 287 exception are invoked through amendments to the Bill's explanatory materials.

(d) What safeguards would operate in respect of information disclosed under these provisions and why are these safeguards considered sufficient?

The Bill introduces a new safeguard into sections 287 and 300 that it must be impracticable or unreasonable to obtain the consent of the person the disclosure relates to. In doing so, the proposed measures in the Bill ensure that any secondary use or disclosure of information received under these exceptions must be for the authorised purpose, contravention of which is an offence punishable on conviction by 2 years imprisonment.

In consultation with law enforcement agencies, the Department understands the management of such data is received and managed according to well-established protocols, and also subject to a range of safeguards of which only one is the Act (which, for example, prohibits disclosure except in specified circumstances, and for which the penalty is two years imprisonment). These procedures and protocols are not public, to avoid disclosure of operational police practices.

The Department will be coordinating a private briefing with law enforcement agencies for the benefit of the inquiry of the Senate Environment and Communications Committee. These protocols and practices are also subject to a range of oversight mechanisms, including at the federal level by a number of oversight bodies.

Immunity from civil liability

Query

The following assesses the appropriateness of providing carriers, carriage service providers, and intermediaries with further civil immunities so that affected persons have their right to bring an action to enforce their legal rights limited to situations where lack of good faith is shown.

Response

Section 313(5) of the Act provides that a carrier or carriage service provider is not liable to an action or other proceeding for damages if an act is done or omitted in good faith under subsections 313(1), (1A), (2), (2A), (3) or (4) of the Act. However, it does not include subsection 313(4A) and (4B). The amendment in the Bill is consistent with similar provisions relating to safeguarding national security and public revenue in the Act, and corrects an error in the National Emergency Declaration Bill 2020, introduced by the former Government.

Under the *National Emergency Declaration (Consequential Amendments) Act 2020* (NED(CA) Act), subsections 313(4A) and (4B) were inserted into the Act. These subsections introduce a duty on telecommunications providers to provide reasonably necessary help during certain emergencies.

It was intended that these entities would not be liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in fulfilment of that duty. The policy intention was set out in the Explanatory Memorandum to the *National Emergency Declaration (Consequential Amendments) Bill 2020* that immunities would extend to the duties under subsections 313(4A) and (4B). Due to an error in drafting, the measures were not included in the Bill, and unfortunately section 313(5) was not amended to give effect to the then Parliament's intention.

Right to an effective remedy

While the Government believes that the Bill does engage the right to an effective remedy under Article 2(3) of the ICCPR, to the extent that it does limit that right, the limitation is reasonable, necessary and proportionate to the objective.

Further information on the compatibility of the measure with the right to an effective remedy was provided to the Parliamentary Joint Committee on Human Rights, and the Government will update the explanatory materials to the Bill to comprehensively outline the engagement of the right in the statement of compatibility.