Australian Government
Attorney-General's Department

February 2023

Submission to the Inquiry into the Telecommunications Legislation Amendment (Information Disclosure, National Interest and Other Measures) Bill 2022

Senate Standing Committees on Environment and Communications

Introduction

The Attorney-General's Department has policy responsibility for a number of areas engaged by the Telecommunications Legislation Amendment (Information Disclosure, National Interest and Other Measures) Bill 2022 (the Bill), specifically, electronic surveillance and law enforcement, information law and privacy, and human rights. The department provides the following background and additional information on the reforms, as arising from these policy responsibilities.

Information use and disclosure

Integrated Public Number Database

The Integrated Public Number Database (IPND) is a record of most Australian phone numbers, including unlisted numbers. Telecommunications providers have an obligation under the *Telecommunications Act 1997* (Telecommunications Act) to keep the IPND up to date.

While the disclosure of information on the IPND is generally prohibited, the Telecommunications Act enables disclosure to emergency call persons. However, the current exemption does not apply to unlisted phone numbers, which means that unlisted numbers cannot currently be disclosed. This is particularly significant because, as set out in the Explanatory Memorandum for the Bill, 95 per cent of the 72 million numbers in active service are unlisted (predominantly because mobile numbers are unlisted by default).

The proposed amendments in Schedule 1, Part 1 of the Bill would allow the disclosure of information about unlisted phone numbers to emergency call persons when the information is related to the matter or matters raised by a call to an emergency service number and it is unreasonable to obtain the person's consent to the particular disclosure or use.

As set out in the Explanatory Memorandum, the amendment aligns with the position expressed by the Australian Law Reform Commission (ALRC) in its review of the *Privacy Act 1988* (Privacy Act) (ALRC Report no. 108), in particular ALRC recommendation 72-13[1]. The department also notes the ALRC's view that most people would expect that unlisted numbers would be able to be disclosed in an emergency call situation.

Crucially, the department notes that this exemption does not provide access to the content of a person's communication. Access to content information remains appropriately protected, with access and use governed by the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

Threat to person's life or health

Section 287 of the Telecommunications Act provides an exemption from the prohibition on disclosing telecommunications-related information if the discloser believes on reasonable grounds the disclosure is reasonably necessary to prevent or lessen a serious and imminent threat to the life or health of a person.

The amendments in Schedule 1, Part 1 of the Bill would remove the current requirement for the threat to be 'imminent'.

The department and the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) consulted with policing agencies on the proposed amendment through the Interception Consultative Committee (ICC) in July and November 2022. Police expressed concerns with the provision as it currently stands and are overwhelmingly positive of the proposed amendments. The concerns raised by police were shared by the Deputy State Coroner in relation to New South Wales Police in the *Inquest into the disappearance of CD* [at paragraph 119][2].

During consultation, policing agencies expressed the view that the risk of harm to an individual *increases* over time, which underscores the importance of seeking information about a missing person as soon as possible including, where possible, *before* serious threat to life becomes imminent. This view is also consistent with the findings of the Deputy State Coroner the *Inquest into the disappearance of CD* [paragraph 121] [3]. However, it is in stark contrast with the current legislative requirements; during consultations one police agency noted 'imminent' could be interpreted as 'in the short term' or 'next couple of hours'.

When considering the proposed amendments, the approach taken when interpreting the equivalent exemption in the *Privacy Act 1988* can also provide guidance; the Australian Privacy Principle (APP) Guidelines (C.9) state that 'a potentially harmful threat that is likely to occur, *but at an uncertain time*, may be a serious threat'[4] [emphasis added].

The department considers removing the word 'imminent' will make the provision clearer and easier to apply and understand. This will assist police and telecommunications providers to have a common understanding of the provision and the circumstances in which it is intended to be used, as well as the public.

---

[1] For Your Information: Australian Privacy Law and Practice (ALRC Report 108) | ALRC.
[2] Inquest into the disappearance of CD (nsw.gov.au).
[3] Inquest into the disappearance of CD (nsw.gov.au).
[4] Chapter C: Permitted general situations - Home (oaic.gov.au).

Further, the department considers the *Inquest into the disappearance of CD*[5] and the *Inquest into the disappearance of Thomas Hunt*[6] represent situations where the community would rightly expect police to access telecommunications-related information. Removing the word imminent will assist them to do so.

The amendments would also implement ALRC recommendation 72-7.[7]

As noted by the ALRC, the department considers the crux of the issue is the seriousness of the threat to the missing person, and that any assessment of the seriousness of a threat must consider the likelihood the threat will eventuate.

The department considers that sufficient safeguards are in place to preserve privacy principles and prevent misuse of information disclosed under section 287 of the Telecommunications Act.

The department recognises individuals may freely choose to disassociate themselves from friends and family for legitimate reasons, including to escape from dangerous situations such as family violence. The department notes that police should have arrangements and clear guidelines in place to ensure the whereabouts of a person are not inappropriately disclosed in such situations. The department understands police have policies and procedures in place, such as mandatory risk assessments, exhaustion of less intrusive methods, and internal authorisation requirements prior to initiating a request. As set out in the Minister for Communication's response to the Senate Scrutiny of Bills Committee, these policies and procedures generally align with the Australia New Zealand Policing Advisory Agency Missing Persons Policy (2020) and Guiding Principles. This ensures requests are only made when appropriate and that information received in response to a request is appropriately used and protected.

Crucially, section 287 does not provide police with access to the content of a person's communication. Access to content information remains strongly protected with access and use governed by the TIA Act.

Privacy Act similarities

The department provides the below analysis on the equivalent disclosure provision in the Privacy Act to provide the Committee with further information and context, as it is a longstanding and well understood area of information law.

Subsection 16A(1) of the Privacy Act contains 'permitted general situations' in relation to the collection, use or disclosure of personal information. This includes a permitted general situation where it is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure, and the APP entity reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety (section 16A, Item 1 of the Privacy Act).

The APP Guidelines provide guidance on the permitted general situations in subsection 16A(1) of the Privacy Act, including lessening or preventing a serious threat to life, health or safety (APP Guidelines C.1-C.13)[8].

---

[5] Inquest into the disappearance of CD (nsw.gov.au).
[6] Inquest into the death of Thomas HUNT (nsw.gov.au).
[7] For Your Information: Australian Privacy Law and Practice (ALRC Report 108) | ALRC.
[8] Australian Privacy Principles guidelines - Home (oaic.gov.au).

The OAIC's APP Guidelines provide interpretative guidance about the meaning and relevant considerations for when it is unreasonable or impracticable for an APP entity to obtain an individual's consent (APP Guidelines C.5-C.6); what constitutes a 'reasonable belief' that collection, use or disclosure is 'necessary' (APP Guidelines C.7-C.8); and the threshold for a 'serious' threat and a 'serious threat to public health or safety' when several people may be affected (APP Guidelines C.9-C.12). The APP Guidelines also provide that before relying on a permitted general situation and if time permits, attempts could be made by the APP entity to seek the consent from the relevant individuals for the collection, use or disclosure (APP Guidelines C.13).

Consent

Consent is defined to mean express consent or implied consent (subsection 6(1) of the Privacy Act). To establish whether it is unreasonable or impracticable to obtain an individual's consent, the APP Guidelines provide that relevant considerations for an APP entity may include:

- the nature of, and potential consequences associated with, the serious threat
- the possible adverse consequences for an individual if their consent is not obtained before the collection, use or disclosure
- the source of the threat
- the ability to contact the individual to obtain consent
- the capacity of the individual to give consent
- the number of individuals whose personal information is to be collected, used or disclosed, and
- the inconvenience, time and cost in obtaining consent (APP Guidelines C.6).

The relevant considerations above highlight the complexities that APP entities may encounter when attempting to obtain an individual's consent and demonstrate that obtaining consent should not be viewed in isolation from the surrounding circumstances of the serious threat to life, health or safety.

Reasonable belief

The department notes the 'reasonable belief' threshold in section 287 is consistent with the equivalent disclosure provision in the Privacy Act and considers it appropriate that the thresholds remain consistent.

'Reasonable belief' is not defined in the Privacy Act. The APP Guidelines provide that the terms 'reasonable' and 'reasonably' have their ordinary meanings, where what is reasonable is a question of fact in each individual case (APP Guidelines Chapter B, B1.5). The phrase 'reasonable belief' is to be applied in the same manner as 'reasonable' and 'reasonably', meaning an APP entity must have a reasonable basis for the belief, and not merely a genuine or subjective belief (APP Guidelines Chapter B, B111). The APP entity is responsible for justifying its reasonable belief (APP Guidelines Chapter B, B.111).

Necessary

'Necessary' is not defined in the Privacy Act. The APP Guidelines note that in the context of the Privacy Act, it would not be sufficient if the collection, use or disclosure of personal information is merely helpful, desirable or convenient (APP Guidelines Chapter B, B.113). This suggests that the exemptions for permitted general situations in section 16A require a higher threshold for the meaning of 'necessary' to justify the collection, use or disclosure of personal information absent individuals' consent.

Lessen or prevent a serious threat to life, health or safety

'Serious' and 'threat' are not defined in the Privacy Act. The APP Guidelines define a 'serious' threat as one that poses a significant danger to an individual or individuals, where relevant considerations include the likelihood of a threat occurring, and the consequences if the threat materialises (APP Guidelines C.9). However, neither of these considerations are determinative on their own as:

- a threat that may have dire consequences but is highly unlikely to occur would not normally constitute a serious threat, and
- a potentially harmful threat that is likely to occur, but at an uncertain time, may be a serious threat, such as a threatened outbreak of infectious disease, to allow an APP entity to take preventative action to stop a serious threat from escalating before it materialises (APP Guidelines C.9).

Where the threat has passed, the permitted general situation under Item 1 of section 16A in the Privacy Act would not apply (APP Guidelines C.9).

A threat to life, health or safety may include a:

- threat to a person's physical or mental health and safety
- potentially life threatening situation or one that might reasonably result in other serious injury or illness
- threat to an individual the APP entity is dealing with or to another person, or
- threat to inflict harm randomly to an unspecified individual (APP Guidelines C.10-C.11).

Consistent with the discussion above, the department considers the proposed amendment strikes an appropriate balance between the community's expectations around privacy, and the need to access information quickly and easily to keep people safe.

Record keeping

Telecommunications providers have an obligation under the Telecommunications Act to record information disclosed under section 287, as well as reporting obligations to the Australian Communications and Media Authority and oversight by the Information Commissioner.

The proposed amendments would require telecommunications providers to keep more detailed records to assist oversight bodies perform their monitoring and compliance activities in relation to the disclosure and use of telecommunications data by agencies outside the TIA Act.

The proposed amendments would implement recommendation 8 from the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) report on its *Review of the Mandatory Data Retention Regime*[9]. That recommendation was in response to a submission OAIC which noted that the information required to be kept by providers did not allow it to consider whether only necessary personal information is being disclosed by providers when responding to information requests from enforcement agencies.

The department supports the proposed amendment.

---

[9] Review of the mandatory data retention regime – Parliament of Australia (aph.gov.au).

Civil immunities

The proposed amendments would provide civil immunity to telecommunications providers for assistance provided to agencies in good faith in particular emergencies, including declared national emergencies under the *National Emergency Declaration Act 2020* (the NED Act). The effect of this amendment would be to mirror the existing immunities already conferred on carriers which provide assistance to agencies in relation to enforcing the criminal law and safeguarding national security.

As set out in the Explanatory Memorandum for the Bill, it was intended that the immunities be provided under the Telecommunications Act through the *National Emergency Declaration (Consequential Amendments) Act 2020* (NED Amendment Act). However, there was an oversight during the development of that legislation and the amendment was not included.

The department notes the Bill engages the right to an effective remedy under article 2(3) of the *International Covenant on Civil and Political Rights* (ICCPR). However, the department considers the immunities are rationally connected to the important objective of ensuring that individuals acting on behalf of a carrier or carriage service provider will provide reasonably necessary assistance in good faith to authorities in the case of disasters and national emergencies.

The department further considers the proposed immunity is proportionate to achieving this important objective and is not arbitrary, unfair or based on irrational considerations. Further the immunity is limited to circumstances where a telecommunications company is assisting in good faith in specified situations and is only related to actions or other proceedings for damages.

Importantly, there remain other avenues for individuals to seek remedies in situations where they believe their privacy may have been violated. This includes making a complaint to the regulator (the Australian Communications and Media Authority) which can take enforcement action, the Privacy Commissioner or seek a remedy against the relevant Commonwealth, State, or Territory body or government official initiating the request for assistance. The Department understands this information will be set out in more detail in a revised Explanatory Memorandum.

The department therefore considers the amendment is consistent with the right to an effective remedy, as laid out in Article 2(3) of the ICCPR.

Conclusion

The department thanks the Committees for considering this submission and hopes that it assists by providing further information to this inquiry. The department would welcome the opportunity to provide any further information to the Committees as required.