Australian Government

Department of Infrastructure, Transport, Regional Development, Communications and the Arts

Committee Secretary
Senate Standing Committee on Environment and Communications
Parliament House
PO Box 6100
Canberra ACT 2600

By email: ec.sen@aph.gov.au

7 February 2023

Re: Telecommunications Legislation Amendment (Information Disclosure, National Interest, and Other Measures) Bill 2022

Dear Committee Secretary

The Department of Infrastructure, Transport, Regional Development, Communications and the Arts welcomes the opportunity to provide additional information in response to matters raised in submissions from other stakeholders to the Senate Standing Committee on Environment and Communications (the Committee).

This supplementary submission will address the concerns raised about the Bill in the submissions received by the Committee. Noting that many of the concerns raised by the Law Council of Australia and the NSWCCL were either resolved prior to the introduction of the Bill or otherwise substantially addressed through the Department's submission to the Committee.

The Department expresses its thanks to interested stakeholder groups for their submissions and feedback to the Committee, and for their scrutiny of the Bill.

Yours sincerely,

[redacted]

Richard Windeyer
Deputy Secretary, Communications and Media
Department of Infrastructure, Transport, Regional Development, Communications, and the Arts

Contents

Response to Stakeholder Submissions

Impact on vulnerable people in the context of domestic or family violence

Submissions

1. In its submission to the Committee, the New South Wales Council for Civil Liberties (NSWCCL) raised concerns about the impact of the proposed measures in the Bill for the safety of vulnerable persons who choose to go missing – for example, to escape family or domestic violence.

2. The Law Council of Australia recommended that clarification should be provided in relation to how these types of sensitive circumstances will be managed in practice.

Response

3. As outlined in paragraphs 39-40 of the Department's submission, ensuring privacy of vulnerable persons was specifically considered in developing the Bill, which proposes to include a consent-based safeguard to the disclosure exceptions in sections 287 and 300 the Act, improving current privacy protections. This ensures that any such disclosure of location information by telecommunications providers to police will always require a consideration of whether a person's consent was able to be sought at that point in time.

4. The amendments do not change the long-standing operational procedures of law enforcement agencies, whose established processes protect the privacy of vulnerable persons reported as missing. As indicated in the Australian Federal Police submission, the operational benefit of these measures will be in locating missing persons identified as 'high-risk', which are often women and children. It is compulsory to assess relevant factors such as vulnerability before determining the right investigative approach.

5. The existing practice prevents the disclosure of location information without the individual's consent, even to the person who filed the missing person's report. As highlighted by https://www.missingpersons.gov.au/sites/default/files/PDF - Publications/NMPCC/Factsheets/17 - 0905 NMPCC Myths and Facts ENGLISH.pdfthe National Missing Persons Coordination Centre, it is not a crime to go missing. If a person is assessed to have voluntarily gone missing, police do not request the disclosure of location data. The proposed introduction of the consent-based safeguard to section 300 of the Act legislates that disclosure in this case would be an offence, punishable on conviction by up to 2 years imprisonment.

6. In practice, the exception in section 287 of the Act will only be relied upon by law enforcement to request disclosures of personal information - such as triangulation information if a person is reported as missing - if there is a serious threat to life or health, but where elements of criminality are not otherwise identified. For example, if the factual circumstances of a missing persons case were to satisfy the requisite thresholds of a suspected criminal offence, the powers in the *Telecommunications (Interception and Access) Act 1979* are used by police to authorise the disclosure of location information without needing to issue a voluntary request to a telecommunications provider.[1] The circumstances in both the *Inquest into the death of*

[1] See: Sections 178, 179, 180 of the *Telecommunications (Interception and Access) Act 1979*.

Thomas Hunt and the *Inquest into the disappearance of CD* suggest disclosures through section 287 of the Act are most likely to assist those in the community at-risk of self-harm through mental health factors.

7. Even so, the Department has informed the Domestic, Family and Sexual Violence Commission and the Department of Social Services about these concerns, and will consult appropriately to provide assurance that if necessary, further safeguards for vulnerable groups can be implemented through guidance material and training. As an example of how this guidance material can help to clarify the circumstances in which the provisions would apply with respect to an individual's rights to life and privacy— a draft version of section 287 guidelines is attached to this submission (**Attachment A**), which was jointly prepared by the Department and the Attorney General's Department for the Interception Consultative Committee.

8. A number of state-based legislative reforms found that lowering various information-sharing thresholds to remove the 'imminent' requirement can be life-saving in domestic violence cases. These reforms include:

   a. In 2014, Part 13A of the *Crimes (Domestic and Personal Violence) Act 2007 (NSW)* introduced privacy exceptions to allow service providers to share information '*to prevent and lessen a serious threat to a person's life, health or safety*' in cases of domestic violence. The NSW Domestic Violence Information Sharing Protocol explains that 'imminent' poses a barrier in domestic violence cases:

      > *This change was made because, in domestic violence situations, a serious threat may exist but it might be hard to determine whether the threat is imminent. For example, in cases of long-term domestic violence where there have been repeated assaults, there may be no identifiable immediate threats to a victim's safety, but serious concerns about the victim's safety remain.*[2]

   b. In 2017, the *Family Violence Protection Amendment (Information Sharing) Act 2017 (Vic)* instituted the Victorian Family Violence Information Sharing Scheme (FVISS) under Part 5A of the *Family Violence Protection Act 2008 (Vic)*. This allowed the sharing of confidential information where an entity reasonably believes it is *'necessary to lessen or prevent a serious threat to an individual's life, health, safety or welfare'* in the context of family violence. This amending Act removed the 'imminent' requirement in the *Health Records Act 2001 (Vic)* and the *Privacy and Data Protection Act 2014 (Vic)*.

      i. The formation of the FVISS was recommended by the 2015 Royal Commission into Family Violence (RCFV), following a 25-day public hearing. The RCFV heard testimony from then Privacy Commissioner of Victoria David Watts[3] and a submission from Victoria Police in favour of removing the 'imminent' qualifier which stated:
      ...in recent years, family violence homicides have occurred without prior police contact and with little warning serious violence was imminent.[4]

   c. In 2018, the Northern Territory Government amended the *Domestic and Family Violence Act 2007 (NT)* to implement an information sharing framework (Part 5A) to permit and, at times, mandate

[2] NSW Department of Justice, Domestic Violence Information Sharing Protocol, p.48.
[3] Royal Commission Into Family Violence (RCFV), Revised Statement of David Geoffrey Watts, 11 August 2015.
[4] RCFV, Victoria Police Submission, p.33.

information disclosure where it would 'lessen or prevent a serious threat to a person's life, health, safety or welfare because of domestic violence.'

9. The removal of 'imminent' in family dispute resolution cases was also supported by Recommendation 14 from A better family law system to support and protect those affected by family violence by the federal House of Representatives Standing Committee on Social Policy and Legal Affairs (2017).

Lowering the threshold to 'reasonable suspicion'

Submissions

10. A number of submissions[5] propose the Bill should introduce a further amendment to lower the threshold in sections 287 and 300 of the *Telecommunications Act 1997* (the Act) such that the disclosure exception would apply where there is a '***suspicion*** *on reasonable grounds that the disclosure or use is reasonably necessary to prevent or a lessen a serious threat to the life or health of a person*'.

11. A similar recommendation was made in the coronial findings of the *Inquest into the Disappearance of CD*.

Response

12. As outlined in paragraph 15.b of the Department's submission, amending the disclosure threshold from 'belief' to 'suspicion' would result in a lower bar than the equivalent standards in the *Privacy Act 1988*. This would be inconsistent with the *'general permitted situations'* in section 16A, where 'suspicion' is the threshold in cases such as unlawful activity or misconduct of a serious nature, while a higher threshold of 'belief' applies for prevention of serious threats to life, health or safety, or for locating a missing person.

13. However, the Department appreciates the position that if there is a clear public interest for the disclosure of an individual's personal information (i.e. to help save their life), a low threshold is justifiable— provided that appropriate safeguards and oversight apply. The Department will monitor for any recommended changes to the existing thresholds for disclosure in the context of the Review of the *Privacy Act 1988*.

14. The Department notes that in discussion with the Coroner's Office on 7 November 2022, the Department advised that it would not be progressing the second recommendation to lower the threshold at this time, given the resulting potential for privacy intrusiveness would require further consultation.

Consideration of less intrusive methods (such as guidance material)

Submissions

15. The submission by the New South Wales Council for Civil Liberties (NSWCCL) inquired about the consideration of less privacy-intrusive means of achieving the same policy objectives of the Bill.

[5] These include submissions by the Uniting Church in Australia, Synod of Victoria and Tasmania and South Australia Police.

Response

16. As outlined in the Minister's response to the Parliamentary Joint Committee on Human Rights (PJCHR)[6], the consultation process of the Bill demonstrated that less intrusive methods such as the provision of guidance and training were insufficient to remove the legislative barrier posed by the term 'imminent.'

17. Notably, In the *Inquest into the Disappearance of CD*, Chief Inspector Charlesworth of the NSW Police, who refused the request to triangulate CD's mobile phone because there was insufficient evidence the threat was imminent, confirmed he would make the same decision today with the benefit of hindsight due to an inability to establish imminence.

Amendments to the explanatory materials for the Bill

Submissions

18. A number of submissions suggest that amendments are required to the Bill's explanatory materials.

19. The following submissions sought further clarification on the operation of measures in the Bill:

    a. The Communications Alliance
    b. The Internet Association of Australia
    c. The Uniting Church in Australia, Synod of Victoria and Tasmania
    d. NSWCCL
    e. The Law Council of Australia

20. The NSWCCL also endorsed the recommendations from the PJCHR and Senate Scrutiny of Bills Committee which sought further justification on the necessity, proportionality and safeguards for the amendments to sections 285 and 313 of the Act.

Response

21. As outlined in paragraphs 7, 26, 40, 49, 52 and 55 of the Department's submission, as well as the Minister's responses to the PJCHR and Senate Scrutiny of Bills Committee, the explanatory materials for the Bill is being updated to address these concerns.

22. The Government will issue a Replacement Explanatory Memorandum and Statement of Compatibility to provide further clarity on the operation of proposed measures, including the existence of safeguards. Revisions to the Explanatory Memorandum include:

    a. clarifications of all existing and proposed safeguards to protect the rights to privacy, life, and an effective remedy in the Act.
    b. details on the operation of the clauses to respond to recommendations from the PJCHR and the Senate Standing Committee for the Scrutiny of Bills.
    c. revisions suggested by the Human Rights Unit of the Attorney-General's Department.
    d. clarifying expectations for record-keeping arrangements through proposed section 306(5) of the Act.

[6] Minister for Communications response to the Parliamentary Joint Committee on Human Rights (PJCHR) Report 6 of 2022, p. 6.

Appendix

Attachment A – Guidelines on threat to life or health under section 287 of the *Telecommunications Act 1997*

Attachment B – Factsheet on the Bill

Australian Government
Department of Infrastructure, Transport, Regional Development, Communications and the Arts

Australian Government
Attorney-General's Department

Guideline – threat to life or health under section 287 of the *Telecommunications Act 1997*

Revised date: 7 September 2022

Summary

Through the Interception Consultative Committee[1] (ICC), police forces have raised concerns about the interpretation of section 287 of the *Telecommunications Act 1997* (Cth) (the Act), particularly in the context of missing persons and risks posed by contagious diseases.

As requested by the ICC, this guideline is a joint statement from the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) and the Attorney General's Department (AGD) on best practice in applying s 287, to assist police forces[2] and service providers. DITRDCA is responsible for the Act, and this guideline has been produced with the assistance of AGD.

While drafted in consultation with ICC members, this guideline is not binding or exhaustive, nor a substitute for legal advice. This guideline is only intended for distribution to ICC member agencies and telecommunications service providers where appropriate.

Statutory context

Section 287 is located within Division 3 of Part 13 of the Act. Division 2 of Part 13 makes it an offence to disclose or use any information or document relating to the contents or substance of communications, or affairs or personal particulars of another person, in connection with various telecommunication roles. Division 3 lists exceptions to those offences. This includes section 286 which enables certain disclosures as a result of calls to emergency service numbers, section 288 which enables certain disclosures to preserve human life at sea, and section 287:

> **287 Threat to person's life or health**
>
> 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.

Sections 286, 287, and 288 all contemplate an emergency situation where disclosure of protected information is necessary to keep a person safe. For each of these the disclosing person may be a carrier, carriage service provider, number-database operator, emergency call person, or their associates.

There are also exceptions to the Division 2 disclosure offences in Chapter 4 of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act). These exceptions include voluntary disclosure of information (s 177) and enforcement agencies authorising the disclosure of information in relation to missing persons (s 178A), enforcement of the criminal law (s 178), enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue (s 179), and prospective data for investigations of serious offences (s 180).

---

[1] The Interception Consultative Committee is a longstanding government consultative committee chaired by the Attorney-General's Department. Members include interception agencies, criminal law enforcement and enforcement agencies as defined under the *Telecommunications (Interception and Access) Act 1979*.
[2] Police forces includes reference to State and Territory Police Forces as defined under the *Telecommunications (Interception and Access) Act 1979* as well as relevant Government agencies such as the Department of Infrastructure, Transport, Regional Development, Communications and the Arts.

Key features of s 287

Given the similarities it shares with other provisions, particular parts of section 287, are relevant to any carrier, carriage service provider, or other entity seeking to rely on it:

- "(b) the first person believes on reasonable grounds that the disclosure or use is reasonably necessary…"
    - The *first person* is the person with access to information as described in Division 2, not the requesting police force member. This *first person* risks committing an offence if the disclosure is made in error.
    - The belief that disclosure or use of the information is *reasonably necessary* must be supported by *reasonable grounds*.
- "…to prevent or lessen a serious and imminent threat to the life or health of a person."
    - *…serious and imminent threat* is very specific, limiting the use of this exception and requiring careful judgment made by the first person. This key phrase is examined in relation to specific scenarios below.
    - *…life or health of a person* is very nonspecific, allowing for broad interpretation. Life or health could be threatened by a broad range of active and passive factors, depending on the situation. The person could be a specific individual known to police, or a person who is not identified at the time of disclosure.

The *first person*, who has been asked to disclose information, **is not compelled to do so** under section 287, and can abstain from disclosing the information sought subject to other measures (e.g. a notice to produce in conjunction with section 280 of the Act).

Serious and imminent threat

It is important to note that being missing does not automatically mean there is a 'serious and imminent threat to the life or health of a person'.

(1) *The threat must be serious*

Severity – how significant are the consequences of the threat? Would the threat result in significant harm to the health or life of a person? While this is not an exhaustive list, it is recommended to consider factors such as:

- known mental, cognitive, and physical health condition;
- age;
- likelihood of self-harm or suicide, including stated intent and inference from behaviour or family members advice;
- substance dependence, including drugs/alcohol and essential medication;
- experience of family and domestic violence or other serious family conflict and abuse;
- education, employment, and/or financial issues; and
- exposure to inclement weather conditions.

Likelihood – judged on a case-by-case basis and taking severity factors into account, the likelihood of a threat supports seriousness. For example, the risks facing a missing toddler are both more severe and more likely, given their inherent vulnerability, increasing the seriousness of the risk compared to an adult.

(2) *The threat must be imminent*.

Timing – how soon is the threat likely to occur? Is this an ongoing threat with unknowable timing but that could eventuate at any moment? Does the threat become more likely as time passes? For example, the threat of a heart attack may increase over time the longer a person is without their medication.

(3) *The threat must be directly linked to the health or life of a person*

Nature of the harm – what type of harm would result to the individual(s)? The type of harm must be to the health or life of a person. Other types of harm such as financial loss or reputational damage are absent from s 287. If the harm involves the commission of an offence that does not involve a threat to life or health, the TIA Act provisions should be used instead. Further, as noted, being missing in and of itself does not indicate harm.

(4) *Reasonable necessity of the information*

Reasonably necessary – would disclosure contribute positively to lessening or preventing the threat? Are there other less privacy intrusive means of reducing or eliminating the threat?

These are indicators, rather than exhaustive or exclusive criteria, for judgment and consideration in determining the availability of section 287.

Information for police forces

Policing operations are sometimes complex, sometimes with little or no distinction between public safety activities and law enforcement functions.

This guidance seeks to help police forces balance the complex interactions around privacy, public expectations and their community protection functions.

As discussed in more detail below, police are often best placed to provide the information needed for a discloser to assess whether disclosure is reasonably necessary to prevent a threat to life or health. The below provides considerations that police can use to provide information to the discloser.

General guidance

Section 287 should only be considered where time is of the essence and a person's wellbeing is at serious risk.

Section 287 has deliberately limited scope. As noted above, a key limiting phrase in s 287 is "serious and imminent threat to the life or health of a person."

For situations where there is a lower level of urgency or seriousness, there are other provisions which could be used instead. These include;

1) Investigations and law enforcement – use TIA Act provisions

Powers from Chapter 4 of the TIA Act should be used when police need telecommunications data for investigation or enforcement activities, for example:

- enforcing the criminal law (section 178 of the TIA Act),
- imposing a pecuniary penalty or the protection of the public revenue (section 179 of the TIA Act), and
- investigating a serious offence (section 180 of the TIA Act).

The TIA Act powers are best suited to the operations of law enforcement agencies working in a law enforcement capacity, with oversight regimes tailored to the realities of law enforcement operations. Section 287 of the Act does not authorise access to information for investigation or enforcement purposes relating to crime, revenue, or national security matters.

Where an investigation uncovers a credible, serious, and imminent threat to the life or health of a person, section 287 enables police to lawfully obtain personal information to help limit or avoid that threat. There is no reason information disclosed through s 287 could not be used for law enforcement or investigation, subject to the normal rules of admissibility. Police forces should seek legal advice on this on a case by case basis.

2) Missing persons – use TIA Act provisions first

Assistance from police is often vital in locating missing persons, and may not involve law enforcement or criminal investigation activity.

It is considered best practice to use section 178A of the TIA Act in the first instance, to access historic data that may help locate a missing person. Section 178A of the TIA Act allows an authorised officer of the Australian Federal Police, or a police force of a state, to authorise the disclosure of historic data if they are satisfied the disclosure is reasonably necessary to find a missing person.

This is the preferred avenue as the TIA Act does not require consideration of the seriousness of the threat and has in place a system of oversight and accountability to ensure this power is used appropriately. Further, there is no obligation on the discloser to form their own belief about the necessity of the release of the information.

3) Use of section 287 for missing persons

However, sometimes intelligence about a missing person supports the existence of a credible, serious, and imminent threat to the life or health of a person.

In those cases, s 287 enables the quick and lawful disclosure of information to help limit that threat. Section 287 does not require a specific procedure, and allows disclosure of *prospective* data, which s 178 of the TIA Act does not permit - noting that historic data includes information from immediately prior to the authorisation. Section 287 also does not require that the person whose wellbeing is under threat, and the person whose information is being sought, be the same person.

Section 287 of the Act should therefore be reserved for situations where avenues for assistance in accessing telecommunications data under the TIA Act are not practicable for the particular circumstances of the case, and a serious and imminent threat to life or health of a missing person exists.

4) Use of section 287 to disrupt spread of communicable diseases

Distinguishing enforcement of the criminal law and protection of individual and community safety is particularly complex in cases of public health emergencies and communicable diseases. The transmission of disease in certain circumstances in some jurisdictions is criminalised, and in such cases it would be more appropriate to use TIA Act provisions. When considering using section 287 for communicable disease related threats, police forces should consider the following questions to establish a threshold of 'serious and imminent threat' in addition to the above listed considerations:

- Is the communicable disease officially recognised as a threat, i.e. in statements made by government or health officials, or in a declaration of national emergency?
- Is the disease significantly transmissible? Can it lead to significant injury or death?
- Has the target tested positive, or is suspected of having tested positive, for the communicable disease?
- Has the target breached, or shown an intention to breach a health order or deliberately expose other people to the risk of catching the disease?
- Has the target infected other persons with the disease?
- Does the target have age, health, or other relevant vulnerabilities?
- Is the target likely to infect vulnerable populations, for example aged care residents?
- Is the objective of apprehending the person to stop the spread of the disease or to prosecute a criminal offence?

Examples

The following examples are not real examples and are not based on actual events.

Example 1: Will the backpacker is missing. Chloe has contacted the police in an attempt to locate him. Will is in good health, regularly enjoys going 'off the grid' for long periods of time, and travels frequently without notifying people when he leaves or when he returns. In this instance, Will has been gone for an abnormal period of time, and Chloe is worried something bad might have happened to him. Could section 287 be used to disclose prospective telecommunications data in this instance?

(1) Should TIA Act provisions be used?

In this scenario, police do not believe there is any unlawful activity behind Will's actions, and so would be acting only in the capacity of seeking to locate Will and mitigate any perceived threat to his life or health. However, section 178A could be relied upon to locate Will on the basis that he has been gone for an abnormal period of time and may be missing.

(2) Should section 287 of the Act be used?

Will is known to travel for long periods of time, and tends not to notify anyone when he leaves or returns. Whilst he has been gone for a longer time than usual, Will is able-bodied, and there is no information which indicates any vulnerabilities or any specific threats.

There is no information currently available to suggest there is a serious and imminent threat to life or harm of Will. On this basis, section 287 could not be relied upon.

Example 2: Rob the suspect is missing. NSW Police have been investigating Rob as a suspect in an ongoing drug trafficking case, and have now been notified that he is missing. Trafficking in prescribed substances is a 'serious offence' for the purposes of section 5D of the TIA Act. NSW Police suspect Rob has gone into hiding to avoid prosecution, and that he may be hiding with a group of other suspects.

(1) Should TIA Act provisions be used?

In this scenario, the information available to police is that Rob is most likely avoiding law enforcement due to him being a suspect in an ongoing investigation into a serious offence. On this basis, sections 178 and 180 of the TIA Act would apply.

(2) Should section 287 of the Act be used?

There is no information that suggests Rob is with the group of other suspects unwillingly, that Rob is a threat to the group of other suspects, or that there is a serious and imminent threat to the life or health of a person. On this basis, section 287 could not be relied upon.

Example 3: Iris the guest is missing. Victoria Police has been notified that Iris was last seen 36 hours ago, where she was seen walking out of a party hosted by one of her friends at a remote location. She has not answered any calls. Iris is known for absconding, and has a history of schizophrenia and diabetes. Further, it is mid-winter and Iris is not dressed for the conditions. Her friend Maude revealed to Victoria Police that she believed Iris to have smoked and distributed marijuana at the party.

(1) Should TIA Act provisions be used?

Police can clearly use section 178A as Iris has been notified as missing. Iris was suspected of distributing marijuana at the party, so police may be able to use section 178 of the TIA Act to access historic telecommunications data, as distribution is a serious offence for the purposes of section 5D of the TIA Act.

(2) Should section 287 of the Act be used?

For these examples, we will work through the factors set out above. Although such a formalised process is not required by the Act, it should be noted that *where practicable*, such an assessment would assist in providing the discloser with the reasonable grounds required to form a belief that disclosing the information is reasonably necessary.

Is the threat serious?

Iris has a history of serious mental illness and had smoked marijuana. The risk of psychosis for people with schizophrenia when smoking marijuana is heightened, placing Iris at greater risk of harming herself. Her history of diabetes may indicate insulin dependence, which can be fatal if she is unprepared or unable to treat herself. Further, the location, conditions, and her dress increase her vulnerability to harm from exposure.

These factors would support a judgment that the threat to Iris is serious.

Is the threat imminent?

It is unusual for Iris not to return missed calls from her friends, and if she is lost in the remote location her phone battery may be close to running out so there may not be time for a formalised

process. The location, weather, Iris's known mental illness, and diabetes are all factors that increase the threat to Iris with the passage of time.

Is the threat directly linked to the life or health of a person?

Yes, the threat would have a direct impact on Iris's life or health.

Is disclosure reasonably necessary?

With limited other methods of locating Iris, a disclosure may be the only way to locate her before her health is seriously impacted. Her phone has been responding, so access to prospective data may assist in locating Iris' current and future position.

On balance it would be appropriate to use section 287 to attempt to protect the life or health of a person. Where possible section 178A of the TIA Act should also be pursued in parallel, to provide more detailed and specific information that may assist in locating Iris.

Example 4: Sylvia the runaway is missing. When reporting her as missing, Sylvia's family also reported her history of depression and anxiety. Sylvia's family described her as appearing 'defeated and reclusive' in the days before her going missing. There were no direct threats of self-harm, but Sylvia had made references to running away and 'not coming back'. Sylvia has not been seen or heard from for several days.

(1) Should TIA Act provisions be used?

In this scenario, there is no indication of unlawful activity behind Sylvia's actions so the police would be acting only in the capacity of seeking to locate Sylvia and mitigate any perceived threat to her life or health.

Police could use section 178A of the TIA Act to locate Sylvia on the basis that she has been notified to the police as a missing person.

(2) Should section 287 of the Act be used?

Police could consider using section 287 of the Act when factoring in Sylvia's family's description of her changed disposition that may indicate an inference of self-harm.

Is the threat serious?

Sylvia has a history of serious mental illness. In the days leading up to her disappearance, her family had noted she appeared 'defeated and reclusive'. Both withdrawing from family members and experiencing a sense of impending doom are risk factors indicative of depression and suicidal tendencies. She had also referenced that upon running away, she would not be coming back. Whilst there were not any direct threats of self-harm, inferences from Sylvia's behaviour could indicate intent to harm herself.

These factors would support a judgment that the threat to Sylvia is serious.

Is the threat imminent?

A threat of self-harm or suicide is not necessarily imminent without some indicative timing. There were no obvious signs pointing to self-harm identified by family members. However the phrase 'not coming back' would indicate finality attached to her decision to run away.

While Sylvia remains missing it may be reasonable to consider this a serious threat, increasing in likelihood with the passage of time. These factors create an urgency to locate Sylvia supporting a judgment that the threat is imminent.

Is the threat directly linked to the life or health of a person?

Yes, the threat would have a direct impact on Sylvia's life or health.

Is disclosure reasonably necessary?

There may be other methods to locate Sylvia, for example CCTV security footage in the local area. Accessing Sylvia's telecommunications data would also assist police to locate her, with the advantage of being faster than other methods with more current data.

On balance, this would be an appropriate instance in which section 287 could be used by police forces to attempt to protect the life or health of a person.

Summary

Section 287 provides for the release of both historic and prospective data in situations where the requirements of the TIA Act cannot be met or cannot be met expeditiously. This provides a crucial tool for police to quickly respond to serious and imminent threats to health and safety. However, to ensure the power is used appropriately the above guidance will assist in a consistent and appropriate approach by agencies.

Information for service providers

Although it is the police that will have the relevant information, section 287 requires the discloser to establish a belief on 'reasonable grounds' and satisfy themselves that the disclosure or use is 'reasonably necessary'. Both 'reasonable grounds' and 'reasonably necessary' involve a balancing of the facts of the particular situation, which can include considering the intrusiveness upon individual privacy of disclosing somebody's affairs or personal particulars.

The legislation specifies that information used to inform a discloser's belief in the need for disclosure is "reasonable".

Noting the discussion above, a police force is often best placed to provide the information needed for a discloser to assess whether disclosure is reasonably necessary to prevent a threat to life or health. Information provided by a police force would therefore significantly assist in giving rise to sufficient 'reasonable grounds' for a discloser to form a belief.

When requesting disclosure of information from service providers, police should therefore supply enough information to give the service provider reasonable grounds to believe the disclosure or use is reasonably necessary to prevent or lessen a serious and imminent threat to the life or health of a person.

When providing information to support a discloser, a police force should clearly state that it needs the information to prevent or lessen a serious and imminent threat to the life or health of a person. Further consultation with industry may help clarify common factors which might constitute reasonable grounds to support a belief enabling disclosure under section 287.

This could include the factors discussed above. Disclosers could also consider publicly available information such as news broadcasts, the Bureau of Meteorology, or state emergency services.

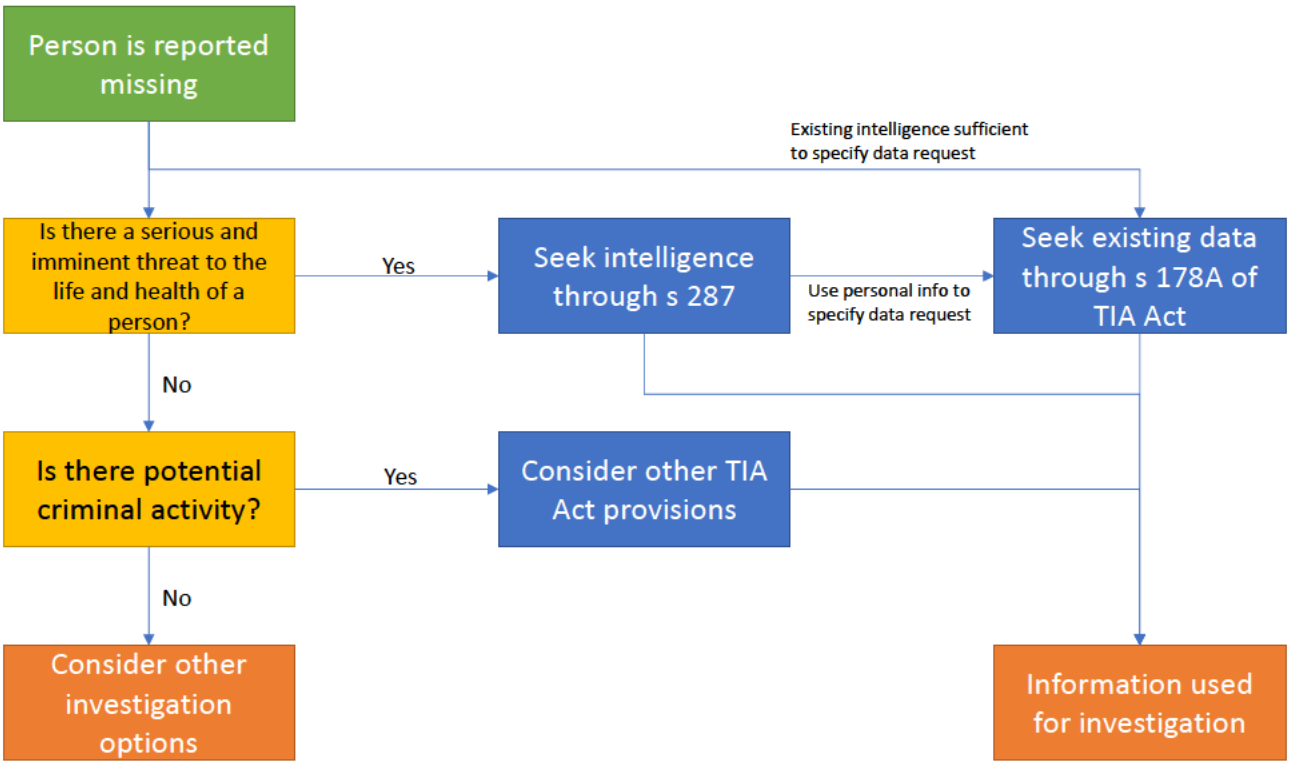
There is no general guide within the legislation, nor a prescribed form, which sets out who is able to make a request under section 287 or how such a request should be made. There is no explicit power within section 287 for police forces to compel disclosure of the information from a service provider.

Assistance from the Department and AGD

Assistance relating to specific circumstances can be obtained from the Telecommunications Security team in DITRDCA at telecommunications.security@communications.gov.au. Questions relating to the TIA Act should be directed to the Office of the Communications Access Coordinator within AGD on 1800 271 030 or cac@ag.gov.au.

Appendix A

Missing Persons



Australian Government
Department of Infrastructure, Transport, Regional Development, Communications and the Arts

***The Telecommunications Legislation Amendment (Information Disclosure, National Interest and Other Measures) Bill 2022 (The Bill)* – Fact sheet**

Helping Police Find Missing Persons

January 2023

On 16 September 2022, NSW Deputy State Coroner, Magistrate Erin Kennedy, released her findings on the Inquest into the disappearance of CD:

"The need for potential amendment of s 287 [of the Telecommunications Act 1997] and the 'serious and imminent' threshold test requires urgent consideration."[1]

In response to the Deputy State Coroner's recommendation to reform the Telecommunications Act 1997, the Government has introduced a Bill aimed at saving lives, into the Australian Parliament.

Telecommunications companies are prohibited from disclosing information about their customers. The penalty for disclosure is 2 years imprisonment.

There are some limited exceptions. One exception, known as section 287, is where sharing information about a customer is needed to prevent or lessen a serious and imminent threat to a person's life or health.

This provision is used by police and emergency service organisations to get help from telecommunications companies to find missing people using ***'triangulation'***.

Triangulation allows telecommunications carriers to estimate the location of mobile phone based on the cell towers that the phone is connected to.

Triangulation is not perfect – it can only estimate where a phone is – but it is hard to overestimate how important it is in helping police to save lives.

In missing people cases, time is of the essence. Delays in getting triangulation data can cost lives. In two recent cases, NSW State coroners have highlighted how difficult it is for telecommunications companies and police to reach a conclusion that a threat to a missing person is ***'imminent'***.

[1] Inquest into the disappearance of CD, paragraph 197

In fact, NSW Deputy State Coroner, Magistrate Erin Kennedy in the inquiry of into the disappearance of CD has said that reform to section 287 is urgent.

The Government has introduced a new bill into the Parliament to solve this problem, to help police save lives.

The bill removes the requirement that telecommunications companies need to reach the conclusion that a threat is imminent. They still need to believe the threat is serious – as the Australian Law Reform Commission has noted, consideration of whether a threat is **'serious'** will include consideration of its relative likelihood.

The Government believes that helping police save lives is of utmost importance, but also wants to improve privacy protections. That is why the bill includes new privacy protection safeguards.

For example, the bill introduces a requirement that it is **'unreasonable' or 'impracticable'** to get the consent of the person involved.

The Act also includes strict **'secondary disclosure'** prohibitions that have been strengthened in the bill – meaning that police are only allowed to use information from telecommunications companies for the purposes that it has been provided for.

Taken altogether, the bill strikes the right balance, will contribute to saving lives, and will help police to do their critical jobs in finding missing people.

"Legislative amendment is of course a matter solely within the province of Parliament. However, it is consistent with my death prevention role to highlight the urgent need for review given the current construction and operation of s 287 in the context of missing person investigations, as was highlighted by this Inquest and that of the Thomas Hunt Inquest."[2]

The case of CD

On 17 June 2019, CD, a NSW man went missing. On 21 June 2019, a NSW Police Detective contacted the Duty Operations Inspector, requesting triangulation of CD's phone. This request was declined on the basis there was no **'serious or imminent threat to the life or health'** of CD within the meaning of the Act.[3]

The Chief Inspector who denied the triangulation has expressed his frustration in the position he was in, as he felt legally obliged to decline the triangulation in this case, and articulated the need for legislative change.[4]

The Detective Chief Inspector (DCI) managing the Missing Persons Registry at NSW Police reviewed the investigation into CD's disappearance and formed the following opinion: **"... I also believe a triangulation should have been requested to discover the location of CD's phone"**.

The DCI believes the triangulation tool should be used for all **'high risk'** missing persons investigations.[5]

The case of Thomas Hunt

On 22 March 2017, Thomas Hunt went missing. As part of the effort to find Thomas, two NSW police officers raised the possibility of organising the triangulation of Thomas' phone. [6]

NSW State Coroner, Magistrate Teresa O'Sullivan commented that **"it is therefore of some concern that the bar is set high for applications under s. 287 [the relevant provision of the Act] by the State Coordination Unit"**.[7]

"...the decision whether to triangulate can be a matter of life and death".[8]

2 Inquest into the disappearance of CD, paragraph 136
3 Inquest into the disappearance of CD, paragraph 48
4 Inquest into the disappearance of CD, paragraph 123
5 Inquest into the disappearance of CD, paragraph 95
6 Inquest into the disappearance of Thomas Hunt, paragraph 62
7 Inquest into the disappearance of Thomas Hunt, paragraph 67
8 Inquest into the disappearance of CD, paragraph 127

Why is it important to help police find missing people?

- In Australia a missing person is anyone who is reported missing to police, whose whereabouts are unknown, and where there are fears for their safety or welfare.
- Unfortunately, missing people in Australia is a serious problem.
- An estimated 38,000 people are reported missing to police each year; that is one person every 15 minutes.
- A long-term missing person is someone who has been missing for more than three months. There are over 2,500 people listed as a long-term missing person.
- The increased occurrence of natural disasters over the last few years during the summer period has the potential to heighten missing persons statistics.
- If you have concerns for someone's safety and welfare, and their whereabouts is unknown, you can file a missing person's report at your local police station.

Common questions/assumptions about the Bill

Q: Does the legislation make it easier for abusers to track down victims of domestic violence?

A: No. The changes will only allow for information to be disclosed by a telecommunications company (telco) where there is a serious threat to life or a person's health and where it is impracticable or unreasonable to obtain the consent of the person in question.

A telco would be relying on the advice of law enforcement and/or emergency services organisations, in accordance with existing practices.

A claim made by a member of the general public, without support or confirmation from law enforcement agencies, would not meet the threshold for disclosure.

Q: Does the legislation reduce privacy protections?

A: No. The changes improve privacy protections. Whilst the ***'imminent'*** qualifier has been deeply problematic and may very well have contributed to loss of life, the changes to the legislation insert a requirement that disclosure from the telco can only occur where is it is impracticable or unreasonable to obtain the consent of the person in question.

Q: Will police get access to my GPS data when they triangulate my phone data?

A: No. Triangulations by carriers do not use GPS technology. A triangulation uses one or more cell towers to provide an approximate area where the handset may be located. Triangulations assist in locating missing persons in about 20% of high-risk missing persons cases in NSW.

Q: Why does there need to be reasonable belief? Why can't it be reasonable suspicion?

A: The use of ***'reasonable belief'*** is consistent with equivalent provisions set out in the *Privacy Act*.

The lower-threshold of ***'reasonable suspicion'*** would create inconsistencies with the *Privacy Act* if it was applied to the Telecommunications Act.

The Government's approach is consistent with the **Australian Privacy Principle Guidelines**, where the '*reasonable suspicion*' test is used for things like misconduct or unlawful activity, while the higher-threshold of '*reasonable belief*' is to be used for locating a person reported missing.

INFRA5615