e:
t:

NSWCCL SUBMISSION

SENATE STANDING COMMITTEES - ENVIRONMENT AND COMMUNICATIONS

TELECOMMUNICATIONS LEGISLATION AMENDMENT (INFORMATION DISCLOSURE, NATIONAL INTEREST AND OTHER MEASURES) BILL 2022 INQUIRY

16 January 2023

Acknowledgment

In the spirit of reconciliation, the NSW Council for Civil Liberties acknowledges the Traditional Custodians of Country throughout Australia and their connections to land, sea and community. We pay our respect to their Elders past and present and extend that respect to all First Nations peoples across Australia. We recognise that sovereignty was never ceded.

About NSW Council for Civil Liberties

NSWCCL is one of Australia's leading human rights and civil liberties organisations, founded in 1963. We are a non-political, non-religious and non-sectarian organisation that champions the rights of all to express their views and beliefs without suppression. We also listen to individual complaints and, through volunteer efforts, attempt to help members of the public with civil liberties problems. We prepare submissions to government, conduct court cases defending infringements of civil liberties, engage regularly in public debates, produce publications, and conduct many other activities.

CCL is a Non-Government Organisation in Special Consultative Status with the Economic and Social Council of the United Nations, by resolution 2006/221 (21 July 2006).

Contact NSW Council for Civil Liberties

http://www.nswccl.org.au
office@nswccl.org.au
Correspondence to: PO Box A1386, Sydney South, NSW 1235

The New South Wales Council for Civil Liberties (NSWCCL) welcomes the opportunity to make a submission to the Senate Standing Committees, Environment and Communications Legislation Committee (Committee) inquiring into the Telecommunications Legislation Amendment (Information Disclosure, National Interest and Other Measures) Bill 2022 (Bill).

1. Introduction

1.1 As set out in the Explanatory Note to the Bill (Explanatory Note), Part 13 of the *Telecommunications Act 1977* (Act) "provides for protection of the confidentiality of the contents of communications carried by carriers and carriage service providers; of the carriage service supplied by them, and of the affairs and personal particulars of other persons (notably, customers and end-users of carriage services). Whilst this includes personal information about individuals, … it also includes information about telecommunications, including …the location of a mobile handset."[1]

1.2 It is an offence for eligible persons to disclose or use information protected by Part 13, otherwise than for the purpose of delivering carriage services or related telecommunications industry functions. There are limited exceptions which permit the provision of this information to third parties. The Act currently permits disclosure of information related to communications(including the location of a person's phone):

- where it is reasonably necessary to prevent or lessen serious and imminent threats to a person's life or health (s287-primary disclosure, and s300- secondary disclosure) and
- in relation to the disclosure of information contained in an Integrated Public Number Database (IPND), for various purposes, relevantly including the making of a call to an emergency service number (s285).

1.3 The Bill amends the Act to, amongst other things:

a. require carriers and carriage service providers to use and disclose information for purposes connected to the prevention of a serious threat to the life or health of a person (removing the "imminent" qualifier;
b. authorise the use and disclosure of unlisted numbers and associated addresses for the purposes of dealing with matters raised by a call to an emergency service number;
c. confer civil immunities on telecommunications companies for the provision of reasonably necessary assistance to the Commonwealth, states or territories to respond during emergencies if a national emergency declaration is in force;
d. and amend record-keeping requirements to require more detailed records of information to be recorded for authorised disclosures.

1.4 NSWCCL objects to the proposed amendments, because they are gratuitous and/or do not provide adequate privacy safeguards to individuals whose records are held by carriage service providers. While NSWCCL understands the purported objectives of the Bill, there may be serious consequences from increasing access to sensitive digital information, particularly without significantly increasing privacy safeguards. Those that may be affected by reduced privacy protections include vulnerable persons such as domestic violence victims or First Nations people who may have good reason, for example, for not wanting to be found.

1.5 NSWCCL considers that no amendments should be made to the Act without a strong regime of privacy protection in place to ensure that police and other agencies properly protect personal information.

[1] Telecommunications Legislation Amendment (Information Disclosure, National Interest and Other Measures) Bill 2022 Bills Digest No. 41, 2022–23, pp 5 and 6 https://parlinfo.aph.gov.au/parlInfo/download/legislation/billsdgs/8891342/upload_binary/8891342.pdf;fileType=application%2Fpdf#search=%22legislation/billsdgs/8891342%22; (Section 275A of the Act makes clear that information about location of a mobile phone is to be taken to be information about the affairs of a customer for these purposes).

1.6 Care should be taken to ensure that limits to privacy are proportionate and adopt strict data retention policy, dealing with who has access to data and how it is collected, used, stored and destroyed. Apart from these considerations, less restrictive alternatives should be explored that could achieve the objective. In this regard, NSWCCL commends to the Committee the reports of the Parliamentary Joint Committee on Human Rights (PJCHR) and the Senate Standing Committee for the Scrutiny of Bills (Scrutiny of Bills Committee) and endorses the recommendations made in those reports.[2]

1.7 NSWCCL does not agree that the appropriate balance between information privacy and the free flow of information has been achieved in the Bill.

2. Requirement for carriers and carriage service providers to use and disclose information for purposes connected to the prevention of a serious threat to the life or health of a person

2.1 *Imminent* -The Bill seeks to remove the qualification in s287 that a threat to a person's life or health needs to be imminent. A further provision requires that it must also be unreasonable or impracticable to obtain the persons consent to the disclosure. These provisions mirror the recommendation of the Australian Law Reform Commission (ALRC) in its 2008 report.[3]

The Explanatory Note inaccurately states that "These measures will….**Permit** the use and disclosure of information for purposes connected to prevention of a serious threat to the life or health of a person".[4] [emphasis added] The Act already permits the use and disclosure of information for those purposes. The amendment purports to change the threshold that needs to be met to disclose information.

2.2 A serious and **imminent** threat is the threshold that, if established, permits the collection, use and disclosure of an individual's personal information in order to lessen or prevent a threat. In this case that information is also sensitive as it is location data that has the potential to identify and track an individual.

2.3 It is contended, in the Explanatory Notes, that requiring a threat to be both serious and imminent can be uncertain and difficult to establish. Further, that removing the word imminent, will enable public sector organisations (police) " to broaden their ability to assist and apply preventative measures where there is a reasonable belief that a serious threat is present." NSWCCL does not agree that the amendment is necessary; that it will, in isolation, achieve the required objective; nor that it should be enacted without embracing strict and detailed privacy safeguards. The Human Rights statement in the Explanatory Notes overstates that "[t]wo recent coronial inquests both concluded that the 'imminent' qualifier was a barrier in saving lives."[5]

---

[2] Parliamentary Joint Committee on Human Rights, Telecommunications Legislation Amendment (Information Disclosure, National Interest and Other Measures) Bill 2022, Report 6 of 2022, https://www.aph.gov.au/-/media/Committees/Senate/committee/humanrights_ctte/reports/2022/Report_6/PJCHR_Report_6_of_2022.pdf?la=en&hash=D7DD8DB38EF45F800F18D15E3A0A5DD76FEE849B; Senate Standing Committee for the Scrutiny of Bills, Telecommunications Legislation Amendment (Information Disclosure, National Interest and Other Measures) Bill 2022, Scrutiny Digest 8 of 2022, https://www.aph.gov.au/-/media/Committees/Senate/committee/scrutiny_digest/2022/PDF/d08_22.pdf?la=en&hash=9BD090D7839B24090BACAA9596DAA836EBFD31FD

[3] ALRC For Your Information: Australian Privacy Law and Practice (ALRC Report 108)- Threat to person's life or health https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/72-exceptions-to-the-use-and-disclosure-offences/threat-to-persons-life-or-health/

[4] Explanatory memorandum Telecommunications Legislation Amendment (Information Disclosure, National Interest and Other Measures) Bill 2022 para 3a p1 https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr6943_ems_49e1acac-3ac3-4858-a3c2-31ba4a0a688c%22;rec=0

[5] ibid

2.4 In fact, Deputy Coroner Magistrate Teresa O'Sullivan, in the 2020 inquest into the death of Thomas James Hunt,[6] found that, "The Missing Persons Standard Operation Procedures ("MP SOPS") that applied at the time of Thomas's disappearance gave police no guidance on the application of s. 287. It became apparent during the evidence that police were, and still are, interpreting and applying the test under s. 287 differently, meaning where the threshold may be met for one officer for the triangulation of the phone of a missing person, it may not be met for another."[7] She found that the threshold test contained in s. 287 is not a high bar that can only be met where proof of a missing person's intentions are available. The community would expect that where there is a threat to a missing person's health or safety all available action ought to be taken and proof is not required.

The Deputy Coroner claimed that there was scope for further guidance and training of police in respect of the interpretation of s. 287 of the Telecommunications Act.[8] It should be noted that by the time of the Report there had been major changes to MP SOPS to deal with operational failings in the police investigation. [9] However, as the PJCHR state, the Explanatory Note does not address why further guidance and training of police does not achieve the same objective as amending s287.[10]

The Coroner in the Inquest into the disappearance of CD did recommend that the Minister be contacted "with a view to considering urgent reform of that provision [s287], including as to whether to… remove the qualifier of an "imminent" threat.[11]

2.5 The PJCHR found the Statement of Compatibility in the Explanatory Note lacking, in failing to identify any safeguards relating to access of and use of the data. For example, the parameters of 'dealing with matters raised' in a call to emergency are unclear.[12] "In particular, it is unclear:

- what is the process by which section 287 is invoked (for example, is it only ever police contacting carriage service providers in practice?), and is a warrant or other formal application a part of the process;
- what specific kinds of information may be requested (for example, would it include the content of a person's text messages or voicemail; their call log; or only Global Positioning System (GPS) phone triangulation);
- how such data is required to be managed on receipt;
- whether, how, and for how long such data is then stored; and
- to whom that data may then be secondarily disclosed or used under section 300."[13]

The Scrutiny of Bills Committee was also concerned at the lack of clarity around; what safeguards would apply to information disclosed under ss287 and 300, what kind of information may be requested under those provisions and the process for considering those requests. They acknowledge the potential unfavourable impact on an individual's privacy in these circumstances.

2.6 It is worth noting that:

---

[6] Inquest into the death of Thomas Hunt https://coroners.nsw.gov.au/coroners-court/download.html/documents/findings/2020/Findings_Thomas_Hunt.pdf
[7] ibid p. 14
[8] Ibid p37-38
[9] For example, the initial investigating officer had not rung Thomas phone, no risk assessment had been done, and there had been confusion about whether a person's health included their mental health.
[10] Op cit PJCHR .p 62
[11] Inquest into the disappearance of CD p3-4 https://coroners.nsw.gov.au/coroners-court/download.html/documents/findings/2022/Inquest_into_to_the_Disappearance_of_CD_-_Findings.pdf
[12] Op.cit PJCHR para 1.123 p. 57
[13] Op.cit PJCHR p. 60

a) there were a number of objections to the proposed ALRC recommendation to amend s287, which was never implemented.

For example the ALRC recommendation "deemed it inappropriate for a threat to be considered 'serious' as well as 'imminent' given that any analysis of 'seriousness' must involve consideration of the gravity of the potential outcome as well as the relative likelihood."[14] The South Australian Government, however, expressed the view that "removing the word imminent and solely relying on the word 'serious' does not fully take into account the 'likelihood' of any threat. Therefore, it would seem more appropriate to replace 'imminent' with another term that represents likelihood, but without the implied urgency or immediacy of 'imminent'. This is consistent with a risk management approach, which generally assesses likelihood as well as consequence."[15] The Office of the Privacy Commissioner (OPC) submitted that if the imminence requirement is removed, 'serious' should be defined to include an assessment of the relative likelihood of the threat eventuating.[16]

The OPC considered that "the imminence test is an important source of privacy protection and removing it would lower privacy protection,"[17] and that "framing the test solely in terms of a 'serious threat' denies individuals the opportunity to exercise an appropriate degree of control over the disclosure of their personal information.",[18] and,

b) the environment in which information collection and sharing has changed since the ALRC Report was prepared.

The ALRCs examination of the removal of the word imminent was mainly in the context of the *Privacy Act 1988* (Privacy Act).[19] The Privacy Act is undergoing a major review with a report being recently handed to the Attorney General. The review is anticipated to include a definition of personal information in line with international data protection frameworks, such as the General Data Protection Regulation, which provides a definition of 'Personal Data' that explicitly includes location data and online identifiers. Including privacy protections around location data, currently lacking in the Privacy Act, is relevant to the proposed amendments to S.287 and necessary to ensure individuals are afforded appropriate privacy protections.[20]

2.7 Any interpretation of a serious threat should take into account what a reasonable person would regard as serious. The ALRC proposed that whether a threat is serious should involve consideration of its gravity as well as its relative likelihood.[21] The Explanatory Note states that, "The Parliament intends that regulated entities would largely be reliant on the representations made by law enforcement or emergency service organisations to determine whether a threat was 'serious'." NSWCCL considers that there needs to be guidance in the Bill as to how operationally a serious threat should be determined in respect of both ss287 and 300.

2.8 A decision to require disclosure of information protected by Part 13 should not be made without consideration of the wishes and circumstances of the person to whom the information relates. This

[14] Op.cit. Explanatory Note- Statement of Compatibility with Human Rights
[15] Government of South Australia, Submission PR 565, 29 January 2008. https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/25-use-and-disclosure/circumstances-in-which-use-and-disclosure-is-permitted/#_ftn97
[16] Office of the Privacy Commissioner, Submission PR 499, 20 December 2007. https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/25-use-and-disclosure/circumstances-in-which-use-and-disclosure-is-permitted/#_ftn101
[17] ibid
[18] ibid
[19] Op.cit. PJCHR p.61
[20] NSWCCL Submission- Attorney-General's Department- Privacy Act Review Discussion Paper (9 January 2022) page 6 https://d3n8a8pro7vhmx.cloudfront.net/nswccl/pages/6282/attachments/original/1643249153/2022.01_NSWCCL_submission_Privacy_Act_discussion_paper.pdf?1643249153
[21] Op.cit. ALRC Report para 25.72

should include considering whether they have expressed any view about not being located in the event of disappearance, and whether they may be the victim of domestic violence. Cogently recorded expressions of a desire not to be located should respected, unless compelling reasons suggest otherwise. Disclosure of information should not be required where such disclosure may place a person at risk of domestic violence.

APP 6.2(a) is relevant, in that it permits an APP entity to use or disclose personal information for a secondary purpose if the individual would reasonably expect the entity to use or disclose the information for that secondary purpose.

The Office of the Information Commissioner (OAIC) explains that the "'reasonably expects' test is an objective one that has regard to what a reasonable person, who is properly informed, would expect in the circumstances. This is a question of fact in each individual case. It is the responsibility of the APP entity to be able to justify its conduct." NSWCCL considers it appropriate for a 'reasonably expects' test to be a factor in determining whether the information should be requested of the carriage service provider.

3. Authorising the use and disclosure of unlisted numbers and associated addresses for the purposes of dealing with matters raised by a call to an emergency service number

3.1 NSWCCL does not support the authorisation of use and disclosure of unlisted numbers and associated addresses without appropriate privacy protections dealing with disclosure, storage and destruction of that information. Importantly "the Bill does not confine the changes to mobile phone triangulation information or to missing persons cases."[22] It is acknowledged that, potentially, metadata could be provided to law enforcement agencies.

3.2 s285 of the Act establishes limited exceptions for the disclosure of information in the IPND. The Scrutiny Committee expressed concerns at amendments to this section in the Bill, namely that:

a) persons receiving disclosed information aren't restricted to emergency call persons,

b) such a provision is unnecessary considering that there are existing provisions in the Act which may be used to disclose information relating to unlisted numbers (exceptions under ss 289,290 or 291).

c) Proposed subsection 285(1B) does not provide safeguards on how data may be handled, used stored or destroyed. [23]

S286 of the Act also provides that a person can make a secondary disclosure to police, fire or ambulance services for purposes connected with dealing with matters raised by an emergency services call. The PJCHR are concerned that the Statement of Compatibility in the Explanatory Note failed to explain why the proposed amendment to s285 "is necessary despite this existing exception."[24]

4. Conferring of civil immunities on telecommunications companies for the provision of reasonably necessary assistance to the Commonwealth, states or territories to respond during emergencies if a national emergency declaration is in force

4.1 The amendment in the Bill is described in the Explanatory Note as a 'technical' amendment to add a reference to subsection 313(4A) and (4B) to paragraph 313(5)(a). It purports to correct a drafting error in the National Emergency Declaration Act 2020.[25]

[22] Op.cit. Bills Digest p.9

[23] Op.cit Scrutiny of Bills Committee para1.1; also, op.cit. PJCHR para 1.125

[24] Op cit. PJCHR para 1.124

[25] Op.cit. Explanatory Notes para 21

4.2 NSWCCL does not support the proposed amendment which, rather than being a mere technical amendment, would have the effect of denying individuals, whose privacy rights have been breached or been caused damage, any redress. The PJCHR emphasised that "parties must comply with the fundamental obligation to provide a remedy that is effective".[26] Individuals should not be expected to bear the burden of managing privacy risks themselves.

4.3 The Scrutiny of Bills Committee considered that there was no sufficient justification for introducing a provision conferring immunity from liability. The committee notes also "that civil immunity would be extended to agents of a carrier or carriage service provider by virtue of the existing subsection 313(6)." [27] Furthermore, there is no detail of any independent oversight of the operation of the conferral of the immunity.

4.4 The Explanatory Notes state that the "proposed amendment reflects the intention that such entities should not be liable to an action or other proceeding in relation to providing assistance."[28] NSWCCL can see no justification for this statement especially considering Australia has no:

a) Commonwealth human rights legislation - NSWCCL affirms its long-standing active support for a national human rights charter. The recurrent resistance of Australia's politicians to a number of widely supported attempts to introduce a national human rights bill/charter over the last 44 years has left Australia as the only liberal democracy without either constitutional or statutory broad protection for fundamental human rights;

b) statutory right to sue for breach of privacy. NSWCCL supports the creation of a direct right of ` action (statutory tort for invasion of privacy) and considers it important that individuals can personally litigate a claim for breach of their privacy. NSWCCL considers that a statutory framework is necessary to ensure that the public's expectation of privacy protection is given form. Currently, the common law has failed to give effect to a tort of privacy invasion, for which there is strong public support. An extensive and robust statutory tort would address a misuse of private information (such as abuses of collection or disclosure of personal information).

5. Amendment of record-keeping requirements to require more detailed records of information to be recorded for authorised disclosures.

5.1 Though NSWCCL supports the principle of recording the secondary purposes for which the information was sought, the information which is retained must be subject to strict data retention rules. The information required to be retained by a carriage service provider under s 187AA(1) of the Act includes personal information such as name, address and information relating to the subscribers' communications. Records are required to be retained for 3 years however details of how those records are stored and destroyed after the 3-year period is unclear. The recent Optus breach has demonstrated the public's need for more data protections and less information sharing.

5.2 The Deputy Coroner in the Thomas Hunt inquest expressed the view that the Missing Persons Registry should "consider and implement a protocol whereby the information available in support of an application to the State Coordination Unit to access the location of a mobile telephone device … be recorded and the reasons for that application decision be recorded."[29]

5.3 NSWCCL agrees with the Deputy Coroner and recommends further that record keeping either by carriage service providers or public service entities be regularly audited and subject to the scrutiny of an independent monitor.

[26] Op.cit. PJCHR para 1.140
[27] Op.cit. Scrutiny of Bills Committee para 1.24
[28] Op.cit. Explanatory Notes part 1 3c(ii)
[29] Op.cit. Thomas Hunt Inquest p.38

6. NSWCCL Recommends that:

6.1 None of the provisions set out in the Bill should be without a strong regime of privacy safeguards in place (including strict data retention measures) to ensure that police and other agencies properly protect personal information held and released by carriage service providers. Those safeguards should encompass consideration of less restrictive alternatives that could achieve the same objective.

6.2 The concerns of the PJCHR and the Scrutiny Committee should be addressed and resolved in their entirety. The Bill should specifically deal with: the process by which s287 is invoked; what specific kinds of information may be requested; how data may be handled, used, stored or destroyed; and, to whom data will be secondarily disclosed.

6.3 There should be sufficient justification for the necessity of the amendment where the Act already permits the use and disclosure of information for the relevant purposes; for example, there are existing provisions in the Act which may be used to disclose information relating to unlisted numbers (exceptions under ss 289,290 or 291) and for secondary disclosures (s286).

6.4 As a result of the lack of adequate privacy safeguards and strict data retention policy-

- the word imminent should not be removed from s.287 as the imminence test is an important source of privacy protection and removing it would lower privacy protection,
- there should be no further authorisation for the use and disclosure of unlisted numbers and associated addresses (s285(1B),
- no amendments should be made until the completion of the Privacy Act review, which is relevant to the proposed amendments to S.287.

6.5 There needs to be guidance in the Bill as to how operationally a serious threat should be determined in respect of both ss287 and 300.

6.6 A decision to require disclosure of information protected by Part 13 should not be made without consideration of the wishes and circumstances of the person to whom the information relates, including but not limited to a ‘reasonably expects’ test.

6.7 The Bill should confine the changes to the Act to mobile phone triangulation information and to missing persons cases noting, for example, the concerns of the Scrutiny Committee that persons receiving disclosed information aren’t restricted to emergency call persons.

6.8 There should be no amendment permitting immunity from civil liability to carriage service providers. The proposed amendment would have the effect of denying individuals any redress if their privacy rights were breached without authorisation.

6.9 Any provision for civil immunity requires independent oversight of the operation of the conferral of that immunity.

6.10 The introduction of both Commonwealth human rights legislation, in the form of a national human rights charter, and a statutory right to sue for breach of privacy, should be an urgent priority.

6.11 Records kept, of the information which is sought from the carriage service provider or retained by the public service entity, must be subject to strict data retention rules. Records of the application for information and their reasons should also be kept by the public service entity.

6.12 Record keeping either by carriage service providers or public service entities must be regularly audited and subject to the scrutiny of an independent monitor.

NSWCCL thanks the Department of Infrastructure, Transport, Regional Development, Communications and the Arts for the recent briefing on the Bill.

This submission was prepared by Michelle Falstein on behalf of the New South Wales Council for Civil Liberties. We hope it is of assistance to the Environment and Communications Legislation Committee.

Yours sincerely,

[redacted]

Sarah Baker
Secretary
NSW Council for Civil Liberties

Contacts in relation to this submission:

Michelle Falstein, Assistant Secretary
Mobile: [redacted]
Email: [redacted]