Chapter 1
New and ongoing matters

1.1 The committee comments on the following bill and legislative instrument, and in some instances, seeks a response or further information from the relevant minister.

Bill

Veterans' Entitlements, Treatment and Support (Simplification and Harmonisation) Bill 2024[7]

Purpose	This bill seeks to simplify and harmonise the legislative framework governing veterans' entitlements, rehabilitation and compensation arrangements by providing for all claims for compensation and rehabilitation received from 1 July 2026 to be determined under the *Military Rehabilitation and Compensation Act 2004* and by closing new claims for compensation under the *Safety, Rehabilitation and Compensation (Defence-related Claims) Act 1998* and *Veterans' Entitlements Act 1986*
Portfolio	Veterans' Affairs
Introduced	House of Representatives, 3 July 2024
Rights	Freedom of assembly; freedom of expression

Contempt offences

1.2 The bill would provide that a person commits an offence if they engage in certain conduct with respect to the Veterans' Review Board (the Board), including if they:

- insult another person in, or in relation to, the exercise of the other person's powers or functions under Part 4 of the *Military Rehabilitation and*

[7] This entry can be cited as: Parliamentary Joint Committee on Human Rights, Veterans' Entitlements, Treatment and Support (Simplification and Harmonisation) Bill 2024, *Report 6 of 2024*; [2024] AUPJCHR 41.

Compensation Act 2004,[8] which relates to review of original determinations by the Board;[9]

- interrupt the proceedings of the Board;
- create, or take part in creating or continuing, a disturbance in or near a place where the Board is sitting; and
- engage in conduct that, if the Board were a court of record, would constitute a contempt of that court.[10]

1.3 The offences would be punishable by imprisonment for six months. By way of background, the Board is a specialist tribunal that reviews original determinations of the Military Rehabilitation and Compensation Commission or the Chief of the Defence Force, namely decisions relating to veterans' entitlements and compensation.

International human rights legal advice

Rights to freedom of assembly and expression

1.4 Prohibiting a person from engaging in insulting conduct, interrupting the proceedings of the Board or creating, or taking part in creating or continuing, a disturbance in or near a place where the Board is sitting, engages and may limit the right to freedom of assembly and the right to freedom of expression. The right to freedom of assembly provides that all people have the right to peaceful assembly.[11] It protects the right of individuals and groups to meet, gather and engage in peaceful protest and other forms of collective activity in public. The right to peaceful assembly is strongly linked to the right to freedom of expression, as it is a means for people to collectively express their views. The right to freedom of expression includes the freedom to seek, receive and impart information and ideas of all kinds, either orally, in writing or print, in the form of art, or through any other media of an individual's choice.[12] The right extends to the communication of information or ideas through any medium, including oral communication and public protest. The right embraces expression that may be regarded as deeply offensive and insulting, subject to the limitations placed on this right in the International Covenant on Civil and Political

---

8 Schedule 3, Part 1, item 10 would repeal and substitute Part 4 of the *Military Rehabilitation and Compensation Act 2004* to extend the Board's jurisdiction to include certain decisions under the *Safety, Rehabilitation and Compensation (Defence-related Claims) Act 1998* and *Veterans' Entitlements Act 1986*.

9 Schedule 3, Part 1, item 10, section 352A would provide that a claimant may make an application to the Board for review of an original determination. Section 345 of the *Military Rehabilitation and Compensation Act 2004* defines 'original determination' as a determination of the Commission under the Act or a determination of the Chief of the Defence Force under the Act that relates to rehabilitation for a person.

10 Schedule 3, Part 1, item 10, section 353L.

11 International Covenant on Civil and Political Rights, article 21.

12 International Covenant on Civil and Political Rights, article 19(2).

Rights.[13] The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has stated that 'the right to freedom of expression includes expression of views and opinions that offend, shock or disturb'.[14] These rights may be subject to permissible limitations that are necessary to pursue certain legitimate objectives, namely to protect the rights or reputations of others, national security, public order, or public health or morals. Additionally, such limitations must be prescribed by law and be rationally connected and proportionate to the legitimate objective.

1.5 The statement of compatibility does not acknowledge that these human rights are engaged and so provides no assessment as to the compatibility of the measure with these rights. The explanatory memorandum states that the contempt offences are based on section 170 of the *Veterans' Entitlements Act 1986*. It states that the policy intent of these provisions is to promote the effective operation of the Board.[15] While promoting the effective operation of the Board is capable of constituting a legitimate objective in general, it must also be demonstrated that this objective is necessary and addresses an issue of public or social concern that is pressing and substantial enough to warrant limiting rights. In this regard, it is not clear that insulting a person or creating a disturbance near a place where the Board is sitting would necessarily prevent the Board from exercising their powers or undertaking their functions such that the Board was unable to effectively operate. Noting the important status of the right to freedom of expression under international human rights law and its protection of insulting expression,[16] it is not clear that insulting a person or creating a disturbance near a place where the Board is sitting would necessarily prevent the Board from exercising their powers or undertaking their functions such that there would be a pressing and substantial need to deter these activities.

1.6 In assessing proportionality, a relevant consideration is the breadth of the measure. The proposed offences capture a broad scope of conduct, including conduct that is insulting or that creates a disturbance near a place where the Board is sitting. Neither of the terms 'insult' or 'disturbance' are defined in the bill, nor is their meaning

---

13 UN Human Rights Committee, General Comment No. 34, *Article 19: Freedoms of opinion and expression* (2011) [11] and [38]. This is subject to the provisions of article 19(3) and article 20 of the International Covenant on Civil and Political Rights. Article 19(3) states that the right to freedom of expression carries with it special duties and responsibilities, and may be subject to restrictions but only such that are provided by law and are necessary for respecting the rights or reputations of others, or to protect national security, public order, public health or morals. Article 20 provides any propaganda for war, and advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited.

14 UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, A/HRC/17/27 (2011) [37].

15 Explanatory memorandum, p. 65.

16 UN Human Rights Committee, *General comment No. 34: Article 19: Freedoms of opinion and expression* (2011) [2]–[3].

addressed in the explanatory materials. By framing the offences so broadly, there appears to be a risk that the provisions may criminalise legitimate criticism of, or objection to, the Board and its proceedings, and legitimate protests in or near buildings within which a proceeding was being held, including protests that do not prevent the Board from carrying out its functions, and may be unrelated to the operation of the Board. It is also not clear why it is necessary to make it an offence to insult a person, interrupt a proceeding or create a disturbance in or near the Board in light of the specific contempt offence in the bill, which makes it an offence to engage in conduct that would constitute a contempt of a court of record.[17] A contempt of court includes conduct that interferes with or undermines the authority, performance or dignity of the courts, including abusing and swearing at a magistrate, refusing to leave the court when directed and disobeying court orders.[18] As such, there appears to be overlap between the specific contempt offence and the other proposed offences of insulting a person, interrupting Board proceedings and creating a disturbance. It is therefore not clear why the specific contempt offence alone is not sufficient to address conduct that may disrupt or interfere with the effective operation of the Board. As drafted, the proposed offences do not appear to be sufficiently circumscribed, and do not appear to be the least rights restrictive way to achieve the stated objective. As such, these provisions risk disproportionately limiting the rights to freedom of expression and assembly.

Committee view

1.7 The committee notes that proposed section 353L of the bill would make it an offence, punishable by six months imprisonment, to insult a person in relation to the exercise of that person's powers or functions under *the Military Rehabilitation and Compensation Act 2004*; interrupt proceedings of the Veterans' Review Board (the Board); create a disturbance in or near a place where the Board is sitting; or engage in conduct that would constitute a contempt of court. The committee considers that this engages and limits the rights to freedom of assembly and expression.

1.8 The committee notes that the statement of compatibility does not acknowledge that this measure limits these rights and so provides no assessment as to whether the limitations are permissible. The committee notes that the purpose of the measure is to promote the effective operation of the Board. While the committee considers this to be an important objective, particularly in light of the important role the Board plays in reviewing decisions about veterans' entitlements and compensation, it is not clear that this objective is necessary and addresses an issue of public or social concern that is pressing and substantial enough to warrant limiting rights. The committee considers there to be a risk that the offences are framed so broadly that they may criminalise legitimate conduct that would otherwise be

---

17 Schedule 3, Part 1, item 10, subsection 353L(5).

18 Judicial Commission of New South Wales, *Local Court Bench Book* (November 2019) [48-020].

protected under international human rights law, such as peaceful protest (including protests not related to the Board) and legitimate criticism of the Board. The committee further considers that the measure is not drafted in the least rights restrictive way to achieve the stated objective, noting that there appears to be overlap between each offence. The committee therefore considers that the measure risks disproportionately limiting the rights to freedom of expression and assembly.

1.9 The committee notes that it has previously reached similar conclusions with respect to contempt offences in other legislation.[19] Most recently, in considering contempt offences in the National Anti-Corruption Commission Bill 2022 (now Act), the committee recommended amending the relevant provision to remove the paragraphs that made it a contempt to use insulting language or create a disturbance near a Commission hearing (given that it was also a contempt to disrupt a hearing or obstruct or hinder a Commission staff member in performing their functions).[20] The Government subsequently advised the committee that it would amend the relevant provision to remove the paragraph that made it a contempt to create a disturbance near a hearing.[21] The committee considers that a similar approach can be adopted with respect to this bill without frustrating its legislative purposes.

Suggested action

1.10 The committee considers the proportionality of this measure may be assisted were the bill amended to:

(a) remove proposed subsections 353L(1) to (4) (which would remove all offences except the contempt of Board offence in subsection 353L(5), which captures much of the conduct targeted in the other offences) or,

---

19 The committee has historically raised repeated concerns regarding the compatibility of similar contempt provisions relating to Royal Commissions (and other bodies invested with the powers of Royal Commissions) and has recommended their amendment. See, for example, Parliamentary Joint Committee on Human Rights, Royal Commissions Amendment Regulation 2016 (No. 1) [F2016L00113], *Thirty-Eighth Report of the 44th Parliament* (3 May 2016) pp. 21-26; Prime Minister and Cabinet Legislation Amendment (2017 Measures No. 1) Bill 2017, *Report 6 of 2017* (20 June 2017) pp. 35-49; Banking and Financial Services Commission of Inquiry Bill 2017, *Report 4 of 2017* (9 May 2017) pp. 42-45; Commission of Inquiry (Coal Seam Gas) Bill 2017, *Report 11 of 2017* (17 October 2017) pp. 51-52; Murray-Darling Basin Commission of Inquiry Bill 2019, *Report 2 of 2019* (12 February 2019) pp. 131–135; National Integrity Commission Bill 2018, National Integrity Commission Bill 2018 (No. 2) and National Integrity (Parliamentary Standards) Bill 2018, *Report 2 of 2019* (12 February 2019), pp. 136–145; National Integrity Commission Bill 2018 (No. 2) and National Integrity Commission Bill 2019, *Report 6 of 2019* (5 December 2019), pp. 99–116.

20 Parliamentary Joint Committee on Human Rights, *Report 5 of 2022* (20 October 2022) pp. 17–20.

21 Parliamentary Joint Committee on Human Rights, *Report 6 of 2022* (24 November 2022) p. 79. The relevant paragraph omitted was section 82(e) of the *National Anti-Corruption Commission Act 2022*.

at a minimum, remove proposed subsections 353L(3) and (4) (which make it an offence to create, or take part in creating or continuing, a disturbance in or near a place where the Board is sitting); and

(b) provide that the conduct that each offence seeks to criminalise must reach such a level that the Board is effectively unable to operate.

1.11 The committee recommends that the statement of compatibility be updated to provide an assessment of the compatibility of the measure with the rights to freedom of assembly and freedom of expression.

1.12 The committee draws these human rights concerns to the attention of the minister and the Parliament.

Legislative instrument

Telecommunications (Interception and Access) (Criminal Law-Enforcement Agency—ACT Integrity Commission) Declaration 2024[22]

FRL No.	F2024L00646
Purpose	This declaration declares the ACT Integrity Commission to be a criminal law-enforcement agency and its staff members to be officers under subsection 110A(3) of the *Telecommunications (Interception and Access) Act 1979* to enable it to access stored communications and telecommunications data
Portfolio	Attorney-General's Department
Authorising legislation	*Telecommunications (Interception and Access) Act 1979*
Disallowance	15 sitting days after tabling (tabled in the House of Representatives on 24 June 2024). Notice of motion to disallow must be given by 22 August 2024 in the House[23]
Right	Privacy

Access to stored communications and telecommunications data by ACT Integrity Commission staff

1.13 This instrument declares the ACT Integrity Commission (the Commission) to be a 'criminal law-enforcement agency' and each staff member of the Commission to be 'officers' for the purposes of the *Telecommunications (Interception and Access) Act 1979* (TIA Act).[24] The declaration is subject to the condition that officers of the Commission may not exercise powers under the TIA Act with respect to any preliminary inquiries conducted by the Commission.[25]

1.14 Declaring the Commission to be a 'criminal law-enforcement agency' means that an officer of the Commission can apply for a stored communications warrant in

---

22 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Telecommunications (Interception and Access) (Criminal Law-Enforcement Agency—ACT Integrity Commission) Declaration 2024, *Report 6 of 2024*; [2024] AUPJCHR 42.

23 In the event of any change to the Senate or House's sitting days, the last day for the notice would change accordingly.

24 Section 3.

25 Section 4. Under section 86 of the *Integrity Commission Act 2018* (ACT), the Commission may carry out a preliminary inquiry to decide whether to dismiss, refer or investigate a corruption report.

order to access stored communications in respect of a person.[26] Stored communication refers to the contents of communications sent via telecommunications systems, such as messages and emails, that are stored by the telecommunications provider or carrier and cannot be accessed by a person who is not a party to the communication without the assistance of the provider.[27] Additionally, the TIA Act provides that authorised officers of an enforcement agency can access and disclose telecommunications data for the purposes of enforcing the criminal law or a law imposing a pecuniary penalty, or for the protection of public revenue.[28] An enforcement agency includes a criminal law-enforcement agency, meaning that officers of the Commission would also be able to access telecommunications data.[29] Telecommunications data is information about a communication – such as the phone number and length of call or email address from which a message was sent and the time it was sent – but does not include the content of the communication.[30] The effect of this declaration is therefore to authorise officers of the Commission to access stored communications, via a warrant, and telecommunications data.

International human rights legal advice

Right to privacy

1.15 Insofar as the effect of this declaration is to enable officers of the Commission to access stored communications and telecommunications data, the right to privacy is engaged and limited. This is acknowledged in the statement of compatibility.[31] The right to privacy includes respect for informational privacy, including the right to respect for private and confidential information, particularly the storing, use and sharing of such information.[32] It also includes the right to control the dissemination of information about one's private life. The type of information protected includes substantive information contained in communications as well as metadata.[33] Stored communications and telecommunications data reveals highly personal information

---

26 *Telecommunications (Interception and Access) Act 1979*, sections 110 and 110A.

27 *Telecommunications (Interception and Access) Act 1979*, section 5 defines 'stored communication' as communication that is not passing over a telecommunications system; and is held on equipment that is operated by, and is in the possession of a carrier; and cannot be accessed on that equipment by a person who is not a party to the communication without the assistance of an employee of the carrier. See also explanatory statement, [4].

28 *Telecommunications (Interception and Access) Act 1979*, Part 4.1, Division 4.

29 *Telecommunications (Interception and Access) Act 1979*, paragraph 176A(1)(a).

30 *Telecommunications (Interception and Access) Act 1979*, section 172. See also explanatory statement, [6].

31 Statement of compatibility, p. 7.

32 International Covenant on Civil and Political Rights, article 17.

33 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/39/29 (2018) [6].

about an individual, including the content of messages, who a person is in contact with, how often and where. The Commission will also be able to access information not only in relation to the person to whom the warrant applies, but also anyone in contact with them. The United Nations (UN) High Commissioner for Human Rights has stated that the generation and collection of data relating to a person's identity, family or life as well as the examination or use of that information, interferes with the right to privacy, as the individual loses some control over information that could put his or her privacy at risk.[34] The right to privacy may be subject to permissible limitations where the limitation pursues a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective.

1.16 The Parliamentary Joint Committee on Human Rights has previously commented on similar declarations that declared the NSW Department of Communities and Justice to be an enforcement agency, and each staff member of Corrective Services NSW to be an officer for the purposes of the TIA Act.[35] The committee concluded that these declarations were not compatible with the right to privacy as the necessity of the power had not been established, noting that all other corrective services agencies access telecommunications data via the police, and the power was insufficiently defined, noting that as a matter of law thousands of employees could access the data. The committee recommended that at a minimum the declaration be amended to specify only those staff members who require access to telecommunications data to be officers for the purposes of the TIA Act.[36] As this declaration enables the Commission to not only access telecommunications data but also stored communications, these same human rights concerns apply and are set out below.

Legitimate objective

1.17 The statement of compatibility notes that the Commission is responsible for investigating alleged and actual serious and systemic corrupt conduct within the ACT public sector and providing support for the prosecution of these crimes by territory and Commonwealth prosecution authorities.[37] It states that in furthering the Commission's ability to combat corruption, the declaration addresses the objectives of national security and public order.[38]

1.18 In general terms, national security and public order have been recognised as being capable of constituting legitimate objectives for the purposes of international

---

34 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/39/29 (2018) [13].

35 See Parliamentary Joint Committee on Human Rights, *Report 5 of 2024* (26 June 2024) p. 8; *Report 8 of 2023* (20 August 2023) pp. 181–189; and *Report 6 of 2023* (14 June 2023) pp. 39–44.

36 Parliamentary Joint Committee on Human Rights, *Report 8 of 2023* (20 August 2023) p. 189.

37 Statement of compatibility, p. 7.

38 Statement of compatibility, p. 8.

human rights law. However, it is not clear that investigating alleged corrupt conduct within the ACT public sector would be such a serious criminal offence as to amount to a genuine threat to national security. The former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression raised concerns with respect to the use of '[v]ague and unspecified notions of "national security"' as a 'justification for the interception of and access to communications in many countries'.[39] The UN High Commissioner for Human Rights has also cautioned that '[v]ague and overbroad justifications, such as unspecific references to "national security" do not qualify as adequately clear laws'.[40]

1.19 In this regard, the explanatory materials cite national security as a justification for the Commission accessing communications data, but do not articulate the specific national security threat which the measure seeks to address or identify how corrupt conduct by territory public servants poses a genuine risk to national security (or public order). It is therefore not clear that the stated objectives of national security and public order would be legitimate in the context of this specific measure. However, accessing communications in order to identify and investigate alleged corrupt conduct would itself appear capable of constituting a legitimate objective for the purposes of international human rights law.[41]

1.20 It must also be demonstrated that there is a pressing and substantial concern which gives rise to the need for the specific measures. The statement of compatibility states that telecommunications data is vital in establishing the ownership or location of mobile phones used to commit offences, and stored communications may disclose criminal or corrupt conduct. It states that accessing this information would assist the Commission to better identify, investigate and prevent serious and systemic corrupt conduct within the ACT public sector and would ensure any criminal offences are appropriately detected and prosecuted. More specifically, the explanatory statement states that accessing this information would increase the Commission's capacity to

---

39 UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, A/HRC/23/40 (2013) [58]. They described national security as an amorphous concept, which is broadly defined, and is thus vulnerable to manipulation by the State as a means of justifying actions that target vulnerable groups such as human rights defenders, journalists or activists (at [60]). They cautioned that inadequate national legal frameworks with respect to accessing and using communications data on the ground of national security 'create a fertile ground for arbitrary and unlawful infringements of the right to privacy in communications and, consequently, also threaten the protection of the right to freedom of opinion and expression' (at [3]).

40 UN High Commissioner for Human Rights, *The Right to privacy in the digital age*, A/HRC/39/29 (2018) [35].

41 Some human rights contained in the International Covenant on Civil and Political Rights may be restricted only in particular circumstances, including where it is necessary for national security or public order (for example, the right to freedom of movement). That restricted limitation does not apply to the right to privacy under article 17 of the ICCPR. See, ICCPR, articles 12-14; 19; and 21-22.

gather and analyse relevant information and pursue search and surveillance device warrants.[42] However, the statement of compatibility does not fully address why it is insufficient for the Commission to rely on the police to access this information for the purpose of investigating and prosecuting alleged offences. This appears to be particularly pertinent given the seemingly small number of investigations undertaken by the Commission into alleged criminal conduct.[43]

1.21 Consequently, it has not been clearly established that there is a pressing and substantial concern that warrants the Commission having direct access to telecommunications data (rather than partnering with the police).

Proportionality

1.22 In order to be proportionate, a limitation on the right to privacy should only be as extensive as is strictly necessary to achieve its legitimate objective and must be accompanied by appropriate safeguards. The UN Human Rights Committee has stated that legislation must specify in detail the precise circumstances in which interferences with privacy may be permitted.[44]

1.23 The declaration declares each staff member of the Commission to be an officer for the purposes of the TIA Act, meaning all staff may access stored communications and telecommunications data obtained. While the Commission appears to have a relatively small number of staff,[45] it is unclear why all staff members require access to communications data rather than it being restricted to only those staff members who require access to the data to perform their functions. The explanatory statement states that the Commission has a purpose-built electronic data storage system for protected and sensitive information that is accessible only by authorised staff, and states that there is a clear hierarchy of approval before consent is given to make an authorisation under the TIA Act. It also states that there are clearly defined processes to record authorisations requests, outcomes and use of information obtained, as well as training on data retention laws, including authorised officer considerations.[46] If

---

42 Explanatory statement, [15].

43 Of the thirteen investigations undertaken by the Commission in 2022-23, only two investigations related to criminal conduct, the rest relating to abuse of office, misuse of official information and mismanagement of a conflict of interest. See ACT Integrity Commission, *2022-23 Annual Report* (September 2023) p. 38. Between 1 July 2023 and 31 December 2023, of all allegations received by the Commission, based on an initial assessment of the type of corrupt conduct being alleged, 9 percent (or 7 allegations) related to criminal conduct (including fraud). See ACT Integrity Commission, *ACT Integrity Commission Statistics 1 July 2023 to 31 December 2023* (2024).

44 UN Human Rights Committee, *General comment No.16: Article 17 (Right to Privacy)* (1988) [8]; *NK v Netherlands*, UN Human Rights Committee Communication No.2326/2013 (2018) [9.5].

45 24 full time equivalent staff as at 31 December 2023. ACT Integrity Commission, *ACT Integrity Commission Statistics 1 July 2023 to 31 December 2023* (2024).

46 Explanatory statement, [21].

these policies and practices were, in practice, to restrict access to communications data to a limited number of staff within the Commission that have a specific need for the data, it may assist with proportionality. However, as a matter of law, all staff members could be authorised to access the data. Where a measure limits a human right, discretionary or administrative safeguards alone may not be sufficient for the purpose of a permissible limitation under international human rights law. This is because administrative and discretionary safeguards are less stringent than the protection of statutory processes and can be amended or removed at any time.

1.24 In addition to the Commission's internal policies and practices outlined above, the explanatory materials identify the following safeguards that may assist with proportionality:

- the requirement to comply with the *Information Privacy Act 2014* (ACT), which includes a binding scheme that provides for the protection of personal information, and the Territory Privacy Principles, which are comparable to the Australian Privacy Principles;[47]
- oversight by the Commonwealth Attorney-General and the Office of the Commonwealth Ombudsman;[48] and
- the condition that the Commission and its staff may not access stored communications and telecommunications data for the purposes of preliminary inquiries.[49]

1.25 In relation to stored communications, requiring a warrant to access stored communications would assist with ensuring that the potential interference with privacy is targeted and only as extensive as is strictly necessary. A stored communications warrant may be issued where the issuing authority is satisfied of certain matters, including that there are reasonable grounds for suspecting that a particular carrier holds the relevant stored communications; the information that would be obtained by accessing the stored communications would likely assist with an investigation of a serious contravention of the Act; and, having regard to specified matters, including the potential interference with a person's privacy and the extent to which alternative methods of investigating the contravention have been used, the issuing authority should issue the warrant.[50] An issuing authority is defined as a judge, magistrate or a person who is an Administrative Appeals Tribunal (AAT) member and

---

47 Explanatory statement, [18] and [19]; statement of compatibility, p. 8.

48 Explanatory statement, [22]; statement of compatibility, p. 8.

49 The statement of compatibility noted that the ACT Government wanted to restrict the use of coercive and covert powers during preliminary inquiries due to the impact of those powers on human rights and thus potential engagement with the *Human Rights Act 2004* (ACT). Statement of compatibility, p. 8.

50 *Telecommunications (Interception and Access) Act 1979*, section 116.

is a legal practitioner who has been enrolled for at least five years.[51] A stored communications warrant remains in force until it is first executed or until the end of the period of five days after the day on which it was issued, whichever occurs sooner.[52] Requiring consideration of certain matters when issuing the warrant, particularly the potential interference with an individual's privacy as well as the extent to which alternative investigation methods have been used, and limiting the time in which the warrant is in force, would assist with proportionality.

1.26 However, the overall safeguard value of a stored communications warrant is somewhat weakened by the fact that warrants may be issued by AAT members. While not an absolute requirement, judicial authorisation of surveillance activities is considered 'best practice' in international human rights law jurisprudence.[53] Indeed, the European Court of Human Rights has held that 'judicial control [offers] the best guarantees of independence, impartiality and a proper procedure'[54] and that 'control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny'.[55] The UN Human Rights Committee has also recommended that States parties provide for 'judicial involvement in the authorization or monitoring of surveillance measures' and consider

---

51 *Telecommunications (Interception and Access) Act 1979*, section 6DB.

52 *Telecommunications (Interception and Access) Act 1979*, section 119.

53 See *Case of Big Brother Watch and Others v The United Kingdom*, European Court of Human Rights, Application nos. 58170/13, 62322/14 and 24960/15 (2019) [320]. See also *Roman Zakharov v Russia*, European Court of Human Rights, Grand Chamber, Application no. 47143/06 (2015) [233]; *Klass and Others v Germany*, European Court of Human Rights, Application no. 5029/71 (1978) [55]; *Szabó and Vissy v Hungary*, European Court of Human Rights, Application no. 37138/14 (2016) [77].

54 *Roman Zakharov v Russia*, European Court of Human Rights, Grand Chamber, Application no. 47143/06 (2015) [233]. See also *Klass and Others v Germany*, European Court of Human Rights, Application no. 5029/71 (1978) [55]: 'The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure'.

55 *Szabó and Vissy v Hungary*, European Court of Human Rights, Application no. 37138/14 (2016) [77].

establishing 'strong and independent oversight mandates with a view to preventing abuses'.[56]

1.27 The Parliamentary Joint Committee on Human Rights has previously raised concerns that AAT members do not have all the necessary attributes of a permanent independent judicial authority, such as security of tenure, sufficient independence from the executive, and a high level of legal expertise (noting that the TIA Act only requires AAT members to have five years' experience as a legal practitioner).[57] The AAT will be replaced by a new Administrative Review Tribunal (ART), which is intended to be more independent and will require members to be appointed through a merit-based process.[58] However, many of the concerns associated with the AAT would still apply to the new ART (in particular, no security of tenure for members, with each term of appointment being five years).[59]

1.28 Noting that it has not been clearly established that there is a pressing and substantial concern that warrants the Commission having direct access to telecommunications data (rather than partnering with the police) and that the declaration is broadly framed and not limited only to those officers that require access

---

56 UN Committee on Human Rights, *Concluding observations on the fourth periodic report of the United States of America*, CCPR/C/USA/CO/4 (2014) [22]. See also UN Special Rapporteur on the right to privacy, *Draft Legal Instrument on Government-led Surveillance and Privacy*, Version 0.6 (2018), p. 16. Similarly, the UN High Commissioner for Human Rights has stated that surveillance measures (including communications data requests) should be authorized, reviewed and supervised by independent bodies at all stages, including when they are first ordered, while they are being carried out and after they have been terminated. See, UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/39/29 (2018) [39].

57 See Parliamentary Joint Committee on Human Rights, Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020, *Report 3 of 2021* (17 March 2021) pp. 63–112, citing UN Special Rapporteur on the right to privacy, *Draft Legal Instrument on Government-led Surveillance and Privacy*, Version 0.6 (2018), p. 16: the UN Special Rapporteur on the right to privacy stated that where domestic law provides for the use of surveillance systems, the law shall 'provide that the individual concerned is likely to have committed a serious crime or is likely to be about to commit a serious crime and in all such cases such domestic law shall establish that an independent authority, having all the attributes of permanent independent judicial standing, and operating from outside the law enforcement agency or security or intelligence agency concerned, shall have the competence to authorise targeted surveillance using specified means for a period of time limited to what may be appropriate to the case'.

58 The Parliamentary Joint Committee on Human Rights commented on the human rights compatibility of terminating certain AAT members in the process of abolishing the AAT and establishing the Administrative Review Tribunal. See Administrative Review Tribunal Bill 2023 and Administrative Review Tribunal (Consequential and Transitional Provisions No. 1) Bill 2023, *Report 1 of 2024* (7 February 2024) pp. 15–42.

59 *Administrative Appeals Tribunal Act 1975*, section 8; *Administrative Review Tribunal Act 2024*, subsection 208(5).

to the data, there is a significant risk that this declaration does not constitute a permissible limitation on the right to privacy.

Committee view

1.29 The committee notes that by declaring the ACT Integrity Commission (the Commission) to be a criminal law-enforcement agency, and its staff to be officers for the purposes of the *Telecommunications (Interception and Access) Act 1979*, the Commission is authorised to access stored communications (via a warrant) and telecommunications data – which includes both the content of messages and emails as well as information about the communication. By authorising the Commission to access this data, the declaration engages and limits the right to privacy.

1.30 The committee considers that accessing communications data to identify and investigate alleged corrupt conduct would likely constitute a legitimate objective. However, the committee considers that it has not been clearly established that there is a pressing and substantial concern that warrants the Commission having direct access to telecommunications data (rather than partnering with the police, who already have the power to access this information). The committee also notes that the declaration is broadly framed and authority to access data is not limited only to those officers that require access to the data. The committee further notes that while requiring a warrant to access stored communications would assist with proportionality insofar as it ensures any interference with privacy is more targeted, the safeguard value of the warrant is weakened by the fact that stored communications warrants may be issued by tribunal members, which departs from best practice under international human rights law. As such, while the measure is accompanied by some safeguards, these do not appear to be sufficient to ensure that any limitation on privacy is proportionate. The committee therefore considers that there is a significant risk that this declaration does not constitute a permissible limitation on the right to privacy.

Suggested action

1.31 The committee considers that the proportionality of this measure may be assisted were the instrument amended to specify only those staff members who require access to telecommunications data to be officers for the purposes of the *Telecommunications (Interception and Access) Act 1979.*

1.32 The committee recommends that the statement of compatibility be updated having regard to the analysis above.

1.33 The committee draws these human rights concerns to the attention of the Attorney-General and the Parliament.