ACT HUMAN RIGHTS COMMISSION
Australian Capital Territory

Ian Govey AM
Independent Review, *Integrity Commission Act 2018*
Via icactreviewsecretariat@act.gov.au

24 March 2023

Dear Independent Reviewer

**ACT Human Rights Commission submission to independent review of the *Integrity Commission Act 2018***

Thank you for inviting the ACT Human Rights Commission to provide a written submission to the review of the ACT *Integrity Commission Act 2018* (the IC Act). Our submission, enclosed below, primarily focuses analysis on the proposal to authorise the ACT Integrity Commission to access telecommunications information under the *Telecommunications (Interception and Access) Act 1979* (TIA Act), given the potential for serious interferences with the right to privacy this could entail.

While the submission below offers brief comment on some other proposed amendments, we have not had opportunity to review these in detail. Proposals we have not addressed in this submission may also have human rights implications that have not been identified in our review. We would therefore welcome the opportunity to assist the Reviewer by providing further advice about the human rights implications of specific proposals that may be recommended at a later stage.

If you have any questions or would like more detailed information on any of the issues raised in this submission, please do not hesitate to contact us on (02) 6205 2222.

Yours sincerely

[redacted]

Dr Helen Watchirs OAM
President and Human Rights Commissioner

# Recommendations

In summary, the Commission recommends that the Independent Reviewer:

1. Assess whether the framework for declared government agencies to access telecommunications information contained in the TIA Act provides for reasonable limitations of the right to privacy and other human rights, including adequate and effective safeguards to ensure that:
    i. Any access to telecommunications material would be strictly necessary for the prevention of corruption or crime and the obtaining of vital intelligence in a particular investigation;
    ii. The scope of any executive or judicial discretion and the manner of its exercise is sufficiently accessible, precise and foreseeable; and
    iii. Decisions about authorising and supervising surveillance incorporate equivalent guarantees in lieu of the subject person's direct participation.
2. Investigate the utility and merits of a Public Interest Monitor function in relation to warrant applications for telecommunications, akin to those operating in Queensland and Victoria.
3. Explore whether the ACT Integrity Commission could be lawfully subject to further obligations and safeguards under ACT legislation, especially in relation to authorised disclosure of telecommunications data under Chapter 4 of the TIA Act.
4. Examine in detail the extent to which telecommunications information could be lawfully used and disclosed by the ACT Integrity Commission for secondary purposes, and the scope (if any) for consideration of human rights in proceedings for remedial relief.
5. Recommend the ACT Integrity Commission be resourced to store lawfully accessed telecommunications information on a separate, secure and dedicated IT system, capable of inspection and audit by the Inspector.
6. Endorse the ACT Integrity Commission's proposal that privilege be partially abrogated for documents and advice belonging to the Territory, but decline to recommend amendments to provide for the Integrity Commissioner to decide claims of privilege.
7. Decline to recommend that the ACT Integrity Commission be empowered to issue witness arrest warrants in *anticipation* of non-compliance with a summons.
8. Recommend that existing legislative constraints on current or former ACTPS employees being engaged or employed by the ACT Integrity Commission be repealed in favour of suitable conflict of interest procedures.
9. Support proposed amendments to ensure greater assistance for witnesses in relation to costs and on-disclosure to registered medical practitioners for health and welfare purposes.

# About the ACT Human Rights Commission

1. The ACT Human Rights Commission (ACTHRC) is an independent agency established by the Human Rights Commission Act 2005 (HRC Act). Its main object is to promote the human rights and welfare of people in the ACT. The HRC Act became effective on 1 November 2006 and the ACTHRC commenced operation on that date. Since 1 April 2016, a restructured ACTHRC has included:

    i. the President and Human Rights Commissioner;

    ii. the Discrimination, Health Services, Disability and Community Services Commissioner;

    iii. the Public Advocate and Children and Young People Commissioner; and

    iv. the Victims of Crime Commissioner.

2. This submission primarily reflects the views and advice of the President and Human Rights Commissioner. Among her various functions, the President and Human Rights Commissioner, Dr Helen Watchirs, advises government on the impact of laws and government services on human rights. She is also responsible for promoting community discussion, and providing education and information, about the HRC Act, the *Human Rights Act 2004* (ACT) (HR Act) and human rights generally.

3. The President and Human Rights Commissioner has previously supported the Select Committee on an Independent Integrity Commission 2018 by providing advice about human rights considerations arising from the draft Integrity Commission Bill.[1] In July 2022, Dr Watchirs and her advisors met with the ACT Integrity Commissioner, Michael Adams QC, to discuss the human rights implications of authorising the ACT Integrity Commission to intercept and access telecommunications and related data.

4. We appreciate that the terms of reference for the Review of the Integrity Commission Act 2018 direct specific attention to whether any recommendations to amend the IC Act are consistent with the HR Act. The ACTHRC has considered the proposals to amend the IC Act and related statutes set out in the ACT Integrity Commission's 2021-22 Annual Report.[2] Our analysis is grounded in the minimum standards contained in the HR Act, with which all legislative proposals must comply to be compatible with human rights.

# A human rights approach

5. In the ACT, the *Human Rights Act 2004* (HR Act) protects a range of fundamental human rights drawn from international human rights law (IHRL) to which all individuals present in the ACT, or subject to its jurisdiction, are entitled.

6. International law and the jurisprudence of foreign and international tribunals relevant to a human right can be drawn on in interpreting the human right (including its nature, scope and content).[3] Rights under the HR ACT are primarily sourced in the International Covenant on Civil and Political Rights. While General Comments and UN treaty body communications are highly relevant, the ACT Supreme

[1] ACT Human Rights Commission, Submission No 07 to Select Committee on an Independent Integrity Commission 2018, ACT Legislative Assembly, *Inquiry into the establishment of an Integrity Commission for the ACT* (31 August 2018), available at: <https://www.parliament.act.gov.au/__data/assets/pdf_file/0011/1244873/07-Human-Rights-Commission.pdf>

[2] See ACT Integrity Commission, *2021-22 Annual Report* (Report, September 2022), from 75; available at <https://www.integrity.act.gov.au/__data/assets/pdf_file/0009/2085129/ACT-Integrity-Commission-2021-22-Annual-Report.pdf>

[3] *Human Rights Act 2004* ('HR Act'), s 31.

Court has also, at times, applied jurisprudence of the European Court of Human Rights (ECtHR). This submission refers to ECtHR jurisprudence as indicative of principles relevant to the right to privacy.

7. It is a general principle of human rights law that human rights are to be interpreted generously and limitations narrowly. Though not expressly recognised in the HR Act, the International Covenant on Civil and Political Rights includes the right to an effective remedy for violations of human rights. European human rights jurisprudence also recognises, as a fundamental principle, that national remedies and procedural rules must not render breaches of human rights impossible or excessively difficult to enforce. This is often communicated as a statement that rights should be practical and effective, not theoretical and illusory.[4] In our view, rights in the HR Act should be understood similarly.

8. Recognising that few human rights are absolute, the HR Act provides for human rights to be subject only to reasonable limits set by laws that can be demonstrably justified in a free and democratic society.[5] In general, this means that any measure that limits a human rights must be: i) set by law; ii) pursue a legitimate objective; iii) be rationally connected to its stated objective; and iv) be proportionate means of achieving that objective.

9. Whether a measure is proportionate will consider whether there are less restrictive ways to achieve the stated aim, adequate and effective safeguards against abuse (including oversight and scope for review), the extent of the interference of the human right and sufficient flexibility to take account of individual circumstances.[6]

10. The HR Act may influence and affect the work of the ACT Integrity Commission in two main ways:

    i. First, section 30 of the HR Act requires that all Territory laws, including the IC Act, must be interpreted in a way that is compatible with human rights so far as it is possible to do so consistently with its purpose. Human rights may therefore be relevant in any legal proceedings to concerning the interpretation of the IC Act, including the scope and operation of coercive powers available to the ACT Integrity Commission.

    ii. Second, Part 5A of the HR Act oblige public authorities, which includes the ACT Integrity Commission,[7] the Commissioner and his staff,[8] to act compatibly with human rights and, when making a decision, to not fail to give proper consideration to a relevant human right.[9] An individual who believes that their human rights have been unreasonably limited by a public authority may initiate proceedings in the ACT Supreme Court or rely on their rights in other legal proceedings including, for example, in criminal prosecutions referred following investigations.

[4] Dr Georgios Serghides, '*The Principle of Effectiveness in the European Convention on Human Rights, in Particular its Relationship to the other Convention Principles*' in *Hague Yearbook of International Law / Annuaire de La Haye de Droit International* 30 (2017), 1-16; see, for example, *M.K. v France* (European Court of Human Rights, App No. 19522/09, 18 April 2013), [44].
[5] HR Act, s 28.
[6] For more information about reasonable limitations of human rights, see Justice and Community Safety Directorate, 'Reasonable and justifiable limitations – Section 28 – Human Rights Act 2004' <https://www.justice.act.gov.au/__data/assets/pdf_file/0008/2072447/Fact-Sheet-W-s-28-Reasonable-and-justifiable-limitations-Human-Rights-Education.pdf>
[7] Explanatory Statement, Integrity Commission Bill 2018 (ACT), 7.
[8] HR Act, s 40(1).
[9] HR Act, s 40B(1).

### *Anti-corruption measures and human rights*

11. The importance of an effective and independent integrity body to investigate, detect and prevent corruption within, and related to, the ACT public sector cannot, in our view, be understated. It is widely accepted in international human rights law (IHRL) and commentary that acts of corruption undermine the protection and enjoyment of fundamental human rights. Corrupt acts often – though not always – represent a violation of an individual's specific human rights; however, they also create and entrench structural barriers that prevent the full enjoyment of all human rights.[10]

12. Corrupt acts may be discriminatory to the extent that they distinguish, exclude, favour, or impair equal protection envisaged by law. It has been suggested that the harms experienced as a result of corruption are disproportionately experienced by marginalised groups or those experiencing vulnerability, often due to barriers they face in accessing justice or remedies.[11]

13. Accountable and effective public administration is vital to good governance, public trust and confidence in government and enjoyment of the fundamental human rights protected in the HR Act. Measures that seek to identify, detect and respond to corruption, whether in the public or private sectors, therefore pursue a legitimate aim for the purpose of limiting human rights.

14. A legislative scheme that creates wide-ranging coercive powers to investigate and report on matters relating to alleged or suspected corruption will, however, also inevitably limit various rights contained in the HR Act. Such powers may limit rights to privacy and reputation (HR Act, s 12), freedom of expression (s 16), the right to fair trial and related criminal proceeding rights (HR Act, ss 21 and 22).

# Powers and jurisdiction

15. Under the Terms of Reference, the Reviewer is asked to consider the powers and jurisdiction conferred on the ACT Integrity Commission by the IC Act, and assess whether they are appropriate and adequate for the investigation of alleged corrupt conduct (including serious and systemic corruption).

16. Our analysis, set out below, primarily focuses on the human rights considerations relevant to the proposal that the ACT Integrity Commission be authorised to intercept and access private telecommunications under the *Telecommunications* (*Interception and Access*) *Act 1979* (Cth) ('TIA Act'). Our assessment is based on relevant human rights standards and principles, as described below.

### *Intercepting telecommunications*

17. The ACTHRC is <u>not</u> necessarily opposed to the ACT Integrity Commission being able to apply for warrants authorising it to intercept telecommunications, and access stored communications and telecommunications data.

18. It is apparent from the report of the Select Committee on an Independent Integrity Commission for the ACT (2018) ('Select Committee') that covert powers, including listening devices and optical

[10] See, for example, Human Rights Council, *Final report of the Human Rights Council Advisory Committee on the issue of the negative impact of corruption on the enjoyment of human rights*, 28th sess, Agenda items 3 and 5, UN Doc A/HRC/28/73 (5 January 2015).

[11] See, for example, André Figueiredo, *Corruption and Human Rights: Beyond the Link*, (Wolf Legal Publishers, 2017).

surveillance, were considered necessary to adequately investigate corrupt conduct.[12] Yet it is not evident that interception of telecommunications under the TIA Act was ever expressly considered by the Select Committee or its predecessor in 2017.

19. Access to telecommunications data and communications would appear to be rationally connected to the effective identification, investigation, and punishment of corruption (in the various forms defined under the IC Act), which is a legitimate aim for the purposes of human rights law. Such power must, however, be demonstrably justified as a legitimate, necessary and proportionate limitation of human rights in accordance with s 28 of the HR Act.

*The right to privacy and reputation*

20. Under the HR Act, a person has a human right not to have their privacy, family, home or reputation interfered with unlawfully or arbitrarily (HR Act, s 12(a)). This 'right to privacy and reputation' encompasses respect for private and confidential information, particularly in relation to its storage, use and sharing, as well as a person's right to control the dissemination of information about their private life. The capture of communications data represents a *prima facie* interference with the right to privacy, as does its retention; whether such data is later used or shared.

21. Covert surveillance, tapping and other forms of interception of telecommunications, whether by government agencies, private enterprise or other third parties, have each been considered a serious interference with the right to privacy,[13] notwithstanding the lack of physical interference with personal integrity or property they involve. The mere *possibility* of communications information being captured under legal frameworks that permit secret access to personal communications has also been held to interfere with privacy, and may have a potential chilling effect on the enjoyment of other human rights, including free expression (HR Act, s 16) and association (HR Act, s 15(2)).[14] In this regard, Andrew Ashworth urges caution against "the covert expansion of the categories to which exceptional and intrusive methods apply."[15]

*Relevant principles*

22. As a first premise, any limitation of the right to privacy must be lawful. This means a measure that limits privacy must be authorised by laws that (a) are publicly accessible; (b) that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (c) are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorising, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected; and (d) provide for effective safeguards against abuse.[16]

23. Measures that interfere with the right to privacy must also not be arbitrary. Arbitrariness is defined not as merely being against the law, but as including elements of "inappropriateness, injustice and lack

[12] Select Committee on an Independent Integrity Commission 2018, ACT Legislative Assembly, *Inquiry into the establishment of an Integrity Commission for the ACT* (Report, October 2018), [6.32].
[13] *Malone v The United Kingdom,* (European Court of Human Rights (Plenary), App No. 8691/79, 2 August 1984), [64].
[14] United Nations Human Rights Council, *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*, 27th sess, agenda items 2 and 3, UN Doc. A/HRC/27/37 (30 June 2014); see also *Klass and Others v Germany* (European Court of Human Rights (Plenary), App No. 5029/71, 6 September 1978), [48].
[15] Andrew Ashworth, *Human Rights, Serious Crime and Criminal Procedure* (Sweet & Maxwell, 2002) 107.
[16] *Weber and Saravia v Germany* (European Court of Human Rights, App No. 54934/00, 29 June 2006) [84]; for comparable discussion of 'set by laws' in ACT jurisprudence, see *Davidson v Director-General, Justice and Community Safety Directorate* [2022] ACTSC 83, [348]-[353].

of predictability."[17] Any interference with privacy must accord with the provisions, aims and objectives of the HR Act and should be reasonable in the circumstances (ie proportionate and necessary to achieve a legitimate aim).[18]

24. Powers of secret surveillance, including covert access to telecommunications, are accordingly tolerable only to the extent that they are strictly necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime[19] and, in particular, for the obtaining of vital intelligence in an individual operation,[20] based on reasonable suspicion with regards to the subject.[21]

25. IHRL acknowledges an appropriate degree of discretion for Governments in assessing whether and the extent to which forms of covert surveillance are necessary; yet emphasises that relevant legislation and decisions applying it must be subject to supervision and oversight.[22] It is therefore highly desirable from a human rights perspective that the judiciary (or an independent administrative body) approve and supervise the conduct of any covert surveillance measures, like telecommunications interception or access to stored communications.[23]

26. Especially where a power reserved to the executive is exercised in secret, the risks of arbitrariness are evident.[24] Due to its inherently secret nature, 'foreseeability' in the context of covert surveillance and interception of personal data has been understood as requiring that an individual would be capable, with legal assistance if necessary, to anticipate when authorities are likely to have recourse to such secret surveillance.[25] In addition, the law must indicate the scope of the discretion granted to the executive or to a judge and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.[26]

27. In particular, a supervising court must be satisfied that there are adequate and effective guarantees against abuse of an authority. To this end, a court must take into account the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law.[27]

---

[17] UN Human Rights Committee, *Views: Communication No 560/1993,* UN Doc CCPR/C/59/D/560/1993 (3 April 1997), [3.1] ('*A v Australia*').
[18] UN Human Rights Committee, *General comment No. 16: Article 17 (Right to privacy)* UN CCPR, 32nd sess, UN Doc CCPR/GC/16 (8 April 1988), [4].
[19] *Szabó and Vissy v Hungary* (European Court of Human Rights (Fourth Section), App No. 37138/14, 12 January 2016), [48]; see also *Digital Rights Ireland Ltd (C-293/12) and Karntner Landesregierung ors (C-594/12) v Minister for Communications, Marine and Natural Resources and ors (Judgment)* (European Court of Justice) C-293/12 and C-594/12 (8 April 2014), [62].
[20] *Szabó and Vissy v Hungary* (European Court of Human Rights (Fourth Section), App No. 37138/14, 12 January 2016), [72]-[73].
[21] *Roman Zakharov v Russia* (European Court of Human Rights (Grand Chamber), App No. 47143/06, 4 December 2015), [260].
[22] Ibid, [232].
[23] Ibid, [233].
[24] *Khan v United Kingdom* (European Court of Human Rights (Third Section), App No. 35394/97, 12 May 2000), [26]-[28].
[25] *Fernández Martínez v Spain* (European Court of Human Rights (Grand Chamber), App No. 56030/07, 12 June 2014), [117].
[26] *Piechowicz v Poland* (European Court of Human Rights (Fourth Section), App No. 20071/07, 17 April 2012), [212].
[27] *Roman Zakharov v Russia* (European Court of Human Rights (Grand Chamber), App No. 47143/06, 4 December 2015), [232].

28. Finally, as the subject person will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established for authorising and supervising surveillance themselves incorporate adequate and equivalent guarantees to safeguarding the subject person's rights.[28]

*Proposed legislative change*

29. The ACT Integrity Commission has sought authorisation to obtain access to telecommunications for the purpose of investigating allegations of corrupt conduct. This would involve:

    i. Obtaining warrants to intercept telecommunications as they occur ('intercepted information');

    ii. Obtaining warrants to access stored communications after they have occurred ('stored communications'); and

    iii. Authorising telecommunications providers to disclose data (ie metadata) about a communication ('telecommunications data').

30. Ability to lawfully intercept telecommunications in real time will depend on the ACT Integrity Commission being declared an 'eligible authority' under Part 2-5 of the TIA Act.[29] Access to stored communications held by service providers will in turn rely on the ACT Integrity Commission being separately declared a 'criminal law-enforcement agency' under Part 3-3 of the TIA Act.[30]

31. Any entity declared to be a 'criminal law-enforcement agency' will also be an 'enforcement agency' for the purposes of Chapter 4 of the TIA Act. That Chapter provides for certain staff of enforcement agencies to authorise service providers to disclose to it telecommunications data (ie metadata, such as mobile service accounts, device IDs, phone numbers, GPS coordinates, times, dates and duration of communications etc.),[31] which they are required to retain for at least two years from the date it was created.[32]

32. Such declarations, effected by the Commonwealth Attorney-General,[33] would also entitle the ACT Integrity Commission to receive intercepted information, stored communications and metadata from other agencies, including the Australian Federal Police; which is presently prohibited.[34]

*Relevant safeguards*

33. Consistent with the human rights principles outlined above, we welcome that applications for warrants under the TIA Act to intercept telecommunications or access stored communications must be decided by an eligible judge or nominated member of the Administrative Appeals Tribunal (AAT), or a federal judge or magistrate.

34. Those who issue such warrants must consider, among other things, the likely interference in a person's privacy, the probative value of the information sought, and to what extent any less restrictive available methods have been used or are available to the agency; each of which, in our view, correspond with whether the interference in the person's privacy would be strictly necessary and proportionate in

[28] Ibid, [233].
[29] *Telecommunications (Interception and Access) Act 1979* (Cth) ('TIA Act').
[30] TIA Act, ss 110-110A.
[31] TIA Act, s 176A(1)(a) and s 187AA.
[32] TIA Act, Part 5-1A (Data Retention).
[33] TIA Act, s 34.
[34] TIA Act, s 63; ss 108-109.

connection with the ACT Integrity Commission's investigation of a serious offence.[35] These criteria, in our opinion, adequately specify the scope of judicial (or quasi-judicial) discretion such as to ensure that the ACT Integrity Commission's access to telecommunications would be strictly necessary in connection with the investigation of serious offences that reflect corruption.

35. We also note that s 35(1)(a) of the TIA Act would require certain minimum safeguards against misuse of intercepted information to be expressly established in ACT legislation and variously implemented by the Integrity Commissioner, the ACT Attorney-General and the Commission's Inspector.[36] Such protections would include:

    - Retention of certain warrant documentation by the Integrity Commissioner;
    - Restricted access to records by authorised personnel and via a secure system;
    - Reporting by the Integrity Commissioner to a responsible Minister within 3 months of a warrant's expiry about how intercepted information has been used or communicated to other persons;
    - Annual reporting to that same Minister and the Australian Government's Minister for Home Affairs about how effective telecommunication services warrants have been;
    - Destruction of records when they are no longer required;
    - Independent inspections of an agency's records by an independent authority;
    - Independent inspection reports to be shared with the Australian Government's Minister for Home Affairs.

36. It is noted that these prerequisite legislative safeguards now apply, as a result of state and territory statutes, to the interception of telecommunications information and data by all interstate anti-corruption bodies in Australia (see Appendix 1). These required provisions and conditions reflect important privacy protections, including physical and digital security of records, duration and destruction, transparency and reporting, and regular audit and oversight.

37. We welcome, in particular, that the proposed ACT legislation would include regular inspections by an independent agency to ensure that intercepted or accessed information is being stored securely and destroyed when no longer required. We understand that, pending consultation, this role would likely be allocated to the Commission's Inspector, which is a role presently performed by the Office of the Commonwealth Ombudsman which provides services as the ACT Ombudsman under a Memorandum of Understanding with the ACT Government.

38. The ACT Ombudsman would, in our view, be a logical body to perform this vital oversight role given its role as Inspector of the Integrity Commission and the Commonwealth Ombudsman's experience and established role in reporting on federal agencies' access to telecommunications under the TIA Act, including non-compliance by ACT Policing in 2021.[37] Oversight of telecommunications interception

[35] TIA Act, ss 46 (for telecommunication service warrants) and 116(2) (for stored communication warrants).
[36] See ACT Integrity Commission, *2021-22 Annual Report* (Report, September 2022), 75.
[37] Commonwealth Ombudsman, *Australian Federal Police's (AFP) use and administration of telecommunications data powers 2010 to 2020:* Access to Immediate Response Location Data under the *Telecommunications (Interception and Access) Act 1979* (Report, April 2021), available at <https://www.ombudsman.gov.au/__data/assets/pdf_file/0021/112476/Report-into-the-AFPs-use-and-administration-of-telecommunications-data-powers.pdf>

may also align well with the Commonwealth Ombudsman's mandated inspection or stored communications and authorised disclosures of telecommunications data under Chapter 4A.[38]

*Public Interest Monitors*

39. Further safeguards exist in other Australian human rights jurisdictions, Queensland and Victoria. Principally, in these jurisdictions a Public Interest Monitor (PIM) must be notified where the relevant integrity body applies for a warrant under Part 2-5 of the TIA Act and supplied with all relevant information about the application, including matters adverse to issuing a warrant.[39] The PIM is then entitled to appear at any hearing of a relevant application to test the content and sufficiency of information relied on in the circumstances of the application.[40]

40. The Queensland Supreme Court has previously characterised the participation of a PIM as a vital safeguard for citizens' right to privacy (albeit prior to enactment of the *Human Rights Act 2019*):[41]

> The role of the public interest monitor is an important one. Just as the courts have been traditionally regarded as "the guardians of the citizens' right to privacy" […], the public interest monitor provides another layer of protection for private citizens who, unknown to those citizens, are sought to be made the subject of a surveillance warrant. In cases such as this where there is an application for the issue of a warrant, the public interest monitor is obliged to critically evaluate the material advanced in support of an application in order to determine whether to question the applicant police officer and/or make submissions on the hearing of the application. This will never be a perfunctory exercise; the public interest monitor must give real attention to the question whether the evidence and information offered by the party applying for the warrant is sufficient to satisfy the decision-maker of the existence of all applicable statutory preconditions and that the material is otherwise such as to justify such an intrusion into the privacy of the citizen in question.

41. The TIA Act provides a limited role for 'Public Interest Advocates' with respect to applications by 'enforcement agencies' for warrants that authorise disclosure of information or documents relating to journalists or intended to identify a journalist's source.[42]

42. From a human rights perspective, the participation of a PIM ensures accountability by providing an independent and adversarial perspective that counterbalances the subject person's necessary inability to themselves contest a warrant application. We acknowledge concerns that such processes may risk undue delay and that PIMs may, in practice, be unable to verify or effectively contest facts, evidence and grounds relied on by an authorised officer in making a warrant application.

43. Submissions by an independent advocate can, in our view, provide vital contestability about the necessity, duration, and potential impacts of warrants on a subject person. Their consideration of application and questioning of an authorised officer may raise new information that assists the court or highlights the risk of disclosure of privileged materials or sources. Insofar as a PIM's participation

---

[38] TIA Act, s 186B.

[39] *Telecommunications (Interception) (State Provisions) Act 1988* (Vic), s 4A; *Telecommunications Interception Act 2009* (Qld), s 7.

[40] *Telecommunications (Interception) (State Provisions) Act 1988* (Vic), s 4A; *Telecommunications Interception Act 2009* (Qld), s 7; for more on various Public Interest Advocate/Monitor, see Law Council of Australia, Submission No 40 to Parliamentary Joint Committee on Security and Intelligence, *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (23 August 2019), available at: <https://www.lawcouncil.asn.au/resources/submissions/supplementary-submission-inquiry-into-the-impact-of-the-exercise-of-law-enforcement-and-intelligence-powers-on-the-freedom-of-the-press>

[41] *R v Riscuta* [2017] QSC 47 (31 March 2017), [23].

[42] TIA Act, s 180X; see also Div 4C.

might risk undue delay or loss of evidence, a decision-maker ought to have inherent jurisdiction or incidental power to require submissions within a reasonable timeframe, having regard to the individual circumstances of the application.

44. A PIM may also serve to promote debate about whether a subject person may, as a condition of the warrant, be notified about the application or access to their telecommunications at some stage in the future (as discussed below) where doing so may no longer prejudice the relevant investigation.

45. We therefore recommend that the Reviewer carefully consider the utility and merits of a PIM with respect to applications by the ACT Integrity Commission for telecommunication service and stored communication warrants. Should an ACT PIM function be recommended, further amendments to the TIA Act akin to those relevant to applications by Victorian and Queensland interception agencies, would be required.[43]

*Warrantless access to metadata and notifying subjects*

46. At a federal level, the Parliamentary Joint Committee on Human Rights ('PJCHR') has examined access to telecommunications data (ie metadata) by criminal law-enforcement agencies under Chapter 4 of the TIA Act.[44] Its analysis identified serious concerns that the framework presented in Chapter 4 did not ensure limitations of that right to privacy that are only as extensive as is strictly necessary, noting:
    - an authorised officer of an enforcement agency being able to themselves authorise a telecommunications service to provide telecommunications data where 'reasonably necessary for the enforcement of a law imposing a pecuniary penalty or the protection of the public revenue',[45] which does not adequately, in the view of the PJCHR, limit the types of investigations for which disclosures of telecommunications data may be authorised.
    - limited constraints on the subsequent use of accessed data for unrelated purposes and the absence of data retention periods or a warrant process.

47. In its concluding report, the PJCHR noted that an enforcement agency may access a person's metadata (which is retained for two years) without the person's knowledge or awareness. Although such data would not include the substance and content of a person's private information, it can still disclose highly sensitive personal information, including about residence, relationships, sexual habits, associations, personal beliefs and religious or medical concerns. As new forms of technology develop, so too do new and more revealing forms of metadata. In this context, the PJCHR highlighted that it is virtually impossible for an aggrieved person who is unaware that their telecommunications *data* has been accessed under Chapter 4 to seek redress for related breaches of their right to privacy (or other rights).

48. The Integrity Commissioner has indicated that the TIA Act would not, by design and operation of various secrecy provisions, permit an agency to notify a subject person that their private information or telecommunications data has been sought, intercepted or otherwise accessed, including after an investigation is closed.[46] These secrecy provisions themselves reflect an important safeguard against

[43] Eg TIA Act, ss 44A, 45, 45A and 46(2).
[44] Parliamentary Joint Committee on Human Rights ('PJCHR'), Parliament of Australia, *Fifteenth Report of the 44th Parliament* (Report, 14 November 2014), 10-22; PJCHR, Parliament of Australia, *Twentieth report of the 44th Parliament* (Report, 18 March 2015, 39-74; and PJCHR, Parliament of Australia, *Thirtieth report of the 44th Parliament* (Report, 10 November 2015), 133-139.
[45] TIA Act, s 179.
[46] TIA Act, s 133 and Chapter 4, Division 6.

misuse of telecommunications information and data to the extent they operate to deter misuse and ensure the policy intent of ensuring effective investigation of serious contraventions of law. Whether a person is practically able to access an effective remedy for breaches of their human rights is, however, highly relevant to the proportionality of limitations, including of the right to privacy.[47]

49. We understand, however, that there may be scope for a warrant issued by an eligible judge or AAT member to impose conditions that a subject person be later notified unless doing so would seriously prejudice the investigation of a serious crime. This serves, in our view, to emphasise the importance of a PIM, referred to and recommended above, as an independent voice about conditions to ensure the least restrictive impact of a warrant on rights to privacy, freedom of expression and fair hearing.

50. Notification to a subject person cannot, however, lawfully occur where an agency has accessed their telecommunications data under Chapter 4 (due to secrecy provisions and the absence of a warrant process).[48] This is compounded by the broader scope for an enforcement agency to authorise a disclosure where considered 'reasonably necessary for enforcement of the criminal law', in contrast to the investigation of a serious offence or serious contravention of an Australian law for which telecommunications and stored communication warrants may be issued.

51. Some limited safeguards are provided; for example, an enforcement agency must first be satisfied on reasonable grounds that any interference with the privacy of any person that may result from the authorised disclosure of telecommunications data is justifiable and proportionate.[49] This assessment must consider the seriousness of any offence or penalty in relation to which the authorisation is sought, alongside the relevance and usefulness of the information and reason for seeking it. The Commonwealth Ombudsman is required to inspect records, including those justifying an authorisation, and report to the Minister for Home Affairs about compliance by agencies annually.[50]

52. We appreciate that easier access to telecommunications data may, as a preliminary step, inform whether the ACT Integrity Commission would choose to apply for interception or stored communications warrants. Despite this and the safeguards discussed above, the lack of independent authorisation creates a real risk of arbitrary and unreasonable interferences with the right to privacy that may only later be identified by the Commonwealth Ombudsman and that cannot be communicated to the subject person so they may seek redress. This concern was again highlighted by the PJCHR in 2016 in the context of proposed amendments to declare the NSW Law Enforcement Corruption Commission an 'interception agency' and 'criminal law-enforcement agency' under the TIA Act.[51]

53. These issues should, in our view, be examined by the Reviewer as part of recommending whether the ACT Integrity Commission should be declared an enforcement agency under the TIA Act, and whether any further safeguards in ACT legislation could appropriately mitigate such risks.

[47] Nb. Part 2-10 of the TIA Act contemplates a civil cause of action for interception of telecommunications other than in accordance with the TIA Act, including interception in accordance with a warrant.
[48] See TIA Act, s 181B.
[49] TIA Act, s 180F.
[50] TIA Act, s 186J.
[51] Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Report 9 of 2016* (Report, 22 November 2016), [1.6]-[1.24]; see also Law Enforcement Legislation Amendment (State Bodies and Other Measures) Bill 2016 (Cth).

*Further issues and considerations*

54. In addition to the preceding information, several issues are, in our view, relevant to whether the TIA Act framework is adequately circumscribed such as to reflect a proportionate limitation of the right to privacy protected in s 12 of the HR Act:

    - **Conditions about notification of subjects where appropriate:** Insofar as evidence gathered from telecommunications interceptions may be sought, intercepted and accessed without a person's knowledge or ability to seek review, equivalent safeguards must be provided at the point of authorisation and supervision.

      The extent to which a Court or AAT member may be invited to consider a condition that a person be notified is therefore relevant to the right to privacy, and may be appropriately advanced by a PIM or otherwise by ACT Integrity Commission officers who are applying for a warrant. We therefore recommend the Reviewer consider any potential scope within the existing framework or proposed amendments to encourage or enable notifications to subject people where reasonable in the circumstances so they might seek redress for any misuse of telecommunications information.

    - **Secondary use or disclosure of information:** The extent to which telecommunications information (including intercepted information, stored communications and telecommunications data) may be used and disclosed by the ACT Integrity Commission for other purposes (and by any secondary recipients) merits careful consideration.

      Offences for disclosure and secondary disclosures of stored communications data and telecommunications data contain broadly framed exceptions for situations in which the use or disclosure of information is reasonably necessary for enforcement of the criminal law, to enforce a law imposing a pecuniary penalty or to protect the public revenue.[52] Other authorisations for the purpose of the TIA Act are outlined in Part 2-6 and Part 3-4, which merit consideration. Absent a comprehensive review of these provisions, which we have been unable to undertake in the relevant timeframe to provide this submission, it is unclear whether permitted disclosures of information that may be obtained by the ACT Integrity Commission are suitably circumscribed.

    - **Use of telecommunications information in related proceedings:** Once amended, the TIA Act would provide greater scope for telecommunications information lawfully obtained by the ACT Integrity Commission to be admitted in 'exempt' proceedings,[53] which include prosecutions for specified offences (including related bail applications and appeals) and unexplained wealth proceedings (such as those under the *Confiscation of Criminal Assets Act 2002* (ACT)). A further amendment to s 5B is, in our view, required to ensure the policy intent that lawfully accessed telecommunications information can be admitted in a proceeding of the ACT Integrity Commission or the Inspector of the ACT Integrity Commission.

      Importantly, the admission of lawfully obtained telecommunications information does not offend the presumption of innocence or the privilege against self-incrimination, as reflected in ss 22 (1) and 22(2)(i) of the HR Act. Although such lawfully accessed telecommunications may tend to incriminate a subject person by virtue of coercive powers, such evidence can be appropriately

[52] TIA Act, ss 181A-182.
[53] TIA Act, s 74.

distinguished from information *compelled* by the ACT Integrity Commission under an examination summons or during an examination that is subject to use and derivative use immunity.[54]

- **Remedial relief and human rights proceedings:** We welcome, in particular, that the TIA Act expressly allows for the giving of lawfully obtained telecommunications evidence in civil proceedings for remedial relief.[55] Parts 2-10 and 3-7 of the TIA Act provide for an aggrieved person to seek remedial relief in the Federal Court of Australia or a State or Territory court for unlawful interception or communication of their telecommunications or stored communications information. These Divisions clarify that any such remedial action is not intended to limit the concurrent operation of a State or Territory law,[56] however it remains unclear whether this would enable regard to the HR Act in the ACT context (especially to the extent such courts would be exercising federal jurisdiction).

  Beyond this ambiguity, it is a relevant consideration that most telecommunications information will not be admissible in other proceedings,[57] including those under s 40C(2)(a) of the HR Act that allege a contravention of the ACT Integrity Commission's human rights obligations. This calls into question the extent to which a person may, in actual practice, be able to raise their rights under the HR Act regarding a decision of the ACT Integrity Commission to access telecommunications information under the TIA Act.

- **Security and storage of telecommunications materials:** We support the Integrity Commissioner's observation that adequate safeguards against misuse will require a dedicated IT and storage system capable of audit that should be managed independently by the ACT Integrity Commission. Secure storage against unauthorised access and misuse on a need-to-know basis is a common component for the consistency of surveillance and informational record databases with the right to privacy. Any such system must, however, be capable of access by the Commonwealth Ombudsman and ACT Ombudsman (as Inspector) for the purposes of their respective oversight functions under the TIA Act.

- **Precursor obligations on ACT Integrity Commission before applications:** Given the principles outlined above and the human rights obligations that currently apply to the decisions and acts of public authorities,[58] the ACT Integrity Commission (including the Commissioner) will arguably be obliged to properly consider the right to privacy, and whether access to telecommunications information is strictly necessary, before applying for a relevant warrant or authorising disclosure of telecommunications data.

  The Reviewer may, however, wish to consider whether there is any scope to reflect further criteria or preconditions in the proposed ACT legislation provided doing so would not present a risk of constitutional inconsistency with the TIA Act framework. Should it be considered feasible to legislate precursor obligations, further requirements could be explored to ensure the ACT Integrity Commission only authorises service providers to grant access to telecommunications data under Chapter 4 where there are no less restrictive means reasonably available to investigate the alleged corruption in the circumstances.

---

[54] *O'Halloran and Francis v United Kingdom* (European Court of Human Rights (Grand Chamber), Apps No. 15809/03 and 25624/02, 29 June 2007), [47]; *Integrity Commission Act 2018*, s 176.
[55] TIA Act, ss 76A, 107A and 165.
[56] TIA Act, ss 107E and 169.
[57] TIA Act, ss 78, 148 and.
[58] HR Act, s 40B.

- **Access to privileged information:** Access to private telecommunications under the TIA Act may involve, whether inadvertently or otherwise, access to classes of information that are inherently sensitive. For example, legally privileged information, information held by journalists concerning confidential sources and other privileged materials may be inadvertently obtained where telecommunications information is accessed by government agencies.

  It is important that any access to telecommunications under the TIA Act incorporate safeguards that consider the likelihood that information sought may divulge privileged materials. As such information may involve a further limitation of rights to freedom of expression (which includes the right to a free press), the right to fair trial (concerning one's right to equality of arms in criminal proceedings) and other human rights that may not be reasonable in the circumstances. It is important that any such risk is proactively identified and considered.

  The TIA Act expressly provides a warrant process for authorising disclosures of telecommunications data where the subject person is known or believed to be a journalist or for the purpose of identifying a known or suspected source.[59] We suggest that the Reviewer consider, in consultation with the ACT Integrity Commission, whether ACT legislation can, and should, provide any further constraints or thresholds around applications to access privileged classes of telecommunications information under the TIA Act.

55. The above principles and considerations are intended to inform the Reviewer's assessment of whether the existing framework for interception of telecommunications and access to stored communications and metadata provided by the TIA Act provides adequate and effective safeguards necessary for consistency with the right to privacy under the HR Act.

# Other proposals

## *Abrogating and determining privilege*

56. Legal professional privilege, journalist privilege, public interest immunity and privileges against self-incrimination and civil penalty each support various human rights protected in the HR Act, including foremost the right to privacy (HR Act, s 12), freedom of expression (including a free press) (HR Act, s 16) and the right to fair trial (HR Act, ss 21 and 22). A blanket waiver of legal professional privilege or journalist privilege may reflect a disproportionate limitation of these rights.

57. The ACTHRC does not in-principle oppose the ACT Integrity Commission's recommendation that the IC Act partially abrogate legal professional privilege. It is understood this amendment, if pursued, would waive legal professional privilege, including client legal privilege under the *Evidence Act 2011*, in respect of any document, advice or other material prepared for, or on behalf of, the Territory. The abrogation of legal professional privilege that belongs to the Territory, as a body politic, rather than an individual, should not in itself engage or limit human rights, like the right to privacy and the right to fair trial. Alternatively, a qualified privilege, whereby an ACT court may determine the public interest in privilege being waived against the public interest in the preservation of confidentiality in the circumstances, could be considered.

58. The Explanatory Statement which accompanied the Integrity Commission Bill 2018 stated that any claim of privilege (other than a claim concerning the abrogated privilege against self-incrimination or

[59] TIA Act, Div 4C.

parliamentary privilege) would "be determined by the Supreme Court which will undertake a balancing exercise to determine whether the privilege should be waived or not."[60] In particular, the explanatory statement indicated the legislature's view that this approach would ensure the Bill was compliant with the HR Act. On balance, we agree that judicial determination of privilege applications provides an important safeguard for relevant human rights and, in the ACT context, consistency of approach.

59. Determination of claims of privilege by the ACT judiciary supports the right to fair trial, which guarantees everyone the right to have rights and obligations decided by a competent, independent and impartial court or tribunal after a fair and public hearing (HR Act, s 21). Although the stated intent of this amendment is to limit cost and expedite proceedings, such objectives cannot alone justify the limitation of rights under the HR Act. To achieve these outcomes, amendments to allow the ACT Integrity Commission to seal only the particular documents, files or other thing over which privilege is claimed might potentially be explored in conjunction with an obligation that those claiming privilege identify and separate privileged materials that have been required under a preliminary notice requirement or other power.

## *Prior inconsistent statements*

60. Section 22(1) of the HR Act reflects the presumption of innocence of everyone charged with a criminal offence until proved guilty according to law and, in s 22(2), that a person charged with a criminal offence must not be compelled to testify against his or herself or to confess guilt.[61] While applicable only in relation to a criminal charge, IHRL jurisprudence has considered the right against self-incrimination to apply from the point a suspect is questioned by police.[62]

61. The Statement of Compatibility prepared in relation to the IC Act suggests that ACT Integrity Commission proceedings should be considered analogously insofar as it considers the abrogation of the right to self-incrimination in s 175 of the IC Act limits rights in criminal proceedings. On this basis, we understand ACT Integrity Commission proceedings to come within the legislature's understanding of a 'criminal charge' for the purposes of the HR Act.

62. We note that the ACT Integrity Commission has proposed an amendment to establish a new exception to the use and derivative use immunities in s 176 of the IC Act. We broadly understand this proposal to intend that a witness in a separate proceeding would be able to be cross-examined about a prior inconsistent statement alleged to have been made during proceedings before the ACT Integrity Commission by virtue of ss 43 and 45 of the *Evidence Act 2011*. A court in a related proceeding will, however, retain its general discretion under ss 135 and 136 of the *Evidence Act 2011* to refuse to admit such statements or limit their use should such statements be considered unfairly prejudicial to a party.

63. To the extent this amendment may limit the presumption of innocence (s 22(1) and privilege against self-incrimination (s 22(2)(i)), consistency with these rights will, in our view, turn on a witness being given advance warning that any evidence they give during an ACT Integrity Commission examination may be used in other proceedings should they make a later inconsistent statement in later proceedings.

[60] Explanatory Statement, Integrity Commission Bill 2018, 134; see also 19-20.
[61] HR Act, s 22(1) and 22(2)(i).
[62] See, for example, *John Murray v The United Kingdom* (European Court of Human Rights (Grand Chamber), App No. 18731/91, 8 February 1996), [45].

## *Witness arrest warrants*

64. We note that the ACT Integrity Commission is seeking an amendment to issue or apply for an arrest warrant for a person whose evidence is desired, necessary and relevant to an investigation under the IC Act and where:

    (a) it is probable that the person will not attend the ACT Integrity Commission to give evidence unless compelled to do so; or

    (b) the person is about to, or is preparing to, leave the Territory and their evidence will not be obtained by the Commission if the person departs.

65. The ACTHRC notes this proposal appears to have been modelled on s 64 of the *Magistrates Court Act 1930*, which provides that:

> **64 First instance warrant**
>
> (1) The court may, instead of issuing a subpoena for the attendance of a witness in a hearing, issue a warrant in the first instance for the arrest of the person if it is—
>
> (a) unlikely that the person will attend the hearing to give evidence unless the person is compelled to do so; and
>
> (b) in the interests of justice to do so.
>
> (2) In deciding whether it is in the interests of justice to issue a warrant, the court must consider the following:
>
> (a) the importance of the evidence the person is expected to give;
>
> (b) whether the evidence could be obtained by other means;
>
> (c) the nature of the matter being heard;
>
> (d) the degree of urgency to resolve the matter;
>
> (e) the likelihood that the issue of a warrant would secure the person's attendance at the hearing;
>
> (f) the impact of using a warrant for the arrest of the person.

66. In *R v Stott* [2017] ACTSC 126, Justice Penfold observed that an equivalent power was not available to the ACT Supreme Court. In doing so, however she cautioned against a broad power to 'issue a warrant to a potential witness who has not been subpoenaed or bound over to appear at trial, and who may in fact be entirely unaware of the trial' (at [40]). Her Honour also suggested that inferring a "power to authorise the arrest of a witness who may have no idea that his or her presence at a trial is required" was unlikely to be compatible with the right to liberty and security of the person in s 18 of the HR Act (at [41]).

67. In our view, the proposed amendment raises significant and similar concerns regarding its consistency with the right to liberty (HR Act, s 18), especially if exercised without judicial oversight. Given the potential for "first instance warrants" to seriously impinge on the rights of individuals, including those affected by alleged offences and conduct under investigation, we are concerned that a provision akin to s 64 would not be sufficient to achieve consistency with s 18 of the HR Act.

68. Rather than compelling attendance by way of arrest warrant, we would suggest the focus should instead be on efforts to enhance supports for witnesses. In cases where compulsion is required, it is not apparent why this could not be achieved by making more effective use of the existing summons

provisions[63] as a pre-emptive measure, based on an individual needs/risk assessment before the examination.

69. In this regard, a preferable approach, which is less rights-restrictive, may be found in the *Evidence Act 2008* (Vic). Specifically, s 194(2) of the Victorian Evidence Act provides that:

> (2) If a subpoena or summons has been issued for the attendance of a witness on the hearing of a civil or criminal proceeding and it is proved, on application by the party seeking to compel his or her attendance, that the witness—
>
> (a) is avoiding service of the subpoena or summons; or
>
> (b) has been duly served with the subpoena or summons but is unlikely to comply with it –
>
> the court may issue a warrant to apprehend the witness and bring the witness before the court.

70. The ACTHRC's previous submission to the Select Committee in 2018 welcomed that the proposed legislation required arrest warrants to be issued by an ACT court rather than the Integrity Commission itself.[64] It expressed concern, however about the lack of any provisions in the IC Act to ensure that the criteria and procedures for issuing and executing a warrant accord with the HR Act. For example, there is no time limit to a detention and no provision as to the manner of detention.

71. In our view, to ensure compliance with the HR Act, the warrant should specify that the witness should be brought before the ACT Integrity Commission immediately. We note that this view is relevant to a further proposal to amend s 160(6) of the IC Act to extend the period for which an arrested person may be detained until the next business day during normal hours of operation. We recall, in this regard, that the IC Act presently provides for a person to be released if a police officer believes on reasonable grounds that the person cannot be brought before the ACT Integrity Commission immediately.

72. Absent appropriate safeguards of this kind, we consider the exercise of these powers and related detention is likely to be characterised as an arbitrary deprivation of the right to liberty, contrary to s 18 of the HR Act.

## *Eligibility for employment of staff*

73. The ACTHRC support the ACT Integrity Commission's recommendation that prospective staff be subject to less restrictive eligibility requirements, including in relation to prior employment within the ACT Public Service.

74. In its submission to the Select Committee in 2018, the ACTHRC raised concern about prohibiting a person from being engaged or employed by the ACT Integrity Commission based on prior political party membership. Our advice observed that integrity bodies in other Australian jurisdictions do not appear to have similarly requirements concerning their employment of staff.

75. As we noted at the time, a blanket exclusion based on prior political affiliations raise significant human rights concerns, and may be incompatible with the right to equality and non-discrimination, which prohibits discrimination on a range of grounds, including political conviction. Prohibiting eligibility based on a personal attribute similarly represents a limitation of the right to have access, on general

[63] *Integrity Commission Act 2018*, s 147.
[64] ACT Human Rights Commission, Submission No 07 to Select Committee on an Independent Integrity Commission 2018, ACT Legislative Assembly, *Inquiry into the establishment of an Integrity Commission for the ACT* (31 August 2018), 2 and 4.

terms of equality, for appointment to the public service (HR Act, s 17). We therefore recommended that a time limit on the exclusion be preferred, though note the *Integrity Commission Bill 2018* as passed ultimately removed this requirement in favour of staff being required to declare relevant personal interests as identified by the ACT Integrity Commission.[65]

76. Section 50(2) of the IC Act nevertheless still prohibits the employment of those who are, or were at any time in the previous five years, an employee of the ACT Public Service. The avoidance of any real or perceived conflict of interests is a legitimate objective that may justify the limitation of human rights, including equality and non-discrimination and equal access to appointment to the public service. Where a person's previous work in the ACT Public Service can be effectively managed by conflict-of-interest procedures, as the ACT Integrity Commission has suggested,[66] this would, in our view, be a less restrictive and reasonably available alternative to the current restriction.

## *Provision of witness assistance*

77. We welcome, and supports, proposals to expand assistance for witnesses who appear during an ACT Integrity Commission examination, including provisions for appropriate on-disclosure to registered medical practitioners in connection with health and wellbeing.

78. As noted above, the Statement of Compatibility accompanying the Integrity Commission Bill 2018 (as passed) accepted that rights in criminal proceedings ought to apply in the context of an examination by the ACT Integrity Commission. Relevantly then, Section 22(2)(f) of the HR Act recognises that anyone charged with a criminal offence is entitled to have legal assistance provided to him or her, if the interests of justice require that the assistance be provided, and to have the legal assistance provided without payment if he or she cannot afford to pay for the assistance. Section 22(2)(b) also requires such persons have adequate time and facilities to prepare their defence.

79. We consider the proposed regulations to extend provide for Territory-funded legal assistance of witnesses would support these rights, as well as the right to equality and non-discrimination of witnesses who are not the subject of an examination. Regulations addressing private individuals and entities' reasonably incurred costs of legal representation, travel and accommodation and the production of documents (including advice about privilege) and things would serve to reduce barriers to participation in proceedings, consistent with equality and non-discrimination and the right to fair trial.[67]

80. Proposed amendments to allow witnesses (and ACT Integrity Commission staff) to make disclosures to registered medical practitioners and registered psychologists in consultations about their health and welfare can support the right to security of person and equality and non-discrimination (HR Act, s 8). While extending permissible disclosures may limit the right to privacy, we anticipate that tailored provisions governing how a practitioner may then use received information consistently with their professional duties can ensure this limitation is reasonable, as required by s 28 of the HR Act.

81. To the extent this proposed amendment would also apply for the benefit of staff of the ACT Integrity Commission, we also note that it would support the right to just and favourable conditions of work under s 27B of the HR Act.

[65] *Integrity Commission Act 2018*, s 50(3)(b).
[66] ACT Integrity Commission, *2021-22 Annual Report* (Report, September 2022), 90-91.
[67] See relevant discussion of witness rights to equality and fair hearing in *R v QIX (No 2)* [2021] ACTSC 244 from [110].

## APPENDIX 1: Telecommunications interception powers available to Integrity Commissions in Australian states and territories – Comparative research

### Summary

The *Telecommunications (Interception and Access) Act* 1979 (Cth) ("**TIA Act**") grants certain eligible State and Territory authorities the power to intercept certain communications. Agencies must satisfy certain preconditions to be eligible for declaration by the Home Affairs Minister as an eligible authority. As such, various States and Territories have enacted legislation providing for these safeguards.

Generally, the safeguards implemented by States & Territories in accordance with the requirements of the TIA Act include:

- The keeping of warrant documentation
- Provision of reports (including an annual report) to the responsible Minister of the State/Territory about certain matters
- Provision of reports by the Responsible Minister to the Home Affairs Minister
- Security of documents, and destruction of non-required records
- Regular inspections by an independent authority of the agency's records, and a provision of a report by the independent authority to the responsible Minister of the State or Territory. This report is to be provided to the Home Affairs Minister.

### Relevant Provisions of the TIA Act

| | |
|---|---|
| **S 34** | **Declaration of an eligible authority of a State as an agency**<br>'Subject to section 35, the Minister may, by legislative instrument and at the request of the Premier of a State, declare an eligible authority of that State to be an agency for the purposes of this Act'. |
| **S 5 (Interpretation)** | **Eligible authority**<br>An eligible authority in relation to a State, means:<br>(a) in any case – the Police Force of that State; or<br>(b) in the case of New South Wales:<br>(i) the Crime Commission;<br>(ii) the Independent Commission Against Corruption; or |

| | |
|---|---|
| | (iii) the Inspector of the Independent Commission Against corruption; or<br>(iv) the Law Enforcement Conduct Commission; or<br>(v) The Inspector of the Law Enforcement Conduct Commission; or<br>(ba) in the case of Victoria – the IBAC or the Victorian Inspectorate; or<br>(c) In the case of Queensland – the Crime and Corruption Commission; or<br>(d) In the case of Western Australia – the Corruption and Crime Commission or the Parliamentary Inspector of the Corruption and Crime Commission; or<br>(e) In the case of South Australia – the Independent Commissioner Against Corruption |
| | **State**<br>Includes all states and the Northern Territory |
| **S 34** | **Declaration of an eligible authority of a State as an agency**<br>Subject to section 35, the Minister may, by legislative instrument and at the request of the Premier of a State, declare an eligible authority of that State to be an agency for the purposes of this Act. |
| **S 35(1)(a); s 38AA** | **Preconditions for declaration** and **Agencies authorised to apply for Part 5.3 warrants** (summary)<br>(i) The chief officer of an eligible authority is required to keep certain warrant documentation;<br>(ii) The chief officer of an eligible authority must give the responsible Minister of their State written reports about certain matters;<br>(iii) The chief officer of an eligible authority must give an annual report to the responsible Minister;<br>(iv) The responsible Minister is to give the Home Affairs Minister certain reports;<br>(v) The chief officer of an eligible authority is to keep restricted records securely and ensure only authorised people have access;<br>(vi) The chief officer of an eligible authority is to destroy non-required records;<br>(vii) Regular inspections by an independent authority of the eligible authority's records are required;<br>(viii) The independent authority must report to the responsible Minister about inspections;<br>(ix) Inspections reports may include an opinion the TIA Act has been contravened; and<br>(x) The responsible Minister is to give the Home Affairs Minister a copy of an inspection report. |

## Relevant Provisions of the State and Territory Legislative Frameworks

| | |
|---|---|
| ***Victoria*** | |
| *Telecommunications (Interception) (State Provisions) Act 1988* (Vic)<br><br>The purpose of the Act is to enable the IBAC and Vic Police to intercept telecommunications under the TIA Act (s 1). | **Part 1 – Preliminary**<br>S 3: Definitions – IBAC means the Independent Broad-based Anti-corruption Commission (Vic)<br>**Part 3 – Functions of the Victorian Inspectorate**<br>Div 3 – Inspection of records of the IBAC<br>Div 4 – General functions and powers<br>**Part 2B – Functions of the IBAC**<br>S 9F: Documents connected with issue of warrants to be kept<br>S 9G: Other records to be kept in connection with interceptions<br>S 9GA: Documents to be given to Minister<br>S 9 GB: Documents to be given by State Minister to Commonwealth Minister<br>S 9 H: Keeping and destruction of restricted records<br>**Part 4 – Miscellaneous**<br>S 21: Copies of reports for Commonwealth Minister<br>S 22: Disclosure by persons under the Minister's administration |
| ***Queensland*** | |
| *Telecommunications Interception Act 2009 (Qld)*<br><br>An Act to enhance law enforcement in Queensland by enabling the Queensland Police Service and the Crime and Corruption | **Part 2 – Notification to and appearance of Public Interest Monitor ("PIM")**<br>S 7: Notification of Public Interest Monitor<br>S 8: full disclosure to PIM<br>S 12: report of PIM to Minister about noncompliance<br>**Part 3 – Record-keeping and related functions of eligible authorities** |

| | |
|---|---|
| Commission to be declared agencies under the TIA Act (long title). | S 14: Eligible authority to keep documents<br>S 15: Other warrant records to be kept in connection with interceptions<br>S 16: Documents to be given to State Minister<br>S 17: Documents to be given to Commonwealth Minister<br>S 18: Keeping of restricted records<br>S 19: Destruction of restricted records<br>S 20: Commonwealth Minister and inspecting entity to inspect restricted record before destruction<br>**Part 4 – Functions and powers of inspecting entity for inspections**<br>S 22: General functions and powers<br>S 23: Regular inspections of warrant records<br>S 24: reports to Minister<br>S 27: inspecting entity's power to obtain relevant information<br>S 28: Inspecting entity to be given information and access despite other laws<br>**Part 5 – Miscellaneous**<br>S 31: Copies of reports for Commonwealth Minister<br>**Schedule – Dictionary**<br>"eligible authority" means the CCC |
| ***New South Wales*** | |
| *Telecommunications (Interception and Access) (New South Wales) Act 1987* (NSW)<br>An Act to enable certain State authorities to be declared to be agencies for the purposes of the TIA Act (long title). | **Part 1 – Preliminary**<br>S 3: Definitions – "eligible authority" means… (c) the Independent Commission Against Corruption, (d) or the Law Enforcement Conduct Commission, or (f) the Inspector of the Independent Commission Against Corruption<br>**Part 2 – Functions of eligible authorities**<br>S 4: Eligible authority to keep documents connected with issue of warrants<br>S 5: Other records to be kept in connection with interceptions<br>S 6: Documents to be given to the Minister |

| | |
|---|---|
| | S 7: Documents to be given by the State Minister to Commonwealth Minister<br>S 8: Keeping and destruction of restricted records<br>**Part 3 – Functions of inspecting officers**<br>S 9: Functions – generally<br>S 10: Regular inspections of records<br>S 11: Reports<br>S 14: Power to obtain relevant information<br>S 15: Inspecting officer to be given information and access despite other laws<br>**Part 4 – Miscellaneous**<br>S 20: Copies of reports for Commonwealth Minister<br>S 21: disclosure by persons under the Minister's administration |
| ***Tasmania*** | |
| *Telecommunications (Interception) Tasmania Act 1999* (Tas) | N/A – The TAS Integrity Commission is not named in this Act or in the Commonwealth TIA Act. Provisions made for the Tasmanian Police Force only. |
| ***Western Australia*** | |
| *Telecommunications (Interception and Access) Western Australia Act 1996* (WA)<br><br>An Act to enable the Corruption and Crime Commission and the Police Force to be declared agencies for the purposes of the *TIA Act* of the Commonwealth and for related purposes (long title). | **Part 1 – Preliminary**<br>S 3: Terms used – "eligible authority" means the Corruption and Crime Commission (WA)<br>**Part 2 – Functions of eligible authority**<br>S 4: Eligible authority to keep warrants and related documents<br>S 5: Other records relating to interceptions to be kept<br>S 6: Documents to be given to responsible Minister<br>S 7: Responsible Minister to give certain reports to Commonwealth Minister<br>S 8: Keeping and destruction of restricted records<br>**Part 3 – Functions of principal inspector**<br>S 9: Functions, generally |

| | |
|---|---|
| | S 10: Regular inspections of eligible authority's records<br>S 11: Reports about inspections<br>S 15: Principal inspector to be given information and access despite other laws<br>**Part 4 – Miscellaneous**<br>S 21: Responsible Minister to give reports on inspections to Commonwealth Minister<br>S 22: Disclosure of information by officials restricted |
| ***South Australia*** | |
| Telecommunications (Interception) Act 2012 (SA)<br>An Act for enabling SA Police and the Independent Commission Against Corruption to be declared agencies for the purposes of the Telecommunications (Interception and Access) Act 1979 of the Commonwealth; and for other purposes (Long title) | S 2: Interpretation – "eligible authority" means (b) the Independent Commission Against Corruption (SA)<br>S 3 – Obligations of chief officer relating to records<br>S 4 – Obligations of chief officer to report to Attorney-General<br>S 5 – Obligations and powers of review agency<br>S 6 – Obligations of Attorney-General |
| ***Northern Territory*** | |
| Telecommunications (Interception) Northern Territory Act 2001 (NT)<br><br>The act was amended in 2018 (in force at 30 November 2018) to include the ICAC (NT) alongside the Police Force as an agency which can be declared for the purposes of the *TIA Act* (Long title) | ***Note: the *TIA Act* does not yet define ICIC (NT) as an eligible authority.<br><br>**Part 2 – Keeping of records of telecommunications interceptions**<br>Div 2 – Records of the ICAC<br>S 8A: Records connected with issue of warrants<br>S 8B: Other records connected with an interception<br>S 8C: Documents to be given to Minister<br>S 8D: Documents to be given to Commonwealth Minister<br>S 8E: Keeping and destruction of restricted records<br>**Part 3A Inspections of ICAC records and reports by Inspector** |

| | |
|---|---|
| | Div 1 – Inspections and reports<br>S 15: General power to inspect and report on ICAC records<br>S 16: Regular inspections if ICAC records<br>Div 2: Powers of Inspecting officers<br>S 16C: general powers for inspections in relation to the ICAC<br>**Part 4 – Miscellaneous**<br>S 17 Report to Commonwealth Minister |