Human Rights Law Centre

Safeguarding our democracy

Submission to the Senate Environment and Communications References Committee inquiry on press freedom

27 August 2019

www.hrlc.org.au

Freedom. Respect. Equality. Dignity. Action.

Contact

Emily Howie (**Legal Director**), Alice Drury (**Lawyer**) and Anna Lane (**Secondee Lawyer**)

Human Rights Law Centre Ltd
Level 17, 461 Bourke Street
Melbourne VIC 3000

T:

E:
W: www.hrlc.org.au

Human Rights Law Centre

The Human Rights Law Centre uses a strategic combination of legal action, advocacy, research, education and UN engagement to protect and promote human rights in Australia and in Australian activities overseas.

It is an independent and not-for-profit organisation and donations are tax-deductible.

Follow us at http://twitter.com/rightsagenda
Join us at www.facebook.com/HumanRightsLawCentreHRLC/

Contents

1. INTRODUCTION 2
2. PROTECTING WHISTLEBLOWERS AND THE PUBLIC'S RIGHT TO KNOW 4
   2.1 Making PIDA worthwhile for whistleblowers 4
   2.2 Disclosures of intelligence information 5
3. DECRIMINALISING JOURNALISM AND WHISTLEBLOWING 7
   3.1 Espionage offences 7
   3.2 Secrecy offences 9
   3.3 Offences relating to ASIO special intelligence operations 10
4. IMPROVING WARRANT PROCESSES FOR JOURNALISTS AND WHISTLEBLOWERS 10
   4.1 Metadata retention regime and journalist information warrants 10
   4.2 TOLA regime and deficient warrant processes 11
   4.3 Warrants to raid whistleblowers and journalists more broadly 11
5. REINING IN SURVEILLANCE OVER ALL AUSTRALIANS 12
   5.1 Pulling back the extensive metadata regime 12
   5.2 TOLA: flimsy safeguards provide inadequate protection 13
6. IMPROVING CULTURE WITHIN GOVERNMENT THROUGH A CHARTER OF RIGHTS 17

1. Introduction

1. Thank you for the opportunity to provide a submission to the Senate Environment and Communications References Committee (**Committee**) in relation to press freedom (the **inquiry**).

2. The June 2019 Australian Federal Police (**AFP**) raids on the ABC's Sydney headquarters and Annika Smethurst's home laid bare some critical tensions in our democratic systems that need urgent attention. The raids happened at a time when faith in our democratic systems is rapidly declining.

   (a) Australians' trust in Federal Government is at just 31%, having more than halved in 10 years.[1]

   (b) There is considerable concern about the use of law enforcement surveillance powers: in one survey three quarters of respondents were concerned about the extensive use of powers to access retained metadata. [2]

   (c) Following the raids, three quarters of participants in one poll were concerned about police raids on journalists.[3]

3. Law enforcement and intelligence agencies are tasked with keeping us safe and protecting our democracy. That is why we entrust them with extraordinary powers that go well beyond what ordinary citizens can lawfully do.

4. However, Australian authorities now have extensive powers to monitor citizens' communications and devices, including those of whistleblowers and journalists. When granting those new powers to law enforcement and intelligence agencies, Parliament has not imposed corresponding safeguards to ensure that these powers are not misused and do not disproportionately limit our right to privacy, freedom of expression and the maintenance of a healthy democracy.

5. At the same time, the Government is increasingly secretive, with more and more laws criminalising whistleblowing and journalism. It is necessary for the Government to keep some secrets in order to keep us safe, but broad laws that prohibit disclosure of government and

[1] G Stoker, M Evans and M Halupka, *Trust and Democracy in Australia*, Democracy 2025, Report no. 1, December 2018, 5 and 10.
[2] P Karp, "Three-quarters of Australians concerned about police raids on journalists, poll shows" *The Guardian*, 25 July 2019, available at https://www.theguardian.com/australia-news/2019/jul/25/three-quarters-of-australians-concerned-about-police-raids-on-journalists-poll-shows (accessed 21 August 2019).
[3] P Karp, "Three-quarters of Australians concerned about police raids on journalists, poll shows" *The Guardian*, 25 July 2019, available at https://www.theguardian.com/australia-news/2019/jul/25/three-quarters-of-australians-concerned-about-police-raids-on-journalists-poll-shows (accessed 21 August 2019).

intelligence information even where disclosure poses no risk to Australia's defence or security, simply create accountability black holes.

6. This inquiry provides an important occasion to address these concerns; to properly protect whistleblowers; to reform laws that criminalise journalism and to rein in and safeguard law enforcement powers to access private data and break encryption. Reforms are necessary across these areas, as they are interconnected and interdependent.

7. The starting point ought to be that the Government is as open and transparent as possible, and agencies that are entrusted with such intrusive powers should be subject to greater scrutiny, not less.

8. The Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) is currently reviewing law enforcement powers and their interaction with the media. We have made a submission to that inquiry, which is provided at Annexure 1.

9. In our view, this concurrent inquiry is important as it will review these concerns outside of the national security frame, which is appropriate given that many of the offences and powers created extend to ordinary criminal and administrative penalties. Further, we welcome this inquiry's terms of reference, which explicitly extend to reviewing whistleblower protection and the culture and leadership within the Government.

10. Our submission briefly overviews five key areas for policy and law reform:

    (a) Strengthening whistleblower protections under the *Public Interest Disclosure Act 2013* (Cth) and creating pathways for disclosing intelligence information.[4]

    (b) Decriminalising journalism and whistleblowing.[5]

    (c) Improving warrant processes for journalists and whistleblowers.[6]

    (d) Reining in surveillance over all Australians.[7]

    (e) Improving the culture within Government through a Charter of Human Rights.[8]

11. For more detailed discussion of each of the above, we refer the Committee to our submission to the PJCIS provided at Annexure 1.

[4] Relevant to terms (a), with respect to how sensitive and classified information may be disclosed publicly, and (b) regarding whistleblower protection, of the Terms of Reference for this Inquiry.
[5] Relevant to term (a) regarding disclosure of sensitive and classified information of the Terms of Reference for this Inquiry.
[6] Relevant to term (a), addressing the appropriate regime for warrants regarding journalists and media organisations and adequacy of existing legislation of the Terms of Reference for this Inquiry.
[7] Relevant to term (f) of the Terms of Reference for this Inquiry, as another matter for the Committee to consider given its remit to review communications matters.
[8] Relevant to term (d), regarding the appropriate culture, practice and leadership of Government in relation to leaks of sensitive and classified information of the Terms of Reference for this Inquiry.

2. Protecting whistleblowers and the public's right to know

2.1 Making PIDA worthwhile for whistleblowers

12. Whistleblowers are brave individuals who speak up when they see something wrong, often at great personal cost. In a democratic country, we rely on them to call out behaviour when other reporting and accountability mechanisms fail. They deserve the country's highest protection.

13. In recent years whistleblowers have exposed the false pretences on which we've gone to war,[9] police misconduct,[10] corruption,[11] the dangerously inadequate clean-up of nuclear waste,[12] and the cruel treatment of asylum seekers in immigration detention.[13]

14. However, whistleblowers are coming under increasing pressure for performing this important service. Currently, whistleblowers are being prosecuted for revealing unethical practices of the Australian Tax Office,[14] exposing Australia's alleged spying on its ally, East Timor, during oil and gas negotiations[15] and for leaking evidence of potential war crimes by Australian forces in Afghanistan.[16]

15. The *Public Interest Disclosure Act 2013* (Cth) (**PIDA**) was a welcome step towards providing safe pathways for people to disclose government information where it is in the public interest to do so. However, the complexity of the Act's disclosure provisions, combined with the threat of a prison sentence for an unprotected disclosure, make whistleblowing overly difficult.

16. In mid-2016, an independent statutory review of PIDA conducted by Philip Moss AM (**Moss Review**) noted that "the experience of whistleblowers under the PID Act is not a happy one.

[9] Brian Martin, "Bucking the System: Andrew Wilkie and the Difficult Task of the Whistleblower" (2005) 180 *Overland* 45.
[10] Yu Shu Lipski was an interpreter at Dandenong Police Station who provided insight into the fatal neglect of Mr G ong Lin Tang in custody. See Liberty Victoria, Statement, "Interpreter whistle-blower takes Voltaire Award 2014," 26 June 2014, available at https://libertyvictoria.org.au/VoltaireAward2014 (accessed 1 February 2016).
[11] See for example, Megan Palin, "AFP whistle blower's explosive claims of mass murder, rape and corruption," *News.com.au*, 23 November 2015, available at http://www.news.com.au/national/crime/afp--whistle--blowers-- explosive--claims--of--mass--murder--rape--and--corruption/news--story/0133a6b654afb765becd0b1676445f79 (accessed 1 February 2016).
[12] Alan Parkinson was the mechanical and nuclear engineer that exposed the inadequate clean--up of the British nuclear test sight at Maralinga, South Australia.
[13] Lexi Metherell, "Immigration detention psychiatrist Dr Peter Young says treatment of asylum seekers akin to torture" *ABC News*, 6 August 2014, available at https://www.abc.net.au/news/2014-08-05/psychiatrist-says-treatment-of-asylum-seekers-akin-to-torture/5650992 (accessed 1 February 2016).
[14] Richard Boyle is currently being prosecuted for 66 charges after revealing that senior ATO officers were engaged in aggressive debt collection practices to meet revenue goals: Adele Ferguson, Lesley Robinson, Lucy Carter, "Whistleblower exposes ATO "cash grab" targeting small businesses" *ABC News*, 9 April 2018, available at https://www.abc.net.au/news/2018-04-09/whistleblower-exposes-ato-cash-grab-targeting-small-businesses/9633140 (accessed 24 July 2019).
[15] Witness K and his lawyer, Bernard Collaery, are being prosecuted in the ACT for blowing the whistle: David Dixon, "Prosecution of Witness K and his lawyer is a disgraceful act of revenge" *Sydney Morning Herald*, 1 July 2018, available at https://www.smh.com.au/politics/federal/prosecution-of-witness-k-and-his-lawyer-is-a-disgraceful-act-of-revenge-20180701-p4zou5.html (accessed 24 July 2019).
[16] Michaela Whitburn, "The ex-Defence whistleblower at the centre of the ABC raids" *Sydney Morning Herald*, 5 June 2019, available at https://www.smh.com.au/national/the-ex-defence-whistleblower-at-the-centre-of-abc-raids-20190605-p51us8.html (accessed 24 July 2019).

Few individuals who had made [public interest disclosures] reported that they felt supported". The Moss Review found that the "prescriptive process" approach was undermining the legislative aim of creating a pro-disclosure culture within the Commonwealth public sector.[17] The Moss Review made a number of recommendations to simplify the procedural requirements of PIDA which have not been actioned.

17. In April 2019, Federal Court Judge John Griffiths described PIDA as "technical, obtuse and intractable", and as "largely impenetrable, not only for a lawyer, but even more so for an ordinary member of the public or a person employed in the Commonwealth bureaucracy." [18]

Recommendation 1: Simplify and expand protection of PIDA

The *Public Interest Disclosure Act 2013* (Cth) should be amended so as to:

(a) Introduce an independent whistleblowing oversight agency to advise and support whistleblowers.[19]

(b) Include provisions to actively encourage and incentivise whistleblowers to come forward with information in the public interest.[20]

(c) Provide more expedient avenues for external disclosure when there are excessive delays using internal disclosure channels.

(d) Broaden the definition of "disclosable conduct" in section 29 to include human rights abuses.

2.2 Disclosures of intelligence information

18. PIDA currently contains a blanket prohibition on public disclosure of "intelligence information". The issue of how and when intelligence information can safely be disclosed has been a subject of interest during public hearings before the PJCIS and in media reports, and as such we have provided some more detailed explanation and analysis in this overview.

19. "Intelligence information" is broadly defined by section 41 to include all information that has originated with or been received from an intelligence agency; and information that has originated with, or has been received from, the Defence Department that is about the collection, reporting, or analysis of operational intelligence.

[17] Moss, P, Review of the Public Interest Disclosure Act 2013, 15 July 2016, [94].
[18] Applicant ACD13/2019 v Stefanic [2019] FCA 548 at [17].
[19] See recommendation 12.1 of the Parliamentary Joint Committee on Corporations and Financial Services, *Whistleblower Protections*, 13 September 2017, 158, which recommends creating a Whistleblower Protection Authority to support whistleblowers in both the public and private sectors.
[20] Moss, P, Review of the Public Interest Disclosure Act 2013, 15 July 2016, [42].

20. The only disclosures outside of the relevant agency permitted by PIDA are to the Inspector-General of Intelligence and Security (**IGIS**). The IGIS performs an important oversight function for intelligence agencies, but that oversight alone does not provide the necessary level of accountability.

21. The IGIS' power of review is mainly concerned with whether the intelligence agencies' conduct was legal and proper.[21] The text, context and legislative history of the Act itself all tend to suggest that the agencies have a very broad remit in which to act "properly", including where activities would otherwise breach Australian and foreign law.[22] If an agency is acting within its functions, the IGIS will not question the policy behind it.[23]

22. This system of oversight means that whistleblowers can never lawfully disclose intelligence and security agency misconduct to a journalist, even if the disclosure of that misconduct does not harm our security.

23. Media oversight provides legitimate scrutiny of our law enforcement and intelligence agencies, and has prompted more formal investigations. The Australian Defence Force only inquired into some of the incidents raised in the Afghan Files after journalists and non-government organisations had raised concerns.[24]

24. During public hearings before the PJCIS, members of that Committee expressed concern that journalists were currently performing the function of determining what aspects of leaked intelligence information were damaging to national security, albeit typically with the advice of intelligence agencies.[25] We can appreciate this concern.

25. In our view, it is important to protect against disclosures that would harm national security, but at the same time allow enough disclosure, where appropriate, to fulfil the public's right to know to the greatest extent possible without harming national security. Whilst the policy settings may be difficult, the answer is certainly not a blanket rule of secrecy for all intelligence information, providing cover for all morally and legally dubious action to be done without any public accountability.

26. Extensive consultation and consideration is required in order to devise a process that will work best for Government agencies, whistleblowers and journalists. Below we provide a suggestion of one such process, as well as a means of confining it to apply to fewer disclosures.

[21] *Inspector-General of Intelligence and Security Act 1986* (Cth), section 8(2).
[22] The report of the Joint Special Committee on the Intelligence Services on the Intelligence Services Bill 2001 contemplates that activities may be conducted in the "proper performance" of ASIS functions even where that conduct breaches both Australian and foreign law.
[23] The Hon Margaret Stone said in oral submissions before the Parliamentary Committee on Intelligence and Security on 14 August 2019, that "If an agency is acting within its functions, as set out in relevant legislation, then I don't look at the policy behind those functions".
[24] Oakes, D, Clarke, S, "What the documents reveal about killing unarmed Afghans", *ABC News*, 11 July 2017, available at https://www.abc.net.au/news/2017-07-11/unarmed-men,-children-among-casualties-of-elite-forces/8424944 (accessed 12 July 2019). According to the article, the details of killings were publicly acknowledged by the ADF only after reporting by the media, and the outcomes of investigations were seldom made public
[25] Senator Fawcett, *Public Hearings*, Parliamentary Joint Committee on Intelligence and Security, 13 August 2019, pages 16-17.

27. An independent review mechanism could be inserted into the PIDA to manage the disclosure of intelligence information in the public interest. This might be a retired judge with an appropriate level of security clearance who is empowered to examine and, where appropriate, authorise the disclosure of intelligence information where they determine disclosure would be in the public interest. Such disclosures should only be permitted in a manner and to the extent that they would not cause undue risk to national security, on the advice of intelligence agencies. This will ensure that the public accountability necessary for good governance is protected as much as possible without causing undue risk to national security.

28. A second possible part of the solution is to raise the threshold of misconduct that is disclosable in an intelligence context, so that it must meet the threshold, for example, of corruption or human rights abuses.[26]

Recommendation 2: A regime for disclosure of intelligence information in PIDA

That the *Public Interest Disclosure Act 2013* (Cth) be amended to establish an independent review mechanism to examine whether and how "intelligence information" that reveals matters in the public interest, such as corruption or human rights abuses, can be disclosed without causing undue risk to national security.

3. Decriminalising journalism and whistleblowing

3.1 Espionage offences

29. The new espionage offences in Division 91, Part 5.2 of the *Criminal Code Act 1995* (Cth) (**Criminal Code**) go well beyond protecting Australia from threats to its defence and security. Espionage offences potentially impose life sentences for reporting legitimate criticism of the Government if it damages Australia's reputation on the world stage.

30. It is far too easy for commentators and journalists to fall foul of these espionage provisions in the course of public interest journalism. For instance, Liberal MP Andrew Hastie's op-ed for *The Age* and the *Sydney Morning Herald* outlining his concerns that China poses a threat to Australia's sovereignty potentially satisfied the elements of the section 91.2 offence.[27] The Chinese Government responded to the article by saying it had been "detrimental" to Australian-Chinese relations, and Trade Minister Simon Birmingham indicated that the article

[26] We note the Law Council's oral submissions before the Parliamentary Joint Committee on Intelligence and Security on 14 August 2019, that different thresholds could apply depending on the nature of the information, at page 66.
[27] A Drury, "Whistleblower protections hang in the balance" *The Sydney Morning Herald*, 15 August 2019, available at https://www.smh.com.au/politics/federal/whistleblower-protections-hang-in-the-balance-20190815-p52hhc.html (accessed 22 August 2019).

was not in the national interest.[28] Mr Hastie is likely protected by a defence for people acting in their capacity as a public official,[29] but others with a high public profile – such as former politicians – could face up to 20 years in prison for expressing such opinions.

31. Given the impact on public interest journalism, there is a question mark over the constitutionality of these provisions.

32. These offences require complete redrafting and would benefit from being the subject of a separate review, in particular to seek feedback on the proper definition of "national security". An appropriately high level of harm and a clearer category of harm, needs to be articulated given that the definition is essential to a number of very serious offences in the Criminal Code. We note that policies such as the Attorney-General Department's Protective Security Policy Framework[30] clearly distinguish between types and levels of harm for the purposes of classifying the security of documents. Such policies could inform a narrower, more carefully considered definition of "national security" in the legislation.

33. In the meantime, this Committee could improve the current legislation by recommending some more discrete amendments to the offences.

Recommendation 3: Reform the espionage offences

That the definition of "national security" and the espionage offences in Division 91 of the *Criminal Code Act 1995* (Cth) be subject to full review to limit their harmful impact on press freedom, whistleblowers and human rights defenders.

That in the interim the offences be immediately amended to:

(a) Include exemptions from prosecution under the espionage provisions for public interest whistleblowing. This should be complemented by amendments to strengthen the *Public Interest Disclosure Act 2013* (Cth).

(b) Include exemptions from prosecution under the espionage provisions for journalists and news outlets engaged in journalistic work in the public interest.

(c) Require that a person who engaged in the offence either caused or intended to cause, or was reckless as to causing *serious* or *grave* prejudice to Australia's national security.

[28] P Coorey, "Hastie's China spray not in the national interest: Minister" *Australian Financial Review*, 11 August 2019, available at https://www.afr.com/politics/federal/hastie-s-china-spray-not-in-the-national-interest-minister-20190811-p52g0g (accessed 22 August 2019).
[29] Section 91.4(1) *Criminal Code Act 1995* (Cth).
[30] Attorney-General's Department, *Protective Security Policy Framework: Sensitive and Classified Information*, 2018, available at https://www.protectivesecurity.gov.au/information/sensitive-classified-information/Documents/pspf-infosec-08-sensitive-classified-information.pdf (accessed 20 August 2019).

(d) That no offence should be based on whether or not a person in fact intended or was reckless as to advantaging another country.

(e) Remove any reliance on security classification as an element of the offence.

(f) Remove reference to "dealing with information" other than by communicating it.

3.2 Secrecy offences

34. The June 2019 raids were conducted in response to alleged secrecy offences under sections 70 and 79 of the *Crimes Act 1914* (Cth) (***Crimes Act***). These laws were replaced by new secrecy offences now found in Division 122 of the Criminal Code.

35. The new secrecy provisions are so complex and broad that they could prevent vital information regarding government wrongdoing from ever coming to the attention of the public. Secrecy offences should require harm to an essential public interest, and include an exemption for public interest disclosures and reporting.

Recommendation 4: Reform secrecy offences

A defence to repealed sections 70 and 79: That the *Crimes Act 1914* (Cth) or the *Criminal Code Act 1995* (Cth) be amended to ensure that any prosecutions under the now-repealed sections 70 and 79 of the *Crimes Act 1914* (Cth) require that any conduct the subject of prosecution must have caused actual harm to a public interest in order to satisfy the offence.

A harm requirement: That all the secrecy offences in new Division 122 of the *Criminal Code Act 1995* (Cth) be amended to require that the disclosure has caused harm, was likely to cause harm or was intended to cause harm, to an essential public interest.

Application to outsiders: That the secrecy offences in Division 122 of the *Criminal Code Act 1995* (Cth) be amended to only apply to Government "outsiders" if they know they are receiving information in breach of a secrecy offence and then further communicate it with the intention of (or recklessness as to) causing harm to an essential public interest.

"Dealing with" information: That the general secrecy provisions in Division 122 of the *Criminal Code Act 1995* (Cth) (such as subsection 122.1(2)) be amended to ensure that they only apply to communications and not "dealing with" information. That specific secrecy offences, insofar as they criminalise conduct other than communicating information, require that the dealing did, or was likely or intended to, damage the security or defence of the Commonwealth.

Exemption for whistleblowers, journalists and human rights defenders: That Division 122 of the *Criminal Code Act 1995* (Cth) include an exemption (rather than a defence) for whistleblowers and journalists, and be extended to human rights defenders who communicate or deal with information in the public interest. This should be complemented by amendments to strengthen the *Public Interest Disclosure Act 2013* (Cth).

3.3 Offences relating to ASIO special intelligence operations

36. Section 35P of the *Australian Security Intelligence Organisation Act 1979* (Cth) (**ASIO Act**) prohibits disclosure of information relating to an ASIO "special intelligence operation" – that is, undercover operations where ASIO agents are granted legal immunity for engaging in a range of otherwise criminal conduct.

37. This section needs to be amended to exempt public interest disclosures and journalism, and to ensure that the journalist knows that the information is related to a special intelligence operation and intended to or was reckless as to harm caused.

Recommendation 5: Amend section 35P of the ASIO Act

Knowledge requirement: Amend section 35P of the *Australian Security Intelligence Organisation Act 1979* (Cth) so that criminal liability for journalists requires that they know the information published related to a special intelligence operation and further that they knew or were reckless as to the harm that eventuated.

Whistleblower exemption: Create an exemption for whistleblowers who, in the course of making a public interest disclosure under a strengthened *Public Interest Disclosure Act 2013* (Cth), disclose information relating to a special intelligence operation. The exemption should also extend to journalists who report on such disclosures.

4. Improving warrant processes for journalists and whistleblowers

4.1 Metadata retention regime and journalist information warrants

38. The relationship of trust between journalists and their sources is the cornerstone of investigative journalism.[31] The journalist information warrant regime under the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**) is meant to protect the confidentiality of sources by prohibiting agencies from making authorisations to access journalists' or their employers' metadata for the purpose of identifying a confidential source without a warrant.[32]

39. However, the regime does not work. The process for obtaining a warrant is itself inadequate: it is conducted in secret, without the journalist or their media organisation knowing or having a chance to contest the warrant. In many cases it will be possible for a law enforcement agency to find a journalists' source by directly targeting a source, without needing to first obtain a warrant.

[31] Alliance for Journalists' Freedom, *White Paper for Press Freedom in Australia*, May 2019, 12.
[32] Section 180H *Telecommunications (Interception and Access) Act 1979* (Cth).

40. Further, to a large extent the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (**TOLA**) makes the journalist information warrant redundant. Although the TOLA purports to provide safeguards that uphold the journalist information warrant regime, deficiencies in the TOLA in fact undermine journalist information warrants. This is discussed in more detail in part 5.2 below.

Recommendation 6: Require judicial warrants for access to metadata

That the metadata retention regime in the *Telecommunications (Interception and Access) Act 1979* (Cth) prohibit law enforcement agencies from accessing the metadata of all people, including whistleblowers and journalists, without a warrant. There should be greater restrictions on accessing journalists' metadata via a warrant, perhaps even a prohibition on access with exceptions such as to allow law enforcement agencies to investigate serious crimes or prevent or mitigate an imminent threat to a person's safety.

4.2 TOLA regime and deficient warrant processes

41. The AFP raids of the ABC and Annika Smethurst's home were enabled, in part, by broad powers granted under the TOLA which was rushed through Parliament late last year.

42. The exercise of many of the intrusive powers granted by TOLA are done without a warrant. This is discussed in more detail in part 5.2 below.

4.3 Warrants to raid whistleblowers and journalists more broadly

43. We are concerned by the ease with which the police were able to obtain the raid warrants, without the journalists having an opportunity to contest them. We support the Right to Know coalition's request for the right to contest warrants seeking access to journalists' and media organisations' information.

Recommendation 7: Introduce a contested judicial warrant regime for journalists

Provide journalists and media organisations with procedural rights to contest warrants to raid their offices and homes. The exact nature of the reforms is subject to consideration, but could include:

(a) Requiring applications for warrants to be heard before a an independent authority with experience considering evidence and matters of significant public interest, at the level of a sitting or retired Supreme Court, Federal Court or High Court judge.

(b) Ensuring proper notice of the warrant is given, as well as an opportunity to be heard.

That the warrant process require evidence to establish the public interest in accessing the information, and for that to be weighed against the public interest in not granting access, including the public's right to know, the protection of sources and press freedom.

5. Reining in surveillance over all Australians

5.1 Pulling back the extensive metadata regime

44. In Australia, telecommunications and internet service providers are required to maintain the communications data of all users in Australia for two years. Back in 2015, it was accepted that access to metadata was less intrusive than access to the content of communications. It is now well understood however, including in comparative jurisprudence, that metadata allows precise conclusions to be drawn about peoples' private lives and is no less sensitive than the content of communications.[33]

45. In 2015, the metadata retention scheme was justified by the Government on the basis that it was central to the investigation of *serious crimes* such as murder, serious sexual assaults, organised crime, terrorism and threats to national security.[34] Furthermore, the TIA Bill was meant to better protect the right to privacy by reducing the number of agencies that could access telecommunications data to only those that "have a clear and scrutinised need for access… and are subject to appropriate privacy and oversight arrangements".[35] This would include a select few "traditional" law enforcement agencies, such as the police and Customs.

46. The reality is that as many as 80 agencies, such as the oversight body for taxi services, are contributing to the 350,000 requests for access to metadata made each year.[36] Media reports indicate that local councils have accessed metadata to pursue unpaid fines and enforce minor infringements, including for littering.[37]

47. Australia's metadata regime is general and facilitates indiscriminate data collection of the kind that the European Court of Justice has found to be a far-reaching and serious infringement on the rights to privacy and freedom of expression, and likely to cause people to feel their private lives are the subject of constant surveillance.[38]

Recommendation 8: Introduce safeguards into the metadata regime

The metadata retention regime in the *Telecommunications Interception and Access Act 1979* (Cth) should either be repealed or, if retained, be amended to:

[33] *Tele2 Sverige AB v Post-och telestyrelsen; Secretary of State for the Home Department v Watson and others* (C-203/15) and (C-698/15), [2016] ECR, at [99]. See also Human Right Council, 23rd Session, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 17 April 2013, A/HRC/23/40, [42].
[34] Turnbull, M, Hansard, House of Representatives, *Second Reading Speech*, 30 October 2014, 12560.
[35] Replacement Explanatory Memorandum, *Telecommunications (Interception and Access) Act 1979* (Cth), at [96].
[36] Stanton, J, Communications Alliance, testimony before the Parliamentary Joint Committee on Intelligence and Security, review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Cth), Canberra, 19 October 2018.
[37] Alexander, Harriet, "Councils pry into residents' metadata to chase down fines" *Sydney Morning Herald*, 15 November 2015, accessed 25 June 2019, available at https://www.smh.com.au/business/consumer-affairs/councils-pry-into-residents-metadata-to-chase-down-fines-20181114-p50fxr.html (accessed 12 August 2019).
[38] *Tele2 Sverige AB v Post-och telestyrelsen; Secretary of State for the Home Department v Watson and others* (C-203/15) and (C-698/15), [2016] ECR, at [100].

(a) Require warrants to access all data.

(b) Limit the broad range of data that is required to be held and the period of time for which it is held.

(c) Limit the number of agencies that can access data.

(d) Raise the threshold in terms of seriousness of offences in relation to which metadata can be accessed.

(e) Require notice to be provided to persons whose metadata is accessed.

5.2 TOLA: flimsy safeguards provide inadequate protection

48. The TOLA sets up a system of notices by which law enforcement and security agencies can request and require designated communications providers to assist in investigations. The extremely broad powers given to agencies under the TOLA include breaking encryption. In light of these extraordinary powers, the TOLA does not contain the kinds of safeguards and oversight mechanisms that would ensure that the powers are not misused.

49. There are three key areas of the TOLA that inhibit press freedom.

50. Firstly, there are flimsy safeguards to protect against the powers that can be exercised under the TOLA:

(a) **Unclear definitions of systemic weakness, systemic vulnerability and target technology:** The TOLA purports to prevent designated communications providers from being required to build systemic weaknesses into their systems of electronic protection. However, the definitions in the TOLA are unclear and do not prohibit agencies from targeting specific devices, for example by inserting an eavesdropping capability into a journalist's Google Home device or breaking past the security passcode on a journalist's smart phone. This compromises the ability of journalists to protect the confidentiality of their sources.

(b) **No independent authorisation of notices**: Agencies who wish to use powers under the TOLA can themselves issue or vary notices requiring compulsory action from communications providers. There is no oversight of this process by a judge, meaning that the broad and intrusive powers granted under the TOLA can be exercised without any independent review.

(c) **Low threshold for engaging powers:** The threshold at which agencies may engage the TOLA powers is far too low. The powers can be used to investigate serious offences, defined to mean crimes that carry a penalty of at least three years

imprisonment. This captures relatively innocuous offences such as making a prank call (which attracts a maximum three year sentence under division 474.17 of the *Criminal Code Act 1995*). The three year threshold is out of step with the TIA Act which already defines "serious offence" as an offence punishable by imprisonment for life or for a period, or a maximum period, of at least **seven years**. The meaning of a serious offence should not differ between Acts.

(d) **Warrant powers can be exercised after the warrant expires:** Warrant powers under the TOLA can be exercised during the warrant or at the earliest reasonably practicable time after the warrant has expired.[39] This presents a risk that privacy-intrusive activities may continue even after a warrant has expired. There need to be strict time limits within which law enforcement and interception agencies can exercise powers granted under a warrant.

51. The second area that we would like to raise is the **reporting requirements** under the TOLA**.** The TOLA only requires reporting on the number of notices issued and, where relevant, the kinds of serious offences to which they relate. Additionally, the Home Affairs Minister is empowered to delete information from the Commonwealth Ombudsman's reports to Parliament about the operation of encryption legislation.

52. The reporting requirements under the TOLA should require reporting of detailed, disaggregated data from all agencies that have the power to issue notices and requests.

53. The third, and possibly most alarming, factor of the TOLA is the underlying warrant regime. The Act purports to insert a safeguard by prohibiting agencies from using technical assistance requests, technical assistance notices or technical capability notices to require providers to do things that would otherwise require a warrant. For example, where a journalist information warrant would be required to look at a journalist's metadata.

54. However, the TOLA requires designated communications providers to comply with notices that would assist in, or facilitate, giving effect to a warrant or authorisation under a law of the Commonwealth, a State or Territory that may be granted for a vastly different purpose.

55. The way this works in practice is unclear and overly complex but we think that despite the attempted safeguards it could nonetheless allow warrantless access to information that would otherwise require a warrant, such as a journalist's metadata.

56. Further, the operation of this provision puts the communications worker who is handed the technical assistance request, technical assistance notice or technical capability notice at a deep disadvantage – they cannot be expected to know if the powers are being applied correctly.

[39] Explanatory Memorandum, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Cth), 99 [512].

57. Finally, the things that can be requested under technical assistance requests, technical assistance notices or technical capability notices are so intrusive that they themselves should require a warrant.

58. The weak safeguards, reporting requirements and underlying warrant regime in the TOLA require reform in order to prevent further damage to press freedom.

Recommendation 9: Delete the definition of systemic weakness

Delete the definitions of systemic weakness, systemic vulnerability and target technology from the *Telecommunications Act* 1997 (Cth) and, instead, more clearly and narrowly articulate the prohibited effects of a request or notice in section 317ZG.[40] The burden should be shifted to the issuing agency to show that a technical assistance request, technical assistance notice or technical capability notice does not require the designated communications providers to implement or build a systemic weakness, where a designated communications provider has raised it as an issue.[41]

Recommendation 10: Require judicial oversight for notices

Amend Part 15 of the *Telecommunications Act 1997* (Cth) to:[42]

(a) Require that a warrant be obtained from a judge in order to issue a notice;

(b) Require judicial consent before varying a notice;

(c) Remove the ability for agencies to circumvent warrants required in other regimes, i.e. that require designated communications providers to do acts or things that would ordinarily require a warrant where the act or thing would assist in, or facilitate, giving effect to a separate warrant.

(d) Ensure that a judge cannot approve the giving or variation of a notice unless the judge is satisfied that**:**

(i) the relevant designated communications provider can comply with the notice; and

(ii) the notice can be validly given under the *Telecommunications Act 1997* (Cth);

(iii) nothing in the *Telecommunications Act 1997* (Cth) prevents the notice from having effect; and

(iv) the designated communications provider has been consulted and given a reasonable opportunity to make submissions on whether the requirements to

[40] Communications Alliance, Submission No 3 to Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018,* 22 January 2019, 4.
[41] An amendment that would bring these changes to the TOLA was tabled by Labor and passed the Senate on 6 December 2018.
[42] This recommendation is modelled on the ALP amendments which passed the Senate on 6 December 2018.

be imposed by the notice are reasonable and proportionate and whether the compliance with the notice is practicable and technically feasible.

Recommendation 11: Increase the threshold of criminality under TOLA

The definitions of "serious Australian offence" and "serious foreign offence" in section 317B of the *Telecommunications Act 1997* (Cth) should be amended as follows:

(a) ***Serious Australian offence*** means an offence against a law of the Commonwealth, a State or a Territory that is punishable by a maximum term of imprisonment of **seven years** or more or for life.

(b) ***Serious foreign offence*** means an offence against a law in force in a foreign country that is punishable by a maximum term of imprisonment of **seven years** or more or for life. This is limited to where there is an equivalent crime in Australia.

Recommendation 12: Introduce safeguards for computer access warrants

The following safeguards should be implemented into the *Australian Security Intelligence Organisation Act 1979* and the *Surveillance Devices Act 2004* to counteract the impact of Government hacking:

(a) The issuing authority (meaning the eligible Judge or Administrative Appeals Tribunal member) must only authorise a computer access warrant if:

(i) they have considered the human rights (as set out in the *International Covenant on Civil and Political Rights* and other international human rights treaties) of any people, including third parties, subject to the warrant; and

(ii) they are satisfied that there are no alternative, less intrusive methods that could be used to access the data.

(b) The issuing authority must only authorise a computer access warrant permitting access to a third party computer if:

(i) they are satisfied that access is **necessary** in all the circumstances, having regard to other methods of obtaining access to the data which are likely to be as effective; and

(ii) they have considered the human rights of the third party and are satisfied that the limits on their human rights are proportionate.

(c) ASIO or a law enforcement agency seeking to exercise "concealment of access" powers under a warrant **after 28 days** from the date of the warrant's expiry must return to an eligible Judge or nominated Administrative Appeals Tribunal member for further authorisation.

(d) Repeal the penalty provisions under subsection 201A(3) and (4) of the *Customs Act 1901* (Cth) and revert them to the previous penalty provision of maximum two years imprisonment or 120 penalty units.

Recommendation 13: Improve reporting requirements under TOLA

The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) should be amended to:

(a) Require the Home Affairs Minister to report more detailed statistical and other information about technical assistance requests, technical assistance notices or technical capability notices under section 317ZS.

(b) Require reporting by all agencies that issue notices and requests, not just interception agencies.

(c) Introduce annual reporting requirements on the part of the Attorney-General in respect of powers exercised under schedules 1 and 2 of the TOLA as they relate to the *Telecommunications (Interception and Access) Act 1979* (Cth).

(d) Require that all reports be made public.

6. Improving culture within Government through a Charter of Rights

59. On several metrics, Australia is regressing when it comes to government openness and accountability.

60. On Transparency International's Corruption Perception Index, Australia has slipped eight points in six years, and while we remain ranked 13th overall, Australia was singled out with four other countries as having made a "troubling" decline.[43]

61. Journalists are reporting that the number of refusals of freedom of information requests is the highest on record, as well as long delays and unnecessary obfuscation.[44] A freedom of information officer from within the Department of Prime Minister and Cabinet has come forward to describe a "culture of disdain for the rule of law" and claimed that there was a "politically-motivated, pervasive and toxic" disregard for freedom of information law.[45]

[43] Transparency International, *Corruption Perceptions Index 2018*, available at https://www.transparency.org/cpi2018.
[44] C Knaus, J Bassano, "How a flawed freedom-of-information regime keeps Australians in the dark" *The Guardian*, 2 January 2019, available at https://www.theguardian.com/australia-news/2019/jan/02/how-a-flawed-freedom-of-information-regime-keeps-australians-in-the-dark (accessed 12 August 2019).
[45] C Knaus, "Whistleblower hits out at PM's department over 'pervasive and toxic' disregard for law" *The Guardian*, 26 June 2019, available at https://www.theguardian.com/australia-news/2019/jun/26/whistleblower-hits-out-at-pms-department-over-pervasive-and-toxic-disregard-for-law (accessed 20 August 2019).

62. There is also a pattern of investigation and prosecution of whistleblowers, which has culminated in a number of alarming prosecutions against people we should probably be rewarding.[46] Evidence before the PJCIS in its inquiry on media raids set out how whistleblowers are increasingly reluctant to come forward as a result of the secrecy and espionage offences that could see them serving prison sentences if they get the complex public interest disclosure process wrong, and journalists are concerned about extended police powers to find journalists' sources.[47]

63. The Federal Government is also taking significant steps toward undermining Australians' right to privacy, including passing world-first anti-encryption legislation[48] and a metadata retention regime that goes well-beyond, for instance, the UK and Europe.[49] These drastic steps have been permitted in Australia where they would be impossible in comparative jurisdictions because we do not have comprehensive statutory or constitutional protection of human rights. In fact, we are the only liberal democracy without it.

64. We know from experience in Victoria and the ACT (and will know, in time, with Queensland) that Human Rights Charters promote a human rights culture across Government departments and agencies, because they are required by law to take human rights into account when making decisions or providing advice and services. It follows, that such Charters strengthen "the democratic process by providing feedback to government and ensures there are checks on legal developments and decision-making".[50]

65. Similarly at a Federal level, protecting human rights in law through a national Charter of Human Rights and Responsibilities will help maintain the health of our democracy and ensure that when governments or corporations overstep and infringe our human rights, anyone can enforce their fundamental human rights and freedoms.

66. Most relevant to this inquiry, a Federal Charter of Human Rights and Responsibilities would require laws that infringe on free speech and press freedom to be carefully weighed against the interests of national security, and for any limitations on rights to be necessary, reasonable and proportionate. It would also require the Department of Home Affairs, AFP and intelligence agencies to apply a similar analysis when enforcing legislation.

[46] For instance, the recent whistleblowers Richard Boyle, Witness K, Bernard Collaery and David McBride.
[47] R Ananian-Welsh, R Cronin, K Gelber, P Greste, R Murray, Submission 17, *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press*, Parliamentary Joint Committee on Intelligence and Security, 26 July 2019, 3.
[48] A Bogle, J Gothe-Snape, "No more WhatsApp? How the proposed encrypted message access laws will affect you" *ABC News*, 5 December 2018, available at https://www.abc.net.au/news/2018-12-04/encryption-whatsapp-signal-messages-explained/10580208 (accessed 12 August 2019).
[49] *Tele2 Sverige AB v Post-och telestyrelsen; Secretary of State for the Home Department v Watson and others* (C-203/15) and (C-698/15), [2016] ECR.
[50] Victorian Equal Opportunity and Human Rights Commission, *Growing a Human Rights Culture*, November 2017, 8, available at https://www.parliament.vic.gov.au/file_uploads/Victorian_Equal_Opportunity_and_Human_Rights_Commission_2016_Charter_Report_7C12GsXb.PDF (accessed 12 August 2019)

Recommendation 14: Introduce a Federal Charter of Human Rights and Responsibilities

The Parliament should legislate a Federal Charter of Human Rights and Responsibilities that protects all the rights contained in the Universal Declaration of Human Rights.