Annexure 1

Protecting press freedom to ensure transparency and government accountability

Submission to the Parliamentary Joint Committee on Intelligence and Security inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press

26 July 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

Human Rights Law Centre

7. Executive Summary

Thank you for the opportunity to provide a submission to the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) in relation to its inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press (the **inquiry**).

The June 2019 raids on media outlets exposed in small part the extent to which Australian authorities now have the power to monitor journalists' communication and devices, access and alter the data of media outlets and dissuade people from revealing information to journalists in the public interest. In the last decade or so, parliament has granted more and more powers of surveillance without also implementing corresponding safeguards to ensure freedom of the press. New laws have increasingly criminalised speech and journalism, and the existing whistleblower protection laws are inadequate to ensure the protection of journalists' sources. Finally, the June 2019 raids highlighted the woefully inadequate warrant system for those cases where law enforcement are seeking access to journalist information.

The inquiry provides an important opportunity to review the exercise of law enforcement and intelligence powers and their impact on freedom of the press. It provides an occasion to address the deep community concerns about raids on journalists and the extent to which law enforcement access private data and break encryption.[51]

Such an inquiry necessarily includes the protection of whistleblowers, the brave individuals who come forward, often at great personal cost, to provide the much-needed transparency and accountability for wrongdoing. In recent years whistleblowers have exposed the false pretences on which we've gone to war,[52] police misconduct,[53] corruption,[54] dangerously inadequate clean-up of nuclear waste,[55] and the cruel treatment of asylum seekers in immigration detention.[56]

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

[51] Paul Karp - https://www.theguardian.com/australia-news/2019/jul/25/three-quarters-of-australians-concerned-about-police-raids-on-journalists-poll-shows

[52] Brian Martin, "Bucking the System: Andrew Wilkie and the Difficult Task of the Whistleblower" (2005) 180 *Overland* 45.

[53] 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 L berty Victoria, Statement, "Interpreter whistle-blower takes Voltaire Award 2014," 26 June 2014, available at https://libertyvictoria.org.au/VoltaireAward2014 (accessed 1 February 2016).

[54] 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).

[55] Alan Parkinson was the mechanical and nuclear engineer that exposed the inadequate clean--up of the British nuclear test sight at Maralinga, South Australia.

[56] 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).

Office,[57] exposing Australia's spying on its ally, East Timor, during oil and gas negotiations[58] and for leaking evidence of potential war crimes by Australian forces in Afghanistan.[59]

Without safe pathways for whistleblowers to disclose information outside of government, journalists are not able to do their jobs, and wrongdoing goes unreported and unaddressed. It is therefore imperative that this inquiry also consider the impact that the criminalisation of whistleblowing is having on journalists.

Our submission covers policies and reforms that fall into five broad categories:

(a) Digital surveillance capabilities;

(b) Laws that criminalise journalism and speech;

(c) Ensuring protection of journalists' sources;

(d) Ensuring the rule of law in granting warrants to journalist information; and

(e) Protecting our rights comprehensively in a Charter of Human Rights.

7.1 Digital Surveillance Powers

Metadata retention regime

In 2015, the metadata retention regime was expected to be used sparingly, for the investigation of serious crimes by a limited number of agencies. Today, as many as 80 agencies, including the oversight body for taxi services, are contributing to the 350,000 requests for access to metadata made each year.[60] Secrecy offences are among the crimes being investigated by police, and journalists' information is being accessed frequently, and at times without a valid warrant.[61] The journalist information warrant regime is a flimsy safeguard for protecting the confidentiality of sources.

[57] 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).

[58] 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).

[59] 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).

[60] 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.

[61] Paul Karp and Josh Taylor, "Police made illegal metadata seaches and obtained invalid warrants targeting journalists", The Guardian, 23 July 2019, https://www.theguardian.com/australia-news/2019/jul/23/police-made-illegal-metadata-searches-and-obtained-invalid-warrants-targeting-journalists?CMP=Share_iOSApp_Other.

Human Rights Law Centre

Recommendation 1

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

- Require warrants to access all data;
- Limit the broad range of data that is required to be held and the period of time for which it is held;
- Limit the number of agencies that can access data;
- Raise the threshold in terms of seriousness of offences in relation to which metadata can be accessed; and
- Require notice to be provided to persons whose metadata is accessed.

That the metadata retention regime in the *Telecommunications Interception and Access Act 1979* (Cth) be amended to prohibit law enforcement agencies from accessing the metadata of whistleblowers, journalists, human rights defenders and activists who, in the legitimate course of their work, disclose government wrongdoing in the public interest. A limited exception to this prohibition could allow law enforcement agencies to access their metadata, with a warrant, if necessary to prevent or mitigate an imminent threat to a person's safety.

TOLA

The *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (Cth) (**TOLA**) was introduced in late 2018 with the stated purpose of helping government agencies to "better deal with the challenges posed by ubiquitous encryption".[62] However, it has created extraordinary powers for law enforcement, unparalleled in comparable democracies, to pursue secret, backdoor, often warrantless access into encrypted communications and devices. The Act does not contain the necessary safeguards to protect journalists and whistleblowers who rely on encryption to ensure the confidentiality of sources. There is also inadequate transparency of the process to protect against abuse.

Recommendation 2

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.[63] The burden should be shifted to the issuing agency to show that a Technical Assistance Request, Technical Assistance Notice or Technical Capability

[62] Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 2.

[63] 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 January2019, 4.

Notice does not require the designated communications provider (**DCP**) to implement or build a systemic weakness, where a DCP has raised it as an issue.[64]

Recommendation 3

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

- ***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.
- ***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 4

Amend Part 15 of the *Telecommunications Act 1997* (Cth) to:[65]

- Require judicial consent before issuing or varying a notice;
- Ensure that a judge cannot approve the giving or variation of a notice unless the judge is satisfied that:
  - the relevant DCP can comply with the notice; and
  - the notice can be validly given under the *Telecommunications Act 1997* (Cth);
  - nothing in the *Telecommunications Act 1997* (Cth) prevents the notice from having effect; and
  - the DCP has been consulted and given a reasonable opportunity to make submissions on whether the requirements to be imposed by the notice are reasonable and proportionate and whether the compliance with the notice is practicable and technically feasible.

Recommendation 5

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:

- The issuing authority (meaning the eligible Judge or AAT member) must only authorise a computer access warrant if:
  - 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
  - they are satisfied that there are no alternative, less intrusive methods that could be used to access the data.
- The issuing authority must only authorise a computer access warrant permitting access to a third party computer if:
  - 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

[64] An amendment that would bring these changes to the TOLA was tabled by Labor and passed the Senate on 6 December 2018.
[65] This recommendation is modelled on the ALP amendments which passed the Senate on 6 December 2018.

    - they have considered the human rights of the third party and are satisfied that the limits on their human rights are proportionate.
- 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 AAT member for further authorisation.
- 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.

Improve transparency and reporting requirements

It is critical that the extraordinary powers given to law enforcement and intelligence agencies under TOLA be accompanied by equally stringent scrutiny and oversight of the exercise of those powers. The metrics currently required to be reported do not provide enough useful information on whether the requests and notices were issued appropriately. Reports produced under the TOLA should contain more detailed, disaggregated data that includes as much information as possible about the types of acts or things done by providers in compliance with a request or notice.[66] Additionally, the Home Affairs Minister should not be empowered to delete information from the Commonwealth Ombudsman's reports to parliament about the operation of encryption legislation.[67]

Recommendation 6

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

- 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.
- Require reporting by all agencies that issue notices and requests, not just interception agencies.
- Introduce annual reporting requirements on the part of the Attorney-General in respect of powers exercised under schedules 1 and 2 of the Act as they relate to the *Telecommunications (Interception and Access) Act 1979* (Cth).
- Require that all reports be made public.

[66] Australian Human Rights Commission, Submission No 47 to Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018,* 12 October 2018, 56.

[67] *Telecommunications and Other Legislation (Assistance and Access) Act 2018,* s 317ZRB(7).

Human Rights Law Centre

7.2 Laws that criminalise journalism and speech

Secrecy offences

The June 2019 raids were conducted in response to alleged 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 Act 1995* (Cth) (***Criminal Code***).

Both sets of laws imposed criminal liability on people for conduct that was not sufficiently serious, and could even be in the public interest. Secrecy offences should require harm to an essential public interest, and include an exemption for public interest disclosures and reporting.

Recommendation 7

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 act the subject of prosecution must have caused actual harm to a public interest in order to satisfy the offence.

Recommendation 8

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.

Recommendation 9

That the secrecy offences in Division 122 of the *Criminal Code Act 1995* (Cth) only apply to government "outsiders" who 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 an essential public interest.

Recommendation 10

That the general secrecy provisions in Division 122 of the *Criminal Code Act 1995* (Cth) (such as section 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, should require that the dealing did, or was likely or intended to, damage the security or defence of the Commonwealth.

Recommendation 11

That Division 122 of the *Criminal Code Act 1995* (Cth) include an exemption for whistleblowers, journalists and human rights defenders who communicate or deal with information in the public interest. This should be complemented by amendments to the *Public Interest Disclosure Act 2013* (Cth), set out in part 5 below.

Human Rights Law Centre

Espionage

The new espionage offences in Division 91, Part 5.2 of the *Criminal Code* need to be completely redrafted. Currently, instead of protecting Australians from grave threats to our security, the laws are so broad they criminalise public interest reporting and legitimate criticism. It would be extraordinarily easy for a news outlet to fall foul of these espionage provisions during the course of working on public interest journalism and there is a question mark over their constitutionality for that reason.

Recommendation 12

That 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:

- Include exemptions from prosecution under the espionage provisions for public interest whistleblowing. This should be complemented by amendments to the *Public Interest Disclosure Act 2013* (Cth) (**PIDA**), set out in part 5 below.
- Include exemptions from prosecution under the espionage provisions for journalists and news outlets engaged in journalistic work.
- 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.
- That no offence should be based on whether or not a person in fact intended or was reckless as to advantaging another country.
- Remove any reliance on security classification as an element in the offence.

Section 35P

Secrecy laws were also expanded in the area of national security by section 35P of the *Australian Security Intelligence Organisation Act 1979* (Cth) (**ASIO Act**), which prohibits disclosure of information relating to an ASIO "special intelligence operation" – operations where ASIO agents are granted legal immunity for engaging in a range of otherwise criminal conduct. The penalties for disclosure range from between 5 and 10 years in prison.

The HRLC remains concerned that section 35P continues to criminalise whistleblowing from within ASIO and reporting in the public interest on wrongdoing by ASIO, even where it poses no risk to ASIO's operational interests.

Recommendation 13

Create an exemption from prosecution under s 35P of the *Australian Security Intelligence Organisation Act 1979* (Cth) for journalists and whistleblowers who make disclosures in the course of public interest reporting.

Human Rights Law Centre

7.3 Protecting journalists' sources and the public's right to know

The Public Interest *Disclosure Act 2013* (Cth) (**PIDA**) was introduced to provide safe pathways for people with government information where it is in the public interest to do so.

While the Act was a step in the right direction to ensuring whistleblower protection, it still creates high barriers to people making a disclosure – especially given the potentially harsh criminal consequences, including jail, if the person gets it wrong. The complexity of the Act's disclosure provisions, combined with the threat of a jail term for an unprotected disclosure, make whistleblowing overly difficult and have a chilling effect on journalists' sources.

Recommendation 14

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

- include provisions to actively encourage and incentivise whistleblowers to come forward with information in the public interest;
- provide more expedient avenues for external disclosure when there are excessive delays using internal disclosure channels;
- broaden the definition of "disclosable conduct" in section 29 to include human rights abuses; and
- include serious violations of human rights in the "emergency disclosures" provisions, where the other relevant criteria for emergency disclosures are met.

Recommendation 15

That the *Public Interest Disclosure Act 2013* (Cth) be amended to establish an independent review mechanism to examine whether "intelligence information" can be disclosed that reveals corruption, misconduct or human rights abuses inside government. Such disclosure should only be allowed where they would not cause undue risk to national security.

7.4 Warrant processes

We support the Right to Know coalition's request for the right to contest warrants seeking access to journalists and media organisations' information.

Recommendation 16

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:

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

- 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.

7.5 Charter of Human Rights

Australia is the only democracy without comprehensive statutory or constitutional protection of human rights. A national Charter of Human Rights and Responsibilities would help to maintain the health of our democracy by requiring 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.

Recommendation 17

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

Human Rights Law Centre

8. Digital surveillance capabilities

8.1 Metadata retention scheme

67. The reality of today's metadata retention regime bears little resemblance to the context in which this Committee reviewed the scheme during its introduction in 2015.

68. In 2015, the regime was expected to be used sparingly, for the investigation of serious crimes by a limited number of agencies. Today, 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.[68] Media reports indicate that local councils have accessed metadata to pursue unpaid fines and enforce minor infringements, including for littering.[69]

69. Secondly, 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, including in comparative jurisprudence, that metadata allows precise conclusions to be drawn about peoples' private lives and is no less sensitive than content of communications.[70]

70. Finally, in 2015, the journalist information warrant regime in the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**) was expected to protect freedom of the press and the confidentiality of journalists' sources. That regime has failed to protect either. It is now abundantly clear that metadata retention laws undermine the ability of journalists to protect their sources.

(a) Journalist information warrants are inadequate

71. The relationship of trust between the journalists and their sources is the cornerstone of investigative journalism.[71] The journalist information warrant regime is meant to protect the confidentiality of sources by prohibiting agencies from making authorisations to access journalists' or their employers' data for the purpose of identifying a confidential source unless a journalist information warrant is in force.[72]

72. However, the warrant 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

[68] 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.

[69] 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>.

[70] *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].

[71] Alliance for Journalists' Freedom, *White Paper for Press Freedom in Australia*, May 2019, 12.

[72] Section 180H *Telecommunications (Interception and Access) Act 1979* (Cth).

or, crucially, having a chance to respond. Instead, any public interest arguments against the granting of the warrant are put by a government-appointed public interest advocate.[73]

73. In practice, journalists' information is being accessed frequently, and at times without a warrant.

(a) In just one year, the AFP accessed the metadata of journalists nearly 60 times using the journalist information warrant.[74]

(b) The AFP unlawfully accessed a journalist's metadata without a warrant in order to identify their source.[75] This admission by the AFP prompted an inquiry by the Commonwealth Ombudsman, who concluded that "a number of officers did not appear to fully appreciate their responsibilities when exercising metadata powers".[76]

(c) Revelations this week show that WA police obtained invalid warrants targeting journalists.[77]

74. Further, journalists will never know if their metadata has been accessed and their source compromised, and if they find out, there is a two year term of imprisonment for publishing the fact of the warrant.

(b) Law enforcement can bypass journalist information warrants

75. The journalist information warrants are also ineffective at protecting sources for two reasons. First, in many cases it will be possible for a law enforcement agency to find a journalists' source without needing a warrant. They will simply access the suspected whistleblower's metadata (ie by accessing the data of the government department suspected of leaking), rather than accessing the metadata of the journalist they are suspected of speaking to.

76. Secondly, the journalist information warrant process was made largely redundant by the TOLA (discussed in more detail in part 2.2 below). The TOLA requires "designated communications providers" to facilitate access to a person's encrypted messaging applications, device or computer when issued with a notice from an Australian law enforcement agency. Section 317ZH(1) seems to preserve the journalist information warrant provided in the TIA Act, however it is unclear how such a warrant, which governs metadata, applies in the context of a TOLA notice, which may grant access to the entire device of a journalist.

---

[73] Section 180X *Telecommunications (Interception and Access) Act 1979 (Cth)*.

[74] Bevan Shields, "Federal Police accessed the metadata of journalists nearly 60 times," The Age, 9 July 2019, https://www.theage.com.au/politics/federal/federal-police-accessed-the-metadata-of-journalists-nearly-60-times-20190708-p52598.html.

[75] https://www.abc.net.au/news/2017-04-28/afp-officer-accessed-journalists-call-records-in-metadata-breach/8480804

[76] Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's inspection of the Australian Federal Police under the Telecommunications (Interception and Access) Act 1979*, October 2017, 1.

[77] Paul Karp and Josh Taylor, "Police made illegal metadata seaches and obtained invalid warrants targeting journalists", The Guardian, 23 July 2019, https://www.theguardian.com/australia-news/2019/jul/23/police-made-illegal-metadata-searches-and-obtained-invalid-warrants-targeting-journalists?CMP=Share_iOSApp_Other.

77. Further, sections 317ZH(4) and (5) then negate and undermine the journalist information warrant. Those sections suggest that any act or thing can nonetheless be requested under TOLA if it would "assist in, or facilitate, giving effect to a warrant or authorisation under a law of the Commonwealth, a State or a Territory". So it would seem that a request for technical information (including a journalists' metadata) under TOLA can be made so long as it would assist in, or facilitate the giving of effect to a warrant or authorisation otherwise provided, for example other warrants and authorisations that might be made under the TIA Act or the *Telecommunications Act 1997* .

78. For this reason, we recommend that the TIA Act be amended to create an exclusion whereby the metadata of whistleblowers, journalists, human rights defenders and activists who, in the legitimate course of their work, disclose government wrongdoing in the public interest, cannot have their metadata accessed. An exception to this could allow law enforcement agencies to access their metadata, with a warrant, if necessary to prevent or mitigate an immediate threat to a person's safety.

Recommendation 1

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

- Require warrants to access all data;
- Limit the broad range of data that is required to be held and the period of time for which it is held;
- Limit the number of agencies that can access data;
- Raise the threshold in terms of seriousness of offences in relation to which metadata can be accessed; and
- Require notice to be provided to persons whose metadata is accessed.

That the metadata retention regime in the *Telecommunications Interception and Access Act 1979* (Cth) prohibit law enforcement agencies from accessing the metadata of whistleblowers, journalists, human rights defenders and activists who, in the legitimate course of their work, disclose government wrongdoing in the public interest. A limited exception to this prohibition could allow law enforcement agencies to access their metadata, with a warrant, if necessary to prevent or mitigate an imminent threat to a person's safety.

Human Rights Law Centre

8.2 *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (Cth)

79. The TOLA was introduced in late 2018 with the stated purpose of helping government agencies to "better deal with the challenges posed by ubiquitous encryption".[78] It introduced a framework whereby particular government agencies can compel industry assistance to access encrypted communications. Through various new request, notice and warrant powers, government agencies can gain access to devices to obtain, and in some circumstances add, copy, delete or alter, the metadata and content of communications without the target ever knowing. TOLA was intended to target serious crimes such as human trafficking, terrorism and child abuse. However, in the short time since the Act was passed, these powers have also been used to target journalists reporting in the public interest.[79]

80. In our view the TOLA needs wholesale repeal. Parliament should reconsider how meet its legislative aims without creating a scheme for secret, backdoor, often warrantless access into encrypted communications and devices. To assist in this Committee's immediate inquiry, however, this submission sets out five amendments that would significantly improve the most egregious aspects in the TOLA regime and better protect press freedom. It suggests:

- deleting the current definitions of systemic weakness, systemic vulnerability and target technology and defining what is prohibited under a notice or request more clearly;
- narrowing the scope of TOLA by lifting the low threshold at which the powers under the TOLA are engaged;
- require a warrant for all access notices under TOLA;
- restraining the broad powers in relation to computer access warrants – and the disproportionality of penalties; and
- expanding the reporting requirements in the TOLA.

(a) Delete the definitions of systemic weakness, systemic vulnerability and target technology

81. The type of assistance that law enforcement agencies can request or require is limited under section 317ZG of the *Telecommunications Act 1997* (Cth). Section 317ZG purports to prevent designated communications providers (**DCPs**) from being required to build a form of systemic vulnerability or systemic weakness into their systems of electronic protection. Systemic vulnerability and systemic weakness are defined as follows:

[78] Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 2.

[79] Josh Taylor, 'Australia's anti-encryption laws used to bypass journalist protections, expert says', *The Guardian* (8 July 2019) <https://www.theguardian.com/australia-news/2019/jul/08/australias-anti-encryption-laws-being-used-to-bypass-journalist-protections-expert-says>

> ***Systemic vulnerability*** *means a vulnerability that affects a whole class of technology, but does not include a vulnerability that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.*
>
> ***Systemic weakness*** *means a weakness that affects a whole class of technology, but does not include a weakness that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.*

82. The definitions are difficult to understand and far too narrow. It is unclear at what point a weakness or vulnerability becomes systemic. It is also unclear what the difference between a weakness and a vulnerability is.

83. The approach that appears to have been taken is that a systemic weakness is a weakness pertaining to the whole system. This narrow definition gives government agencies the power to request or require a very broad range of potentially exploitable weaknesses to be built into software and devices.

84. Concerning from a press freedoms perspective, the reference to a "class of technology" does not prevent agencies from targeting a specific service or device. It is not a defined term in the TOLA. An example of the way in which this power could be abused is if the AFP Commissioner issued a notice to require a DCP to insert an eavesdropping capability into a journalist's Google Home device or break past the security passcode on a journalist's smart phone. This would not enliven the requirement to obtain a journalist information warrant under the TIA Act and has the potential to undermine this framework.

85. The term "systemic" does not prevent the government from undermining specific encrypted systems. This sort of tailored or targeted weakness could have far-reaching negative impacts on journalists and whistleblowers, who rely on encrypted communications to protect their confidentiality.[80]

86. Data breaches and cyber insecurity are of specific concern to journalists who are duty bound to protect the confidentiality of their sources. The uncertainty around the kind of weaknesses that can be created in various technologies may have a detrimental impact on the ability of journalists to protect their sources or on the willingness of sources to come forward, therefore having a chilling effect on public interest reporting.

Recommendation 2

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

[80] Communications Alliance, Submission No 43 Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018,* 12 October 2018, 16.

effects of a request or notice in section 317ZG.[81] 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 provider (**DCP**) to implement or build a systemic weakness, where a DCP has raised it as an issue.[82]

(b) Increase the threshold at which powers under TOLA are engaged

87. The threshold at which law enforcement may engage the powers conferred by TOLA – investigating a crime that carries a penalty of at least three years or in relation to safeguarding national security -- is far too low. This captures relatively innocuous offences such as making a prank call (which attracts a maximum three year sentence under the *Criminal Code Act 1995*).[83] Further, "national security" is not defined in TOLA, leaving scope for significant discretion as to what may constitute "safeguarding national security".

88. The three year threshold is included in the definition of "serious Australian offence" and "serious foreign offence" in the Act. This is out of step with the TIA Act which already defines "serious offence" in section 5D to mean 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. The TIA Act sets an appropriate threshold that should be adopted in TOLA.

Recommendation 3

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

- ***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.
- ***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.

(c) Need for judicial oversight

89. Agencies who wish to use powers under TOLA can themselves issue or vary notices requiring compulsory action from communications providers. There is no oversight of this process by a judge – the broad and intrusive powers granted under the TOLA can be exercised without any

[81] 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 January2019, 4.
[82] An amendment that would bring these changes to the TOLA was tabled by Labor and passed the Senate on 6 December 2018.
[83] See div 474.17 – Using a carriage service to menace, harass or cause offence: https://www.legislation.gov.au/Details/C2019C00152/Html/Volume_2#_Toc7424596

independent review. There is no effective transparency and accountability for decision-making and access.[84]

90. Judicial consent should be a compulsory barrier to issuing a notice under TOLA, given the extreme breadth of the powers being granted, the intrusion into peoples' most private information and the secrecy of the process that means the person affected will not be able to advocate for their own interests. This sort of independent review mechanism will help to prevent the kind of overreach and abuse that has been seen in relation to the metadata retention regime under TIA Act generally (see paragraph 9 above).

Recommendation 4

Amend Part 15 of the *Telecommunications Act 1997* (Cth) to:[85]

- Require judicial consent before issuing or varying a notice;
- Ensure that a judge cannot approve the giving or variation of a notice unless the judge is satisfied that:
  - the relevant designated communications provider (**DCP**) can comply with the notice; and
  - the notice can be validly given under the *Telecommunications Act 1997* (Cth);
  - nothing in the *Telecommunications Act 1997* (Cth) prevents the notice from having effect; and
  - the DCP has been consulted and given a reasonable opportunity to make submissions on whether the requirements to be imposed by the notice are reasonable and proportionate and whether the compliance with the notice is practicable and technically feasible.

(d) Broad warrant powers and disproportionate penalties

91. A computer access warrant enables officers to search electronic devices covertly and remotely and access content on those devices – essentially permitting government agencies to develop and grow their own hacking capacities. Government hacking has been acknowledged as one of the most invasive government surveillance activities in the modern world.[86] It substantially interferes with human rights, particularly the right to privacy and freedom of expression.

92. The broad powers granted under Schedule 2 permit government agencies to access protected information, both stored or in transit, even while it is being created. It also permits access to the computers of innocent third parties who are not the subject of the warrant. These powers can be exercised during the warrant or at the earliest reasonably practicable time after the

[84] Australian Human Rights Commission, Submission No 47 to Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018,* 12 October 2018, 54 [286].

[85] This recommendation is modelled on the ALP amendments which passed the Senate on 6 December 2018.

[86] Access Now, Submission No 33 to Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018,* 12 October 2018, 13.

warrant has expired.[87] This presents a risk that privacy-intrusive activities may even continue after a warrant has expired.

93. Further, TOLA permits ASIO and law enforcement agencies to seek assistance orders which compel assistance from a target or a person who could assist with gaining access to the target's computer. TOLA implements harsh penalties on the subject of an assistance order for failure to comply with warrants and orders made under these extended powers. For example, the maximum sentence for failing to comply with an assistance order is 10 years imprisonment,[88] which may be significantly longer than the offence which is being investigated. The maximum sentence for failing to comply with a warrant or order should not be longer than the maximum sentence for the offence being investigated.[89]

Recommendation 5

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:

- The issuing authority (meaning the eligible Judge or AAT member) must only authorise a computer access warrant if:
  - 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
  - they are satisfied that there are no alternative, less intrusive methods that could be used to access the data.
- The issuing authority must only authorise a computer access warrant permitting access to a third party computer if:
  - 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
  - they have considered the human rights of the third party and are satisfied that the limits on their human rights are proportionate.
- 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 AAT member for further authorisation.

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.

(e) Improve transparency and reporting requirements

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

[88] *Customs Act 1901* (Cth), sub-ss 201A(3)-(4).

[89] Australian Human Rights Commission, Submission No 47 to Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018,* 12 October 2018, 77, 93.

94. The Home Affairs Minister is required to report on the number of requests or notices issued and, where relevant, the kinds of serious offences to which they relate. These metrics do not provide enough useful information on whether the requests and notices were issued appropriately.

95. It is critical that the extraordinary powers given to law enforcement and intelligence agencies under TOLA, powers that are unparalleled in comparative democracies, are accompanied by equally stringent scrutiny and oversight of the exercise of those powers.

96. Reports produced under TOLA, including reports from the Home Affairs Minister and from the Commonwealth Ombudsman, should contain more detailed, disaggregated data that includes as much information as possible about the types of acts or things done by providers in compliance with a request or notice.[90] Information such as whether notices are active or expired, how many have been varied and whether any are subject to legal challenge would increase transparency without impacting operational requirements. These metrics, as well as data on how many requests have been "escalated" to notices and what the reasons were that a DCP gave for not voluntarily providing the assistance under a request, will allow better scrutiny of the practical application of the legislation.[91]

97. The reporting requirements under section 317ZS of TOLA only apply in relation to interception agencies. Therefore, if a request or a notice has been given by ASIO, ASD or ASIS, the Home Affairs Minister does not have to report on it.

98. Additionally, the Home Affairs Minister is empowered to delete information from the Commonwealth Ombudsman's reports to parliament about the operation of encryption legislation.[92] The Commonwealth Ombudsman made a submission to the current PJCIS inquiry into the TOLA that these powers are "inconsistent with the ombudsman's role as an independent and impartial office."[93]

Recommendation 6

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

- 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.

[90] Australian Human Rights Commission, Submission No 47 to Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018,* 12 October 2018, 56.

[91] Communications Alliance sub to the Bill review, page 19 rec 2.12.

[92] *Telecommunications and Other Legislation (Assistance and Access) Act 2018,* s 317ZRB(7).

[93] Paul Karp, 'New encryption powers used at least five times by federal and NSW police', *The Guardian* https://www.theguardian.com/technology/2019/jul/10/new-encryption-powers-used-at-least-five-times-by-federal-and-nsw-police?CMP=Share_iOSApp_Other (accessed 10 July 2019).

- Require reporting by all agencies that issue notices and requests, not just interception agencies.
- Introduce annual reporting requirements on the part of the Attorney-General in respect of powers exercised under schedules 1 and 2 of the Act as they relate to the *Telecommunications (Interception and Access) Act 1979* (Cth).
- Require that all reports be made public.

Human Rights Law Centre

9. Laws that criminalise journalism and speech

99. There is a maze of laws in Australia that require secrecy of government information and criminalise some acts of journalism and limit free speech.[94] However, in recognising that this review was initiated in response to the June 2019 raids on the ABC headquarters and Annika Smethurst, we have focussed only on the repealed sections 70 and 79 of the *Crimes Act 1914* (Cth) (***Crimes Act***) that provided the basis for the warrants, and the secrecy offences introduced last year into the *Criminal Code Act 1995* (Cth) (***Criminal Code***) to replace them. We will also address the new espionage offences, which further criminalised public interest reporting, and the need for reform of section 35P of the ASIO Act.

100. We recognise that a functioning government relies on select information remaining confidential. The release of certain information known to government officials may jeopardise essential public interests and the privacy of individuals who provide personal information to the government. Criminal offences have a role to play for disclosures where serious harm is caused or is intended to be caused by the person disclosing the information.

101. Unfortunately the laws discussed go too far, criminalising too-broad a range of conduct, including the work of whistleblowers and journalists in pursuit of the public interest. Without robust safeguards, these laws pose a significant risk to open government and our democratic rights.

9.1 Secrecy provisions

(a) Prior secrecy provisions: sections 70 and 79 of the Crimes Act

102. According to the AFP's media release, both of the June raids related to publishing classified material in contravention of the secrecy offences in Part 6 and 7 of the *Crimes Act*.[95] The relevant secrecy offences in those parts were, prior to their repeal, sections 70 and 79.

103. Section 70 of the *Crimes Act* was a "general secrecy offence": that is, a secrecy offence that applied to all Commonwealth officers, regardless of the agency they worked for or information they handled. Specifically, it provided that it was an offence, punishable by up to two years' imprisonment, for a Commonwealth officer to disclose (i.e. publish or communicate) information "which it is his or her duty not to disclose".

104. Section 79 of the *Crimes Act* was also a general offence and prohibited the use or disclosure of official secrets. Unlike section 70, section 79 applied to "any persons" – that is, it captured not only Commonwealth officers, but journalists also. The penalties for the offences ranged

[94] In 2010, the Australian Law Reform Commission reported it had identified 506 secrecy offences in 176 pieces of legislation and subordinate legislation, 70% of which created criminal offences: Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, ALRC 112, (2010), 22.

[95] Australian Federal Police, "AFP statement on activity in Canberra and Sydney", 5 June 2019, available at https://www.afp.gov.au/news-media/media-releases/afp-statement-activity-canberra-and-sydney (accessed on 12 June 2019).

between six months and seven years. Section 79 operated as both a general and a specific secrecy provision, depending on the kind of information disclosed. Under subsections 79(1)(a) and (c) it prohibited dealing with disclosure of specific categories of defence and security information. However, section 79 also governs a more general category of information which has been entrusted to the person by a Commonwealth officer. Section 79(1)(b) is similar to that in s 70, insofar as it relies on a "duty to treat [the information] as secret".

105. Neither sections 70 nor 79 contained an exception or defence for persons who disclose information "in the public interest".[96]

106. In 2009-2010, the Australian Law Reform Commission (**ALRC**) conducted a comprehensive review into all secrecy offences and developed a consistent approach to safeguarding Commonwealth information.[97] In its report, the ALRC recommended that both sections 70 and 79 be repealed and replaced with laws that adhere to the following principles:[98]

- general secrecy offences should only criminalise the disclosure of information where it causes, is reasonably likely to cause or is intended to cause actual harm to an essential public interest, such as protecting national security and law enforcement; and
- specific secrecy provisions should likewise include an element of harm to an essential public interest, except where the offence covers a narrowly defined category of information and the harm to an essential public interest is implicit.

107. Given that the secrecy offences in the Crimes Act remain operable for investigations of leaks that occurred prior to the repeal of the provisions, we urge the Committee to recommend that safeguards be introduced to ensure the protection of press freedom in those circumstances. Those safeguards should reflect the ALRC's recommendations for reform of the provisions, in particular amendments to ensure that offences should only criminalise the disclosure of information where it causes, is reasonably likely to cause or is intended to cause *actual harm*.

Recommendation 7

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 act the subject of prosecution must have caused actual harm to a public interest in order to satisfy the offence.

(b) The new secrecy offences should apply only to disclosures that cause harm to an essential public interest

[96] Section 79(3)(b) contained an exception that permitted a person to communicate information "in the interests of the Commonwealth", however the meaning and scope of this exception is unclear: Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, ALRC 112, (2010) at [3.133].

[97] Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, ALRC 112, (2010).

[98] Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, ALRC 112, (2010), recommendations 4, 5 and 8.

Human Rights Law Centre

108. In 2018, sections 70 and 79 of the Crimes Act were repealed and replaced with new secrecy offences in Division 122 of the *Criminal Code*. Unfortunately, these new offences did not fully incorporate the ALRC's recommendations, and accordingly continue to pose a significant threat to press freedom in Australia.

109. First, the secrecy offences in Division 122 of the *Criminal Code* still criminalise the disclosure of information without always requiring that disclosures cause harm to an essential public interest, such as the security or defence of Australia. For example, section 122.4 substantially replicates section 70 of the *Crimes Act*, and should be amended to include harm to an essential public interest as an element of the offence.

110. Similarly, Division 122 also creates offences for Commonwealth officers who communicate or deal with "inherently harmful information", in which the harm is assumed based on the source or subject matter of information. Inherently harmful information includes security classified information, information obtained or generated by a domestic or foreign intelligence agency, and information relating to the operations of a domestic or foreign law enforcement agency.[99]

111. Whilst disclosures of these types of information may be sufficient to warrant disciplinary or employment-based sanctions on those who engage in unauthorised disclosure, it does not warrant criminal sanction. Our position is that Criminal sanctions are only necessary where harm to an essential public interests results or is intended, and that harm in disclosure should not be inferred from the type of documents, such as security information.

112. Future criminal liability should not be triggered by administrative classifications that are not governed by law, yet form an element of a criminal offence.[100] This is a basic rule of law issue. With respect to security classified information, the ALRC warned that the assignment of security classification is not always an accurate indicator of the harm that could be caused by the unauthorised disclosure of the information.[101] This is because documents are often over-classified, or not re-classified as their national security sensitivity reduces over time.[102] Thus, public servants could be put in prison for up to seven years for disclosing information marked "secret",[103] even though no harm could possibly come from the disclosure.

[99] Section 121.1 of the *Criminal Code Act 1995* (Cth).

[100] See s. 90.5 of the *Criminal Code Act 1995* (Cth) for the definition of "security classification". We note, with concern, that the definition could be extended to broad categories of documents by regulation.

[101] Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, ALRC 112, (2010), [8.61].

[102] Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, ALRC 112, (2010), [8.51], citing Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004).

[103] See s. 90.5 of the *Criminal Code Act 1995* (Cth) for the definition of "security classification".

Human Rights Law Centre

Recommendation 8

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.

(c) "Outsiders" must have knowledge of their breach of secrecy offences

113. Section 122.4A is an offence that applies to disclosure by non-Commonwealth officers, including journalists. It is harm-based, with the exception of the disclosure of security-classified documents. However, it is not in keeping with the ALRC's recommendation that criminal liability should only be imposed on non-Commonwealth officers who 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 an essential public interest.

Recommendation 9

That the secrecy offences in Division 122 of the *Criminal Code Act 1995* (Cth) only apply to government "outsiders" who 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 an essential public interest.

(d) Conduct other than disclosure

114. Finally, some of the secrecy offences in Division 122 still apply to conduct other than disclosure of information, such as dealing with information. The ALRC recommended that general secrecy offence provisions should only apply to disclosure, not other dealings with information, as it is normally only disclosure that can harm essential public interests.[104]

115. Specific secrecy offences, insofar as they criminalise conduct other than communicating information, should require that the dealing did, or was likely to or was intended to, harm the security or defence of the Commonwealth,[105] consistent with the ALRC's recommendation.

Recommendation 10

That the general secrecy provisions in Division 122 of the *Criminal Code Act 1995* (Cth) (such as section 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.

---

[104] Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, ALRC 112, (2010), [9.56].
[105] Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, ALRC 112, (2010), at [9.56].

Human Rights Law Centre

(e) Exemptions for journalists, news outlets and whistleblowers

116. It is vital that journalists are provided protection from criminal liability. There is a defence that covers journalists engaged in the business of reporting news (section 122.5(6)), however operating as a defence, it still allows a journalist to be charged and places the burden on journalists to prove the defence, and bear the cost and stress of court proceedings. The June 2019 media raids showed how damaging the mere conduct of raids can be in terms of creating a broader chilling effect.

117. Instead of defences, there should be exemptions to secrecy offences for journalists.

118. Similarly, whistleblowers should be exempted from secrecy offences where they provide information in accordance with PIDA. Section 122.5(4) of the Criminal Code addresses whistleblowers insofar as it provides a defence for persons who have communicated or dealt with information in accordance with PIDA. However, this defence is incomplete and inadequate because of underlying weaknesses with PIDA. Further, for reasons similar to those for journalists, an exemption is more appropriate than a defence.

119. We note that there is a gap in defences for any person who discloses abuses in other scenarios, such as reporting of human rights abuses to international watchdogs and to not-for-profits organisations.

Recommendation 11

That Division 122 of the *Criminal Code Act 1995* (Cth) include exemption for whistleblowers, journalists and human rights defenders who communicate or deal with information in the public interest. This should be complemented by amendments to the *Public Interest Disclosure Act 2013* (Cth), set out in part 5 below.

9.2 Espionage

(a) Reform the espionage provisions in the Criminal Code

120. The 2018 espionage offences introduced in Division 91, Part 5.2 of the Criminal Code need to be completely redrafted. Currently, instead of protecting Australians from grave threats to the security and defence of Australia, the laws are so broad they criminalise public interest reporting and legitimate criticism.

121. There are a number of new espionage offences. The first is an offence with maximum sentences of between 25 years (recklessness) and life (intentional) for people who:[106]

- deal with information that has a security classification or concerns "national security";
- have an intention or are reckless as to whether the conduct will prejudice Australia's national security or advantage that of another country; and

[106] Section 91.1 *Criminal Code Act 1995* (Cth).

- where the conduct results (or will result) in it being made available to a foreign principal.

122. This may sound straightforward, but the devil is in the definitions. "National security" is defined so broadly as to include Australia's political and economic relations with another country.[107] To cause "prejudice" to Australia's national security is to cause something more than "mere embarrassment".[108]

123. More dangerous still, is section 91.2. This section sets out an offence, punishable by up to 25 years in prison for:

- dealing with *any information* (not just classified information or intelligence information);
- with the intent to prejudice or being reckless as to prejudicing Australia's national security;
- where it results (or will result) in the information being made available to a foreign principal.

124. The Attorney-General's Department has confirmed that the information covered by this section includes privately, professionally or commercially produced research, opinions, advice or analysis: it "applies to any information and does not require it to be security classified or concern national security".[109] Further, information may be "made available" to a foreign principal by publishing it on the internet as a news item.[110]

125. It would be extraordinarily easy for a news outlet to fall foul of these espionage provisions during the course of working on public interest journalism. For instance, were it to happen now, the ABC and Guardian journalists who reported on the Australian Signals Directorate's interception of Indonesian President Susilo Bambang Yudhoyono's phone calls, could face lengthy prison sentences.

126. There is a question mark over the constitutionality of the espionage provisions on the basis that they impermissibly burden the implied freedom of political communication. Nonetheless, while these offences remain on the books, they will suppress important journalism and human rights reporting.

127. These offences require complete redrafting and would benefit from being the subject of separate review, in particular to seek feedback on the proper definition of "national security".

---

[107] Section 90.4(1)(e) *Criminal Code Act 1995* (Cth).

[108] Section 82.1 *Criminal Code Act 1995* (Cth). The prejudice to Australia's national security is not required to be serious or substantial but is intended to be more than a minor or trivial prejudice that has no long-lasting effect, nor embarrassment to an Australian person or Australia's people: Replacement Explanatory Memorandum at [317]. The Attorney-General's Department advised that "prejudice" extends to the government's reputation or relationships with a foreign government, or between officials": Attorney-General's Department, Submission 6.1, p 45.

[109] Attorney-General's Department, Parliamentary Joint Committee on Intelligence and Security inquiry into *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* Submission 6.1, 68.

[110] Attorney-General's Department, Parliamentary Joint Committee on Intelligence and Security inquiry into *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* Submission 6.1, 34.

However this Committee could significantly reduce the most harmful impact of the provisions by making some small amendments to the definitions.

Recommendation 12

That 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:

- Include exemptions from prosecution under the espionage provisions for public interest whistleblowing. This should be complemented by amendments to the *Public Interest Disclosure Act 2013* (Cth) (**PIDA**), set out in part 5 below.
- Include exemptions from prosecution under the espionage provisions for journalists and news outlets engaged in journalistic work.
- 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.
- That no offence should be based on whether or not a person in fact intended or was reckless as to advantaging another country.
- Remove any reliance on security classification as an element in the offence.

9.3 Reforming offences relating to ASIO special intelligence operations

128. Secrecy laws were also expanded in the area of national security by section 35P of the ASIO Act. That section prohibits disclosure of information relating to an ASIO "special intelligence operation" – that is, operations where ASIO agents are granted legal immunity for engaging in a range of otherwise criminal conduct. The penalties for disclosure range from between five and 10 years in prison. This section needs to be repealed, or at the very least amended to exempt disclosures made in good faith in the public interest.

129. The new laws were strongly opposed by many groups including all the major news organisations.[111] While the Government claimed that the section 35P secrecy provision was necessary to protect national security, the Parliamentary Joint Committee on Human Rights concluded it was not a reasonable, necessary and proportionate limitation on the right to freedom of expression and would potentially stifle public reporting and scrutiny of ASIO's activities.[112]

[111] See the submissions to the Parliamentary Joint Committee on Intelligence and Security's inquiry, September 2014, available at http://www.aph.gov.au/Parliamentary_Business/ Committees/Joint/Intelligence_and_Security/ National_Security_Amendment_Bill_2014/ Report1 (accessed 1 February 2016).

[112] Parliamentary Joint Committee on Human Rights, *16th Report of the 44th Parliament,* October 2014, 56-57.

130. In 2015 the Independent National Security Legislation Monitor, Roger Gyles AO QC, sounded the alarm that section 35P could fall foul of the implied freedom of political communication because of its impact on journalists.[113] He noted the impact was twofold:

> "1. It creates uncertainty as to what may be published about the activities of ASIO without fear of prosecution. The so-called chilling effect of that uncertainty is exacerbated because it also applies in relation to disclosures made to editors for the purpose of discussion before publication.
>
> 2. Journalists are prohibited from publishing anywhere at any time any information relating to an SIO, regardless of whether it has any, or any continuing, operational significance and even if it discloses reprehensible conduct by ASIO insiders."

131. Gyles' recommendation to distinguish between "insiders" – ASIO employees; and "outsiders" – primarily journalists, was implemented through amending legislation in November 2016.[114] However, the HRLC remains concerned that section 35P continues to criminalise whistleblowing from within ASIO and reporting in the public interest on possible wrongdoing by ASIO, even where it poses no risk to ASIO's operational interests. This provision should be subject to an exemption for disclosures made in compliance with PIDA, as amended below.

Recommendation 13

Create an exemption from prosecution under s 35P of the *Australian Security Intelligence Organisation Act 1979* (Cth) for journalists and whistleblowers who make disclosures in the course of public interest reporting.

[113] Gyles, R, *Report on the impact on journalists of section 35P of the ASIO Act*, Independent National Security Legislation Monitor, 21 October 2015, 2.

[114] *Counter-Terrorism Legislation Amendment Act (№1) 2016.*

Human Rights Law Centre

10. Reforming the *Public Interest Disclosure Act 2013* (Cth)

132. PIDA was introduced to provide safe pathways for people to disclose government information where it is in the public interest to do so.

133. While the Act was a step in the right direction to ensuring whistleblower protection, the complexity of the Act's disclosure provisions combined with the threat of a jail term if they get it wrong, still has a chilling effect on journalists' sources.

134. The Act creates significant disincentives to individuals that wish to make urgent disclosures in the public interest but who are unsure whether the emergency disclosure provisions apply. Emergency disclosure provisions only apply to disclosures that relate to "substantial and imminent danger to the health or safety of one or more persons or to the environment". It is for the individual to assess whether their disclosure falls within those provisions.

135. Individuals are otherwise required to use internal disclosure provisions, and that process may take months to play out before a disclosure can be made publicly. The Act seems to allow a Minister, the Speaker of the House of Representatives or the President of the Senate to effectively prevent external or public disclosures being made under the protection of the Act. A would-be whistleblower is deprived of the protection of the Act where any of these office-holders is "taking action" in response to an internal disclosure.

The process for blowing the whistle should be simplified

136. PIDA should be simplified to allow for disclosure of information in the public interest. This is important for press freedom, open government and fundamentally for keeping government accountable in a healthy democracy. In mid-2016, an independent statutory review of PIDA conducted by Philip Moss AM (**Moss Review**) noted that the "prescriptive process" approach was undermining the legislative aim of creating a pro-disclosure culture within the Commonwealth public sector.[115] He made a number of recommendations to simplify the procedural requirements of PIDA which have not been actioned. Echoing similar views in a decision of April this year, Federal Court Judge John Griffiths described PIDA as "technical, obtuse and intractable".[116]

Recommendation 14

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

- Include provisions to actively encourage and incentivise whistleblowers to come forward with information in the public interest;

[115] Moss, P, *Review of the Public Interest Disclosure Act 2013*, 15 July 2016, [94].

[116] *Applicant ACD13/2019 v Stefanic* [2019] FCA 548 at [17].

- Provide more expedient avenues for external disclosure when there are excessive delays using internal disclosure channels;
- Broaden the definition of "disclosable conduct" in section 29 to include human rights abuses; and
- Include serious violations of human rights in the "emergency disclosures" provisions, where the other relevant criteria for emergency disclosures are met.

Ensure grave misconduct, including human rights abuses, within intelligence and defence agencies can be made public

137. PIDA currently contains a blanket prohibition on public disclosure of intelligence information. "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.

138. The only disclosures outside of the relevant agency permitted by PIDA are to the Inspector-General of Intelligence and Security (**IGIS**), in the case of intelligence matters, or the Inspector-General of the Australian Defence Force (**IGADF**).

139. The existing reporting avenues to the IGIS and IGADF are insufficient to ensure misconduct, corruption and human rights abuses are publicly reported. For instance, in the ABC's Afghan Files, journalists Dan Oakes and Sam Clark reported that a number of inquiries into the killings of unarmed Afghan civilians or unarmed insurgents by the Australian Defence Force (**ADF**) had only been inquired into because journalists or NGO's raised concerns.[117] The details of killings were publicly acknowledged by the ADF, but only after reporting by the media and the outcomes of investigations were reportedly seldom made public. [118]

140. Instances of corruption and human rights abuses can undoubtedly be reported on without compromising Australia's national security. For instance, details such as the identity of persons involved, their exact location and the precise time at which conduct occurred can be removed.

141. It is vital that an independent review mechanism – such as a retired judge – be empowered to examine and where appropriate authorise the disclosure of "intelligence information" where such information reveals that Australian government employees have been involved in corruption, misconduct or human rights abuses. This will ensure that the public accountability necessary for good governance is protected as much as possible without causing undue risk to national security.

[117] 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.

[118] 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.

Human Rights Law Centre

Recommendation 15

That the *Public* Interest *Disclosure Act 2013* (Cth) be amended to establish an independent review mechanism to examine whether "intelligence information" can be disclosed that reveals corruption, misconduct or human rights abuses inside government. Such disclosure should only be allowed where they would not cause undue risk to national security.

Human Rights Law Centre

11. Ensure rule of law in granting warrants

Proper processes for issuing search warrants on the media

142. The June 2019 raids revealed how easily police can obtain a warrant to do something as potentially damaging to democracy as raiding a news outlet or journalist's home. In both cases, police acted on the basis of warrants that were obtained *ex parte*. We support the Right to Know coalition's request for the right to contest warrants seeking access to journalists and media organisations' information.

Recommendation 16

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:

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

Human Rights Law Centre

12. Charter of Human Rights

143. Australia is the only democracy without comprehensive statutory or constitutional protection of human rights. Australia has agreed to be bound by the major international human rights treaties, but individuals cannot enforce these protections directly under Australian law.

144. 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, any human being can enforce their fundamental human rights and freedoms.

145. In this space, it 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.

Recommendation 17

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