August 2, 2019
Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

Submission by Human Rights Watch to the Australian Parliamentary Joint Committee on Intelligence and Security on the Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press

Summary

Human Rights Watch welcomes the invitation to make a submission regarding the Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press.

Problematic national security provisions that have a chilling effect on reporting in the public interest include the revised espionage offences and section 35P of the Australian Security Intelligence Organisation Act 1979 (ASIO Act). The expansive powers afforded to law enforcement under the metadata and encryption reforms, and the lack of protections for those disclosing information in the public interest reinforce this chilling effect. In an annex, we provide a list of several examples of problematic law enforcement responses on matters in the public interest.

The impact of the exercise of law enforcement and intelligence powers on the freedom of the press has been highly publicized surrounding the June 2019 media raids on journalists working for the Australian Broadcasting Corporation (ABC) and News Corp. But journalists and traditional media outlets are not the only ones who are impacted by Australia's overly broad national security legislation. Human rights activists, lawyers, whistleblowers and those who witness or speak out about government misconduct are also affected.

Authoritarian governments around the world use broadly drafted national security laws to silence human rights defenders, journalists, bloggers, and critics of the government. Australia should not join them by having overly broad laws on the books that are open to misuse. Australia needs safeguards to protect disclosures made in the public interest. Officials and those who expose government misconduct play an important role in holding authorities to

account. The Australian government should be careful to protect the country's democratic freedoms, especially the right to freedom of opinion and expression.

I. Espionage

In 2018, Australia enacted new espionage and foreign interference legislation, which expand the scope of espionage offences and increase penalties for unauthorized disclosure of information. These offences are directed at the way a person "deals with" information, and whether that "dealing" may prejudice Australia's national security or advantage the national security of a foreign country. The definition of "national security" is sweeping and in contravention to international law, including as it does "the country's political, military or economic relations with another country or other countries," a qualifier so broad it could cover almost any matter at all.

There is no public interest defence and no requirement of "intention to cause harm" as part of these offences. The vagueness of these provisions means anyone who receives or communicates politically sensitive information in a public manner could be guilty of one or more espionage offences. Human rights activists and journalists advocating or reporting on politically sensitive arenas are particularly exposed.

II. Use of Section 35P

Section 35P of the ASIO Act criminalizes disclosures of information "that relates to a special intelligence operation (SIO)" punishable by five or ten years imprisonment.[1] A 2016 report on section 35P by Roger Gyles, the independent national security monitor, found these amendments were likely to be unconstitutional and had a significant "chilling effect" on freedom of expression.[2] Specifically, the national security monitor report found the impact section 35P has on journalists is to create uncertainty about what may be published about the activities of ASIO without fear of prosecution. He found section 35P does not contain adequate safeguards for protecting the rights of "outsiders"[3] and is not proportionate to the threat of terrorism or the threat to national security. It is inconsistent with Article 19 of the International Covenant on Civil and Political Rights and as such not in accordance with Australia's international obligations.

---

[1] *Australian Security Intelligence Organisation Act 1979*, Part III, Division 4, s 35P(1) and (2); there are exceptions for disclosures: in the administration or execution of Division 4: for the purposes of a legal proceeding arising out of Division 4 or a report of such a proceeding; in accordance with a requirement imposed by law; in connection with the performance of ASIO functions, duties or powers; for the purpose of obtaining legal advice in relation to a SIO; or to and by officials of the Inspector-General of Intelligence and Security: s 35P(3).

[2] Roger Gyles, "Report on the impact on journalists of section 35P of the ASIO Act," https://www.pmc.gov.au/sites/default/files/publications/inslm_report_impact_s35p_journalists.pdf (accessed August 2, 2019), pp. 13-14.

[3] The report defines 'insiders' as ASIO employees, contractors and people who have entered into an agreement or arrangement with ASIO. 'Outsiders' are defined as third parties such as journalists.

Following Gyles' report, the law was amended to require that an outsider would not be committing an offence unless "the disclosure will endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation." However, section 35P remains on the books and as such it intimidates those involved in public interest reporting and whistleblowers who are still at risk of prosecution.[4]

III. Metadata and encryption

The current thresholds for law enforcement and intelligence agencies to access electronic data has a chilling effect on not only the media, but human rights organizations, whistleblowers, and those who have witnessed government misconduct. Secrecy offences and enhanced data surveillance powers risk criminalizing the legitimate actions of those trying to disclose information in the public interest. After the 2015 metadata retention scheme was introduced which requires telecommunications companies and internet service providers to retain metadata for at least two years, journalists were advised to avoid using their own mobile devices in source communications and to encrypt communications wherever possible.[5]

These laws mean law enforcement and intelligence agencies have unprecedented access to stored metadata in the interest of "national security." The Australian Federal Police (AFP) has acknowledged they accessed the metadata of journalists 58 times in the year from July 1, 2017 to June 30, 2018.[6] A Commonwealth Ombudsman report for the period July 2016 to June 2017 has revealed how police conducted a series of illegal metadata searches, including Western Australian police obtaining invalid warrants targeting journalists.[7] In the wake of the report's disclosures, Australian Capital Territory (ACT) police acknowledged accessing metadata of Australian citizens more than 3,300 times without proper authorisation.[8] This illustrates how metadata retention can be subject to abuse by authorities, and journalists, activists and whistleblowers may be at risk without proper oversight.

The Human Rights Law Centre has noted how "there is no independent body that will authorise access to data in appropriate cases, with criminal law enforcement and intelligence agencies

---

[4] Paul Farrell, "Journalists to get greater reporting protections on AFP cases," *The Guardian*, February 16, 2017, https://www.theguardian.com/australia-news/2017/feb/16/journalists-to-get-greater-reporting-protections-on-afp-cases (accessed August 2, 2019).

[5] Misha Ketchell, "Why the raids on Australian media present a clear threat to democracy," *The Conversation*, June 5, 2019, https://theconversation.com/why-the-raids-on-australian-media-present-a-clear-threat-to-democracy-118334 (accessed August 2, 2019).

[6] Bevan Shields, "Federal police accessed the metadata of journalists nearly 60 times," *The Sydney Morning Herald*, July 8, 2019, https://www.smh.com.au/politics/federal/federal-police-accessed-the-metadata-of-journalists-nearly-60-times-20190708-p52598.html (accessed August 2, 2019).

[7] Paul Karp and Josh Taylor, "Police made illegal metadata searches and obtained invalid warrants targeting journalists," *The Guardian*, July 23, 2019, https://www.theguardian.com/australia-news/2019/jul/23/police-made-illegal-metadata-searches-and-obtained-invalid-warrants-targeting-journalists (accessed August 2, 2019).

[8] Paul Karp, "ACT police admit they unlawfully accessed metadata more than 3,000 times," *The Guardian*, July 26, 2019, https://www.theguardian.com/australia-news/2019/jul/26/act-police-admit-unlawfully-accessed-metadata-more-than-3000-times (accessed August 2, 2019).

such as the Australian Security Intelligence Organisation and the Australian Federal Police able to self-authorise access to the stored metadata."[9]

Australia's Assistance and Access Act, enacted in 2018, creates a new framework for compelling assistance from communications service providers to access communications, content and data that may be protected by encryption or other technical measures. This law is also overly broad, lacking adequate safeguards to protect individuals from misuse by government officials. The attorney-general can issue notices without prior judicial oversight and can determine whether a notice is reasonable and proportionate. The law also excludes a "merits review"[10] of decisions taken to issue technical assistance or capacity notices, meaning an affected person cannot ask a tribunal to examine the correctness of a decision to issue a notice. The courts' powers of judicial review only enable an examination of whether the decisions are made within the legal limits of the legislation. This raises serious concerns that it will be inadequate to detect, prevent, and remedy abuses of the broad powers the law creates.

Government efforts to weaken encryption endangers people and undermines rights.[11] Without sufficient oversight, there may be instances where law enforcement determine it is "reasonable" and "proportionate" to issue a notice against a journalist, lawyer, human rights activist or other individual involved in exposing government misconduct.

IV. Protection for whistleblowers

Whistleblowers play an important role in keeping the government honest. The United Nations Human Rights Committee has noted that governments must take "extreme care" to ensure that laws relating to national security are not invoked to suppress or withhold from the public information of legitimate public interest that does not harm national security, or to prosecute journalists, activists, or others who disseminate such information. As the Alliance for Journalists' Freedom has noted, disclosures by whistleblowers in the private sector are only protected in a narrow set of circumstances and for those in the public sector, certain conditions have to be met. The Public Interest Disclosure Act 2013 limits the subject matter of disclosures whereas any breach of human rights should be added to the list of disclosable conduct.

Some of the most significant revelations of human rights violations come from disclosure of once-classified information relating to the misconduct of security agencies. Without significant

---

[9] Rachel Hardy, "UK Court of Appeal finds metadata retention regime inconsistent with EU law," *Human Rights Law Centre*, January 30, 2018, https://www.hrlc.org.au/human-rights-case-summaries/2018/3/26/uk-court-finds-metadata-retention-regime-inconsistent-with-eu-law (accessed August 2, 2019).

[9] Ibid.

[10] *Assistance and Access Bill 2018,* Explanatory Document (2018).

[11] Letter from Human Rights Watch to the Hon. Malcolm Turnbull MP, "Letter to Prime Minister Turnbull re Encryption and Human Rights," August 3, 2017, https://www.hrw.org/news/2017/08/03/letter-prime-minister-turnbull-re-encryption-and-human-rights.

protections in place, many people could be prosecuted simply for holding their government to account, and many others would be deterred from doing so.[12]

Human Rights Watch recommends the Joint Parliamentary Committee:

- Ensure safeguards are in place for all offences so that disclosures in the public interest are protected. Not only for journalists, but also for human rights activists, lawyers, whistleblowers and others making disclosures in the public interest;
- Revise the Espionage and Foreign Interference Act 2018, in particular by narrowing the definition of "national security" by, at the very minimum, excluding the proposed subsection (e) "the country's political, military or economic relations with another country or other countries," removing "reckless" as a level of culpability and requiring "intent to cause harm" as an element of all offences;
- Repeal and revise the current metadata and encryption laws to ensure appropriate judicial oversight and that any restriction on encryption in a given case is truly necessary and proportionate. This would include ensuring prior authorization by an independent judge, avenues to challenge a decision on the merits, and serving notice for affected individuals which can be delayed until such notice would not pose a threat to security or jeopardize an ongoing investigation but still remain a viable means of challenging the law or any decision taken under it;
- Repeal section 35P of the ASIO Act that criminalize disclosures related to special intelligence operations.

Annex: Examples of problematic law enforcement responses on matters in the public interest

I. Media raids

- On June 5, 2019, AFP officers spent more than eight hours raiding the ABC's Sydney headquarters. The raids were connected to a series of 2017 stories known as "The Afghan Files" which alleged unlawful killings and misconduct by Australian special forces in Afghanistan.[13] The allegations were based on hundreds of pages of secret Defence documents leaked to the ABC. The warrant named investigative journalists Dan Oakes and Sam Clark, and director of News Gaven Morris. AFP officers searched for article drafts, graphics, digital notes, visuals, raw television footage and all versions of scripts. The warrant authorized the AFP to search for and record "fingerprints found at the premises" and to take samples from the ABC for "forensic purposes." It also authorized the AFP to "add, copy, delete or alter other data … found in the course of a search."

[12] Alliance for Journalist's Freedom, "Press Freedom in Australia – White Paper," May 2019, https://www.journalistsfreedom.com/wp-content/uploads/2019/06/AJF-Press-Freedom-In-Australia-2019.pdf (accessed August 2, 2019), pp.16-17.

[13] Lorna Knowles, Elise Worthington and Clare Blumer, "ABC raid: AFP leave Ultimo building with files after hours-long raid over Afghan Files stories," *ABC*, June 6, 2019, https://www.abc.net.au/news/2019-06-05/abc-raided-by-australian-federal-police-afghan-files-stories/11181162 (accessed August 2, 2019).

- On June 5, 2019, the AFP raided the home of News Corp Australia journalist Annika Smethurst after executing a warrant investigating the "alleged publishing of information classified as an official secret." It allowed the police to search Smethurst's home, computer and mobile phone. The warrant was in relation to the April 2018 news story regarding a leaked plan to allow the Australian Signals Directorate to spy on Australian citizens for the first time. Under the plan, intelligence operatives would have been allowed to secretly access emails, bank accounts and texts messages with approval from the defence and home affairs ministries.[14]
- On June 4, 2019, hours after Annika Smethurst's house was raided by the AFP, 2GB Drive presenter and Sky News contributor Ben Fordham revealed he was also being targeted for his reporting on a story about six asylum seeker boats attempting to reach Australia. After his story went to air, his producer was contacted by an official from the Department of Home Affairs to advise the material being reported was "highly confidential" and that the Department would investigate the disclosure which may lead to a criminal investigation. While Fordham was told he was not the subject of potential charges, Home Affairs wanted his assistance in identifying his source.[15]
- On March 15, 2019, the AFP demanded that the airline Qantas disclose private travel arrangements of Daniel Oakes, one of the two ABC investigative journalists who broke "The Afghan Files" story. This was publicly disclosed on July 7, 2019.[16]

II. Witness K and Bernard Collaery

- Currently an ACT court is holding proceedings in secret against barrister Bernard Collaery and "Witness K." Collaery and Witness K were involved in legal disputes between the governments of Australia and Timor-Leste concerning entitlements to revenue from oil and gas fields in the Timor Sea. The two men are charged under section 39 of the Intelligence Services Act with conspiracy to communicate information from the Australian Secret Intelligence Service. Charges under that section, punishable by up to two years in prison, can only be brought by prosecutors with the consent of the attorney-general.
- The Timor-Leste government filed documents with the International Court of Justice in the Hague in 2014 stating that in 2004, "Australia covertly spied on the Timor-Leste negotiating team by means of listening devices surreptitiously and unlawfully placed by Australian personnel in the Timor-Leste government offices. This enabled the Australian negotiating team to become aware of the private discussions of the Timor-

[14] Paul Karp, "Federal police raid home of News Corp journalist Annika Smethurst," *The Guardian*, June 4, 2019, https://www.theguardian.com/australia-news/2019/jun/04/federal-police-raid-home-of-news-corp-journalist-annika-smethurst (accessed August 2, 2019).

[15] Shannon Molloy, "Radio star Ben Fordham targeted after Australian Federal Police raid political editor Annika Smethurst's home over spy story," *News.com.au*, June 4, 2019, https://www.news.com.au/finance/business/media/radio-star-ben-fordham-targeted-after-australian-federal-police-raid-political-editor-annika-smethursts-home-over-spy-story/news-story/ee864fd6be6c84dfa108647565c7ee25 (accessed August 2, 2019).

[16] Kylar Loussikian and Bevan Shields, "Federal Police forced Qantas to hand over the private travel records of an ABC journalist," *The Sydney Morning Herald*, July 8, 2019, https://www.smh.com.au/national/federal-police-forced-qantas-to-hand-over-the-private-travel-records-of-an-abc-journalist-20190707-p524xu.html (accessed August 2, 2019).

Leste negotiating team and of its position in relation to various issues arising in connection with the 2002 Treaty and the attempt to amend it by the drafting of the 2006 Treaty." The Australian government has not confirmed or denied the allegations.

- Witness K, who was part of the Australian bugging team, complained to Australia's inspector-general of intelligence about the legality of the operation in 2007 and subsequently, with the inspector-general's approval, sought legal advice from Collaery. Collaery was a legal advisor to the Timorese government.
- In December 2013, when the case was going to be heard at the International Court of Justice, ASIO agents raided Witness K's home and Collaery's office, seizing documents and data. They cancelled Witness K's passport, preventing him from traveling to the Hague, where he was due to give evidence. Timor-Leste then initiated proceedings against Australia regarding the seizure of documents, data, and other property that it said belonged to Timor-Leste or that Timor-Leste had the right to protect under international law.
- Details of the charges against the two men were only made public on June 28, 2017, when a member of parliament, Andrew Wilkie, used parliamentary privilege to disclose the prosecution.