HUMAN RIGHTS WATCH

January 22, 2018
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 National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017

Summary

Human Rights Watch is concerned that provisions of the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 ("the Bill") infringe on basic rights, particularly the rights to freedom of opinion and expression and the implied right to political communication. These rights are protected under the International Covenant on Civil and Political Rights and other treaties to which Australia is a party.[1]

This submission raises specific concerns about the espionage[2] and secrecy[3] provisions in the Bill, which risk criminalizing the legitimate actions of whistleblowers, journalists, and human rights activists, and will have a chilling effect on disclosing information in the public interest.

The Bill comprises amendments that aim to "counter the threat of foreign states exerting improper influence over our system of government and our political landscape."[4] In the second reading of the Bill, Prime Minister Malcolm Turnbull said that "[g]lobally, Russia has been wreaking havoc across the democratic world" and that "by enacting this legislation, and building the capability to properly use it, we are sending an unmistakable signal: We will not allow foreign states to use our freedoms to erode freedom; our open democracy to subvert democracy; our laws to undermine the rule of law." However, this Bill threatens to facilitate the destruction it wards against by eroding a fundamental pillar of democracy: the right to freedom of opinion, expression and political communication.

---

[1] International Covenant on Civil and Political Rights (ICCPR), G.A. res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, entered into force March 23, 1976, article 19. Australia ratified the ICCPR in 1980.

[2] National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 ("Espionage and Foreign Interference Bill") schedule 1, part 1, items 10-17 (proposed Part 5.2 Division 91 of the Criminal Code).

[3] Espionage and Foreign Interference Bill schedule 2, part 1 (proposed Part 5.6 of the Criminal Code).

[4] Second Reading Speech, Espionage and Foreign Interference Bill, December 7, 2017, available at http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansardr%2F716f5e71-dee3-40a3-9385-653e048de81b%2F0193%22.

The Australian government already has broad powers to counter foreign interference with Australia's political, governmental or democratic processes. Australia has a raft of measures in place to limit the disclosure of classified information including strict penalties for espionage, treason, terrorism, and disclosure of official secrets.[5]

If Australia adopts the Bill in its current form it is following in the steps of repressive countries such as Cambodia and Turkey. The proposed measures exceed what is necessary for or proportionate to the goal of protecting national security and democracy.[6] Australia's parliament should ensure that the Bill is, at the very minimum, amended to include adequate protections for matters in the legitimate public interest. Legal provisions that chill free expression do not protect Australia's democratic values but undermine them.

Findings and Recommendations

With respect to the espionage offences, Human Rights Watch is particularly concerned about the potential for the Bill to:

1. Apply overly broad definitions of "dealing with" and "national security";

2. Subject a person to criminal and punitive sanction for conduct that is legitimate and in the public interest; and

3. Encroach upon freedom of political communication and a free press by facilitating retaliation against those who publish or disclose information that has the potential to embarrass officials or the government.

We recommend that the Parliamentary Joint Committee:

- Narrow 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";
- In the espionage offence, require the information or article both "has a security classification and concerns Australia's national security," instead of "or";
- Remove "reckless" as a level of culpability;

---

[5] See, for example, Criminal Code Act 1995 (Cth) ("Criminal Code") sections 80.1AA , 91.1(1) and 91.1(2).

[6] The United Nations Human Rights Committee, the independent expert body that interprets the ICCPR and monitors state compliance, has stated in its General Comment on the right to freedom of expression: "When a State party invokes a legitimate ground for restriction of freedom of expression, it must demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat." UN Human Rights Committee, General Comment No. 34, Article 19: Freedoms of Opinion and Expression, U.N. Doc. CCPR/C/GC/34 (July 21, 2011), para. 35.

- Require intent to cause harm as an element of all offences; and
- Include a general "legitimate public interest" defence.

Background – existing law

Under existing Australian law, espionage is an offence committed where a person unlawfully communicates or makes available information concerning Australia's security or defence or information acquired from the Australian government concerning the security or defence of another country.[7] The act must be committed with intent to prejudice Australia's security or defence or advantage another country's security or defence. The maximum penalty is imprisonment for 25 years.

The existing law also contains offences that cover the making, obtaining or copying of a government record relating to Australia's security or defence or information concerning the security or defence of another country.[8] The term "record" is defined broadly to include information in any form, including but not limited to, a document, paper, database, software system or other article or system containing information or from which information can be derived.[9] Information includes an opinion.[10]

Espionage offences in the Bill

The Bill introduces a range of new espionage offences. These offences are directed at the way a person deals with information, and whether that dealing may affect national security by i) prejudicing Australia's national security; or ii) advantaging the national security of a foreign country (together, **"**prejudice national security**"**).

The amendments will increase the maximum penalty for an espionage offence committed with intent from imprisonment for 25 years to imprisonment for life.

Under the Bill, a person is taken to deal with information if the person: (a) receives or obtains it; (b) collects it; (c) possesses it; (d) makes a record of it; (e) copies it; (f) alters it; (g) conceals it; (h) communicates it; (i) publishes it; or (j) makes it available.[11]

The already extremely broad definition of "information" remains unchanged, and means information of any kind, whether true or false and whether in a material form or not, and includes an opinion and a report of a conversation.[12]

---

[7] Criminal Code sections 91.1(1) and 91.1(2).

[8] Criminal Code, sections 91.1(3) and 91.1(4).

[9] Criminal Code, section 90.1 definition of "record."

[10] Criminal Code, section 90.1 definition of "information."

[11] Espionage and Foreign Interference Bill, schedule 1, part 1, item 10, definition of "deal" (proposed section 90.1(1) of the Criminal Code).

[12] Criminal Code, section 90.1, definition of "information."

"National security" is defined to mean, in summary, any of the following: (1) the defence of the country; (2) the protection of the country or the people of the country from espionage, sabotage, terrorism, political violence, and foreign interference; (3) the protection of the integrity of the country's territory and borders from serious threats; and (4) the country's political, military or economic relations with another country or countries.

Several of the new espionage offences require the offending person to have an intent to "prejudice national security" or relate to dealing with information with a security classification and so may be unlikely to affect the layperson.[13] However, "reckless conduct" and "conduct regarding information that "concerns" Australia's national security" are also criminalized and will carry the previous maximum penalties of imprisonment for 25 and 20 years respectively.

For example, section 91.1(2) states that a person: (a) who deals with information that concerns Australia's national security; (b) who is reckless as to whether their conduct will Prejudice National Security; and (c) whose conduct results in the information being made available to a foreign principal, is guilty of an offence and may be imprisoned for 25 years. Section 91.2(2) makes it an offence for a person to recklessly deal with any information, which is not necessarily information that concerns Australia's national security, in a way that may prejudice Australian national security and results in the information being made available to a foreign principal. The penalty is 20 years' imprisonment.

Section 91.3 creates an offence if a person deals with information that "concerns Australia's national security" in a way that results in the information being made available to a foreign principal, regardless of the absence of any intent or recklessness. Further, the Bill provides the same penalty for dealing with information that is not classified but that "concerns Australia's national security."

The lack of specificity in what exactly constitutes national security, what "concerns" national security and how it may be prejudiced, and the very broad definition of what constitutes "dealing with" information, could mean that any person who receives or communicates political 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 would be particularly exposed.

Such standards could easily be used to deter important investigative reporting, since a reporter or activist will have to guess whether information could be deemed to endanger state security in some undefined way and self-censor, or may even be made liable at a later date for risks the reporter or activist could not possibly be in a position to foresee.

[13] See, for example, Espionage and Foreign Interference Bill, proposed sections 91.1(1)(b)(i) and 91.1(2)(b)(i).

Finally, section 91.11 makes it an offence to engage in conduct "making it easier" to "solicit" or "procure" an espionage offence. Intention to cause harm is not required and it does not matter if another person read, heard, or viewed the information in question – just the act of making it available to others will be sufficient, regardless of the actual threat to national security. This is because it is not clear how strong the causative link needs to be between a person's conduct and information becoming available to a foreign principal. For example, the new offences may apply to users of social media who share leaked information by reposting it on Facebook or Twitter. Similarly, sections 91.1(2), 91.2(2) and 91.3 may in effect criminalize the publication of politically sensitive information that a foreign principal may independently access.

A defence is only available against the above offences if a defendant can establish that information was dealt with in accordance with a law of the Commonwealth, an arrangement with the Commonwealth, or in their capacity as a public official. In addition, if the information that is being dealt with had already been communicated to the public with the authority of the Commonwealth, a defence may also be claimed. The defendant again bears the burden of proof in establishing an applicable defence.

Disclosures in the public interest

Human rights activists and organizations meet regularly with foreign diplomats, United Nations representatives and regional groups like ASEAN and the European Union to raise concerns about abusive governmental policies and press for change. But no one should face criminal charges for bringing such issues to the attention of foreign governments. Journalists likewise should not face prosecution for investigating and reporting on such matters. The Bill threatens to criminalize these interactions if information discussed is deemed to "prejudice national security." The definition of "national security" under the Bill is so broad that it encompasses "the country's political, military or economic relations with another country or other countries," making the ambit for what is considered "espionage" extremely broad.

The requirement of consent of the attorney-general prior to the prosecution of an offence of espionage, foreign interference, sabotage, theft of trade secrets, or other threats against security does not remedy the threat to liberty that the offence carries. Further, considering whether the conduct in question was authorized, and therefore whether the accused has a defence available, is an insufficient safeguard against legitimate public interest reporting if there is not such defence available. Having these espionage offences as law will likely chill advocacy and reporting on legitimate public interest issues because activists, journalists and editors will be rightly hesitant to risk prison time.

These concerns are not farfetched: overly broad espionage laws have been used to intimidate and imprison journalists and peaceful activists in Cambodia, Turkey and other countries.

In Cambodia, espionage laws have been used to silence independent media and activists critical of the government. In August 2017, the government revoked radio licenses for stations broadcasting Voice of America and Radio Free Asia (RFA), forcing RFA's Cambodian bureau to close, and closing the independent radio station Voice of Democracy.[14] Authorities charged two RFA journalists with espionage in November for allegedly providing information to RFA.[15] In June, authorities also charged an Australian filmmaker, James Ricketson, with espionage over allegations he collected information prejudicial to the country's national security. Ricketson had been making a documentary relating to the Cambodian main opposition party. He remains in prison awaiting trial.[16]

In Turkey in 2016, police charged journalists Can Dündar, then-editor of the daily newspaper *Cumhuriyet*, and Erdem Gül, *Cumhuriyet's* Ankara bureau chief, with espionage for an article under Dündar's byline that included photographs and a link to an online video purporting to show large quantities of mortar shells, grenade launchers, and ammunition hidden in a Turkish truck bound for Syria in January 2014. In publishing the story and images, the newspaper challenged Turkish government claims that the trucks had been part of a humanitarian assistance operation to Syria run by Turkey's National Intelligence Agency (MİT).[17] The two were charged with espionage, but ultimately convicted of the lesser offence of obtaining and revealing state secrets that might harm state security or Turkey's domestic and foreign interests. The court determined that it had not been able to prove intent to spy.

Secrecy offences

The Bill amends secrecy offences to better target unauthorised disclosure and unlawful handling of Commonwealth information. Schedule 2 of the Bill creates a number of new offences for disclosure of certain types of information in a wide range of circumstances.

Human Rights Watch echoes the concerns of the Human Rights Law Centre that the limits the Bill places on freedom of expression and open government are disproportionate and overly broad and that criminalize the unauthorised disclosure of "information obtained by a public servant" that is "inherently harmful" or "likely to harm Australia's interests." We refer the Committee to the Human Rights Law Centre's submission in this regard.[18]

---

[14] Human Rights Watch, "Cambodia: Crackdown Crushes Media, Opposition," January 18, 2018, https://www.hrw.org/news/2018/01/18/cambodia-crackdown-crushes-media-opposition.

[15] Human Rights Watch, "Cambodia: Crackdown Crushes Media, Opposition."

[16] Camille Bianchi, "Family, activists fight for Australian filmmaker's release as he awaits trial in Cambodia," *SBS News,* January 110, 2018, https://www.sbs.com.au/news/family-activists-fight-for-australian-filmmaker-s-release-as-he-awaits-trial-in-cambodia_1 (accessed January 22, 2018).

[17] Human Rights Watch, "Turkey: Silencing the Media," December 15, 2018, https://www.hrw.org/news/2016/12/15/turkey-silencing-media.

[18] Human Rights Law Centre, Submission to the Australian Parliamentary Joint Committee on Intelligence and Security on the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017, January 22, 2018, https://www.hrlc.org.au/submissions/.

Protecting whistleblowers vital to democracy

The government has a responsibility to protect legitimate national security interests, and not all leaks deserve protection. However, whistleblowers are those who reveal misconduct or unethical policies in the public interest, and they play an important role in keeping government honest. Whistleblowers need protection from retaliation for their disclosures in the public interest. We are concerned that if this Bill becomes law, it will have a chilling effect on whistleblowers.

In a post-Snowden and Wikileaks world, it is evident that simply cloaking something as "classified" doesn't mean it should automatically be free from public scrutiny. Under this Bill, government officials may be tempted to reclassify information with a higher security rating so that it cannot be shared. Nor should public discourse be stifled by the threat of prosecution for receiving unclassified information that concerns such wide-ranging and vague topics as "the country's political, military or economic relations with another country or other countries." Whistleblowers, journalists and human rights activists play a crucial role in revealing misconduct and unethical policies in the public interest.

It is very dangerous for democratic values to introduce such sweeping laws that restrain publication of materials in the public interest. The UN 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"[19] or to prosecute journalists, activists, or others who disseminate such information.

Punishing whistleblowers who leak security information or those who publish it is problematic because it suppresses information that may be vital for the exercise and protection of human rights, accountability and democratic governance. Some of the most significant revelations of human rights violations come from disclosure of once-classified information relating to the misconduct of security agencies. If the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 passes into law, many people could be prosecuted simply for holding their government to account, and many others would be deterred from doing so.

[19] UN Human Rights Committee, General Comment No. 34, Article 19: Freedoms of Opinion and Expression, U.N. Doc. CCPR/C/GC/34 (July 21, 2011), para. 30.