PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

Advisory Report on the Foreign Intelligence Legislation Amendment Bill 2021

Parliamentary Joint Committee on Intelligence and Security

August 2021
CANBERRA

ISBN 978-1-76092-287-0 (Printed Version)

ISBN 978-1-76092-288-7 (HTML Version)

Contents

Terms of Reference

The Foreign Intelligence Legislation Amendment Bill 2021 (the Bill) was referred to the Committee by the Minister for Home Affairs for review and report on 20 August 2021.

Members

Chair

Senator James Paterson

Deputy Chair

Hon Anthony Byrne MP

Members

Senator the Hon Eric Abetz

Dr Anne Aly MP

Hon Mark Dreyfus QC MP

Senator the Hon David Fawcett

Ms Celia Hammond MP

Senator the Hon Kristina Keneally

Mr Julian Leeser MP

Senator Jenny McAllister

Mr Tim Wilson MP

List of Recommendations

Recommendation 1

1.29 The Committee recommends that the Foreign Intelligence Legislation Amendment Bill 2021 be amended to require that the Committee be notified that a mandatory written procedure (as inserted by subsection 11C(6)) has been issued or varied, and that the Committee be provided with a briefing on the procedure as soon as practicable once it has been issued.

Recommendation 2

1.31 The Committee Foreign Intelligence Legislation Amendment Bill 2021 be amended so that the Committee may conduct a review of the amendments made by it not less than five years from when the Bill receives Royal Assent

Recommendation 3

1.37 The Committee recommends that, subject to the amendments outlined above, the Foreign Intelligence Legislation Amendment Bill 2021 be passed.

1. Committee's review of the Bill

1.1 The Foreign Intelligence Legislation Amendment Bill 2021 (the Bill) was referred to the Committee for private review and report on Friday 20 August 2021 by the Minister for Home Affairs, the Hon Karen Andrews MP. The Bill and Explanatory Memorandum (EM) were referred on an embargoed basis as the Bill had not yet been tabled in the Parliament.

Conduct of the inquiry

1.2 The Committee agreed to the government's request to expeditiously consider this legislation in a private inquiry given the sensitive nature of the intelligence capability concerned and the risk of disruption to parliamentary sittings posed by the COVID outbreak in the ACT.

1.3 The Committee held a classified briefing on Monday 23 August 2021 with officials from relevant agencies.

The Bill

1.4 The following section gives a brief overview of the Bill as described in the Explanatory Memorandum (EM).

1.5 The Foreign Intelligence Legislation Amendment Bill 2021 (the Bill) amends *the Telecommunications (Interception and Access) Act 1979* (TIA Act) and the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) to address critical gaps in Australia's foreign intelligence warrant framework. Foreign intelligence means intelligence about the capabilities, intentions or activities of people or organisations outside Australia. Without the proposed changes, gaps in foreign intelligence collection will continue to grow and Australia will not have visibility of possible threats to Australia and its security. The

Bill will improve intelligence agencies' ability to collect intelligence about foreign threats to Australia, and keep Australia safe and prosperous.

1.6 Schedule 1 of the Bill amends the foreign communications warrant in section 11C of the TIA Act to overcome the difficulty intelligence agencies face in distinguishing between foreign and domestic communications in the modern technological environment. Under the reforms, the Director-General of Security will be able to apply for a warrant authorising the interception of a communication for the purpose of obtaining foreign intelligence from foreign communications. Currently, the interception of any domestic communications is strictly prohibited.

1.7 Schedule 1 is designed to restore the foreign communications warrant to its original scope and function. The removal of the strict prohibition is accompanied by robust safeguards to protect domestic communications in the same way the original prohibition intended.

1.8 Schedule 2 of the Bill enables the Attorney-General to issue foreign intelligence warrants to collect foreign intelligence on Australians in Australia who are acting for, or on behalf of, a foreign power. Currently, requesting a warrant for the purpose of collecting information concerning an Australian citizen or permanent resident is prohibited in all circumstances.

Schedule 1: Section 11C foreign communications warrant amendments (section 11C of the TIA Act)

1.9 Currently, foreign communications warrants, issued by the Attorney-General under section 11C of the TIA Act, authorise the interception of foreign communications for the purpose of obtaining foreign intelligence about a matter specified in the warrant.

1.10 The challenge with the existing foreign communications warrant is that the interception of domestic communications (communications that both start and end within Australia) is prohibited, even where that interception is inadvertent or unavoidable.

1.11 This restriction made sense when the warrant was introduced into the TIA Act in 2000. The primary forms of communication technologies were telephone and fax, which used reliable geographic identifiers such as country code, city code and exchange code. These identifiers enabled intelligence agencies to determine the location of the sender and receiver of communications, even prior to the interception occurring.

1.12 Since then, advances in technology—particularly widespread use of internet-based communications and mobile applications—mean that it can be impossible to know, at the point of interception, if a communication is foreign or domestic.

1.13 Currently, to avoid breaching the TIA Act, intelligence agencies do not intercept foreign communications where there is even the smallest risk of incidentally intercepting domestic communications. This considerable constraint on the collection of foreign intelligence is creating the real risk that intelligence agencies are missing critical foreign intelligence.

1.14 The reforms will allow intelligence agencies to intercept communications, including where the geographic location of the sender and recipient of the communications cannot be determined prior to their interception. Robust safeguards accompany these reforms:

- The proposed warrants can only be issued for the purpose of obtaining foreign intelligence from foreign communications (paragraph 11C(1)(a)).
- The warrant request must specify how the risk of intercepting domestic communications will be minimised (paragraph 11C(3)(a)).
- The Attorney-General must issue a mandatory written procedure (subsection 11C(6)) to:
  - screen for domestic communications that may have been intercepted
  - destroy all records of any domestic communication so identified (unless the communication relates, or appears to relate, to activities that present a significant risk to a person's life), and
  - notify the Inspector-General of Intelligence and Security (IGIS) of any identified domestic communication that relates, or appears to relate, to activities that present a significant risk to a person's life.
- The mandatory procedure issued by the Attorney-General may also deal with any other matters relating to communications intercepted under a warrant under section 11C (subsection 11C(7)).
- Before issuing or varying the mandatory procedure, the Attorney-General must consult the Minister for Defence, Minister for Foreign Affairs, IGIS and the Director-General of Security (subsection 11C(9)).
- The Attorney-General must review the mandatory procedure as soon as practicable within one year of it being issued, and then every 3 years.
- The term 'screening' is intended to capture a continuous process for identifying domestic communications.
- The existing safeguards for foreign communications warrants will also continue to apply:

- Requesting these warrants for the purpose of collecting information concerning an Australian is specifically prohibited unless the Director-General reasonably suspects the Australian is acting for, or on behalf of, a foreign power (subsection 11D(5), as amended by Schedule 2).
- The Attorney-General must be satisfied, on the advice of the Minister for Defence or the Minister for Foreign Affairs, that the collection of foreign intelligence is in the interests of Australia's national security, Australia's foreign relations, or Australia's national economic wellbeing (subparagraph 11C(1)(b)(i)).
- The Attorney-General must be satisfied that it is necessary to intercept foreign communications in order to collect foreign intelligence, and that alternative foreign intelligence warrants would be ineffective (subparagraphs 11C(1)(b)(ii) and (iii)).

1.15 Only in the exceptional circumstance where there is a significant risk to life will intelligence agencies be able to rely on inadvertently intercepted domestic communications. This exception will ensure Australia's intelligence agencies can respond to, for example, an imminent terrorist attack.

1.16 The IGIS will also continue to have oversight of agencies' activities under these warrants, and will oversee the compliance with the mandatory procedures issued by the Attorney-General. The IGIS has extensive powers, akin to those of a standing Royal Commission and is an essential safeguard.

Schedule 2: Australians or permanent residents acting for, or on behalf of, a foreign power (subsection 11D(5) of the TIA Act and 27A(9) of the ASIO Act)

1.17 Currently, subsections 11D(5) of the TIA Act and 27A(9) of the ASIO Act prohibit the Director-General of Security from requesting the issue of a foreign intelligence warrant for the purpose of collecting information concerning an Australian citizen or permanent resident.

1.18 The Comprehensive Review of the Legal Framework of the National Intelligence Community (Comprehensive Review), conducted by Dennis Richardson AC, recommended reforms to allow foreign intelligence to be collected on Australian citizens and permanent residents in Australia, who are acting for or on behalf of foreign powers.

1.19 These amendments will close a legislative gap where foreign intelligence can be collected offshore on an Australian working for a foreign power, but that

same intelligence cannot be collected inside Australia on that Australian under a warrant. As the Comprehensive Review observed:

> Preventing some forms of collection when the Australian target is onshore, but enabling it when the target is offshore, seems a disproportionate restriction that costs Australia a significant intelligence dividend. It can also cost the Government the opportunity to collect valuable foreign intelligence that has a direct bearing on Australia's national security, foreign relations and national economic well-being more securely and cost effectively than offshore collection.
>
> …An Australian serving the interests of a foreign government… remains an agent of a foreign power whether they are onshore or offshore.

1.20 There are circumstances where Australian citizens and permanent residents are of legitimate foreign intelligence interest. For example, where an Australian citizen is acting as an agent of a foreign state.

1.21 Robust safeguards will accompany these reforms:

- The law will continue to prevent the request of a foreign intelligence warrant on Australian persons who are not acting for, or on behalf of, a foreign power (subsection 27A(9) in the ASIO Act and subsection 11D(5) of the TIA Act).
- The Director-General of Security must include, in the request of a warrant, details about the grounds on which he or she suspects that the person is acting for, or on behalf of, a foreign power (paragraph 27A(9A)(a) of the ASIO Act and paragraphs 11A(3)(a), 11B(4)(a) and 11C(3A)(a) of the TIA Act).
- The Attorney-General must not issue a warrant unless he or she is satisfied that the person is, or is reasonably suspected by the Director-General of Security of, acting for, or on behalf of, a foreign power (paragraph 27A(9A)(b) of the ASIO Act and paragraphs 11A(3)(b), 11B(4)(b) and 11C(3A)(b) of the TIA Act).
- The Attorney-General must be satisfied, on advice from either the Minister for Defence or the Minister for Foreign Affairs that the collection is in the interests of Australia's national security, foreign relations or economic well-being (existing paragraph 27A(1)(b) in the ASIO Act and existing paragraph 11A(1)(b), and subparagraphs 11B(1)(b)(i) and 11C(1)(b)(i) of the TIA Act).

1.22 The IGIS will also continue to have oversight of agencies' activities under these warrants. The IGIS has extensive powers, akin to those of a standing Royal Commission and is an essential safeguard.

Committee Comment

1.23 The importance of Australia's Intelligence Community to be able to collect foreign intelligence in a legal, proportionate and timely manner cannot be understated.

1.24 These are not powers that the Parliament provides lightly and the Committee sees its role in reviewing the provision of such powers as one of its most important functions. In stating this the Committee notes the following from the Explanatory Memorandum:

> Without the proposed changes, gaps in foreign intelligence collection will continue to grow and Australia will not have visibility of possible threats to Australia and its security. The Bill will improve intelligence agencies' ability to collect intelligence about foreign threats to Australia, and keep Australia safe and prosperous.[1]

1.25 The Committee also notes the important and continuing oversight role played by the IGIS. The Committee has been assured during the course of its inquiry that any non-compliance will be reported to the IGIS and that the Committee will have an opportunity to examine these issues with the IGIS as part of its oversight responsibilities.

The mandatory procedure

1.26 The Committee notes that the Attorney-General must issue a mandatory written procedure (subsection 11C(6)) to:

- screen for domestic communications that may have been intercepted
- destroy all records of any domestic communication so identified (unless the communication relates, or appears to relate, to activities that present a significant risk to a person's life), and
- notify the Inspector-General of Intelligence and Security (IGIS) of any identified domestic communication that relates, or appears to relate, to activities that present a significant risk to a person's life.

1.27 The Committee notes that before issuing or varying the mandatory procedure, the Attorney-General must:

- consult the Minister for Defence, Minister for Foreign Affairs, IGIS and the Director-General of Security (subsection 11C(9)); and,

---

1 Explanatory Memorandum, p. 1.

- must review the mandatory procedure as soon as practicable within one year of it being issued, and then every 3 years.

1.28 To provide further oversight and an assurance to the Parliament and, through it, the Australian people the Committee recommends it be notified that a mandatory written procedure (as inserted by subsection 11C(6)) has been issued or varied and be provided with a briefing on the mandatory written procedure as soon as practicable.

Recommendation 1

1.29 The Committee recommends that the Foreign Intelligence Legislation Amendment Bill 2021 be amended to require that the Committee be notified that a mandatory written procedure (as inserted by subsection 11C(6)) has been issued or varied, and that the Committee be provided with a briefing on the procedure as soon as practicable once it has been issued.

1.30 In addition the Committee recommends that the Bill be amended so that the Committee may commence a review of the amendments made by the Bill within 5 years of it receiving Royal Assent.

Recommendation 2

1.31 The Committee Foreign Intelligence Legislation Amendment Bill 2021 be amended so that the Committee may conduct a review of the amendments made by it not less than five years from when the Bill receives Royal Assent

1.32 The Committee notes that this Bill aligns Australia with the Five Eyes community but with a stronger set of safeguards. Further information on this is provided in Appendix One.

1.33 The Committee appreciates the time sensitive nature of this legislation, and is grateful that despite this, the Government appropriately consulted with committee members and provided classified briefings necessary for the committee to discharge its duties. Although required to do so quickly, the Committee has discharged its responsibilities to the parliament by robustly testing the rationale for the bill and each of the provisions of the bill.

1.34 It is not ordinarily the preference of the Committee to conduct private inquiries nor to do so on an expedited basis. The Committee only agreed to in this instance because of the unique circumstances of this bill and the

additional risks to Parliamentary sittings caused by the current COVID outbreaks.

1.35 The Committee believes this Bill provide the National Intelligence Community with the necessary powers and tools to protect Australia and Australians against threats to their security.

1.36 Overall, the Committee is satisfied with the provisions contained in the Bill and recommends that the Foreign Intelligence Legislation Amendment Bill 2021 be passed.

Recommendation 3

1.37 The Committee recommends that, subject to the amendments outlined above, the Foreign Intelligence Legislation Amendment Bill 2021 be passed.

Senator James Paterson
Chair

24 August 2021

A. Five Eyes Foreign Intelligence Gathering Legislation

The following table compares foreign intelligence gathering legislation across the "Five Eyes" community against the following:

- Incidental collection
- Destruction of domestic incidental collection;
- Destruction of irrelevant collection;
- Retention of incidental collection;

Foreign Intelligence Legislation Amendment Bill 2021 – Five Eyes Legislation Comparison

	Australia – Current law	Australia – Amendments	UK	US	Canada	New Zealand
Authorising legislation	*Telecommunications (Interception and Access) Act 1979* (TIA Act)	Foreign Intelligence Legislation Amendment Bill 2021 (FILA Bill)	*Investigatory Powers Act 2016* (IPA)	*Foreign Intelligence Surveillance Act 1978* (FISA)	*Communications Security Establishment Act 2019* (CSE Act)	*Intelligence Services Act 2017* (IS Act)
Incidental collection	**Not permitted.** Section 11C of the TIA Act only authorises the collection of foreign communications.	**Permitted.** The FILA Bill will allow for the collection of communications (regardless of where they start or end) for the purpose of collecting foreign intelligence (cl 11C(1)).	**Permitted.** A bulk interception warrant authorises the interception of communications not described in the warrant (s 136(5)).	**Permitted.** FISA authorises the targeting of persons reasonably believed to be outside the United States to acquire foreign intelligence information. Domestic communications and citizens must not be intentionally targeted (§ 702).	**Permitted.** CSE is authorised to acquire domestic information incidentally in the course of carrying out activities under an authorisation (s 23(4)).	**Permitted.** Both Type 1 (NZ person) and Type 2 (foreign intelligence) warrants authorise an activity for the purpose of collecting information. There is no prohibition on the type of communication that may be collected (s 53 and 54).
Destruction of domestic incidental collection	**Not applicable.**	**Required**. The FILA Bill requires the Attorney-General to establish a procedure for destroying all records of identified domestic communications (cl 11C(6)(b)).	**Not required.**	**Required.** FISA requires incidental domestic collection to be destroyed upon recognition (§ 106).	**Not required.**	**Required.** Unauthorised information must be destroyed immediately after it is obtained (s 102(2)).
Destruction of irrelevant collection	**Required.** Section 14 of the TIA Act requires the Director-General of Security to cause the destruction of communications when satisfied they are no longer required by the Organisation in the performance of its functions or the exercise of its powers.	**Required.** The FILA Bill requires the Director-General of Security to cause the destruction of communications, when satisfied they are not relevant to the purposes specified in the warrant (cl 11C(5)).	**Required.** Material obtained under a warrant must be destroyed as soon as there are no longer any relevant grounds for retaining it (s 150(5)). *IPA Interception of Communications Code of Practice* Destroying data involves taking reasonable steps to make the data unavailable or inaccessible, but does not involve taking steps such as the physical destruction of hardware (paragraph 9.23).	**Not required.**	**Not required.**	**Required.** Irrelevant information (information no longer required by the agency for the performance of its functions) must be destroyed as soon as practicable (s 103).
Retention of incidental collection	**Not applicable.**	**Permitted.** The FILA Bill permits domestic communications to be retained if it relates to a significant risk to a person's life (cl 11C(5)(c) and 11C(6)(b)).	**Permitted.** Material may be retained if it is in the interests of national security, preventing or detecting serious crime, or in the interest of economic wellbeing (s 150(6)).	**Permitted**. Domestic collection may be retained if the Attorney General determines the contents indicate a threat of death or serious bodily harm to any person (§ 106).	**Permitted.** Domestic communications may be retained if the information is essential to international affairs, defence or security (s 34(2)(c)).	**Permitted.** Incidental collection may be retained for the prevention of serious crime, threats to life and threats to New Zealand's security or defence.