# Parliamentary Joint Committee on Intelligence and Security

## Attorney-General's Department

**Hearing date:** **N/A**

**Question date:** 16 May 2024

**Peter Khalil asked the following question:**

1. In his submission, the Parliamentary Inspector of the Corruption and Crime Commission of Western Australia has welcomed the changes in Schedule 5, but has noted that they are not picked up in the definition of 'prescribed investigation' in paragraph 5(1)(j) of the TIA Act. The Parliamentary Inspector notes that the existing language in this definition ('dealing with a matter of misconduct in the performance of the Parliamentary Inspector's functions under the Corruption and Crime Commission Act') is narrower than that used in the definitions which apply to the other listed state-based oversight bodies. The Parliamentary Inspector proposes that the paragraph be rephrased as 'an investigation that the Parliamentary Inspector is conducting in the performance of the Parliamentary Inspector's functions under the Corruption, Crime and Misconduct Act 2023 (WA)'.

a. Does the Attorney-General's Department have any concerns with the Parliamentary Inspector's proposed re-formulation of paragraph (j) of the definition of 'prescribed investigation'? Is the Department aware of any other reason why this Committee should not recommend that the Parliamentary Inspector's suggestion be adopted?

**The response to the question is as follows:**

The department notes the submission of the Parliamentary Inspector of the Corruption and Crime Commission of Western Australia (Parliamentary Inspector) that the definition of 'prescribed investigation' in paragraph 5(1)(j) of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) should be drafted more broadly to ensure the Parliamentary Inspector can access telecommunications interception information for the full scope of its investigatory functions, and not just for investigations relating to officer misconduct.

The department agrees with the Parliamentary Inspector that the drafting of this provision is inconsistent with analogous amendments applying to other oversight bodies within Schedule 5 of the Bill, and should be corrected. As noted in the Explanatory Memorandum (at paragraph 21), the intention of the measure is to expand the definition of 'permitted purpose' for each oversight body to align with the definition within the oversight bodies' respective enabling legislation *to accurately encompass their oversight functions* [emphasis added].

The department does not have any concerns with the Parliamentary Inspector's suggestion.

# Parliamentary Joint Committee on Intelligence and Security

## Attorney-General's Department

**Hearing date:** **N/A**
**Question date:** 16 May 2024

**Peter Khalil asked the following question:**

1. Schedule 5 to the Bill proposes to extend the permitted purposes for which lawfully intercepted information and interception warrant information can be disclosed to oversight bodies for state-based integrity agencies. In its submission, the Law Enforcement Conduct Commission (NSW) has requested that the Committee consider the extension of these disclosure powers to include stored communications information accessed under Chapter 3 of the TIA Act, and telecommunications data accessed under Chapter 4.

a. Is the Attorney-General's Department aware of any reason why it would not be appropriate for stored communications or telecommunications data accessed by state-based integrity agencies to be disclosable to the oversight bodies for those agencies?

**The response to the question is as follows:**

As with intercepted information and interception warrant information, stored communications and telecommunications data contain sensitive information. As such, any extension to agencies' ability to receive and use the information would need to be robustly justified as being necessary to the performance of that agency's functions, balanced with the resulting impact on human rights such as the right to privacy and right to freedom of expression as outlined in the International Covenant on Civil and Political Rights (ICCPR).

The extension of access to intercepted information and interception warrant information in Schedule 5 of the Bill is justified by the fact that oversight bodies of integrity agencies already perform inspection functions in relation to state and territory compliance with interception record-keeping obligations imposed by Chapter 2 of the *Telecommunications (Interception and Access) Act 1979* (TIA Act). Further, there are no other agencies that oversee integrity agencies' use of interception powers. It is, therefore, a sensible extension of oversight bodies' inspection functions to enable them to receive and use interception information and interception warrant material for their whole-of-agency oversight functions.

The benefit of extending access to stored communications and telecommunications data to oversight bodies of integrity agencies is less clear cut. This is because the Commonwealth Ombudsman already oversees state and territory agency compliance regarding stored communications and telecommunications data under Chapters 3 and 4 of the TIA Act. It does this through routine compliance audits which include the inspection of files and systems, interviews with staff, observing practices and obtaining and maintaining a working knowledge of each agency's systems, policies and procedures.

Given state and territory integrity agencies' use of Chapters 3 and 4 of the TIA Act is already overseen by the Commonwealth Ombudsman, allowing those agencies' oversight bodies to receive and use stored communications and telecommunications data would likely duplicate the role of the Commonwealth Ombudsman. This may be viewed as an unnecessary extension of the use and disclosure provisions for sensitive information obtained through covert surveillance.

Section 186F of the TIA Act also allows the Commonwealth Ombudsman to give information it has obtained under its stored communications and telecommunications data inspections to a state and territory inspecting body if it is satisfied that the giving of the information is necessary to enable the inspecting authority to perform its functions. Through this mechanism, oversight bodies of integrity agencies have an avenue to be made aware of issues pertaining to the broader range of their functions without needing to receive and use stored communications or telecommunications data.

The department is open to consulting state and territory integrity agencies and their oversight bodies in relation to the suggestion proposed in the submission of the Law Enforcement Conduct Commission (NSW) before finalising a policy position. Such an amendment, if determined to be necessary following this consultation, could form part of wider electronic surveillance reforms to be undertaken by the department in response to the Comprehensive Review of the Legal Framework of the National Intelligence Community.