Australian Government
Attorney-General's Department

October 2022

Parliamentary Joint Committee on Intelligence and Security – Review of Item 250 of the National Anti-Corruption Commission (Consequential and Transitional Provisions) Bill 2022

Attorney-General's Department Submission

Introduction

The Attorney-General's Department welcomes the opportunity to make a submission to the Committee on the Committee's review of an amendment to subsection 110A(1) of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) included in the National Anti-Corruption Commission (Consequential and Transitional Provisions) Bill 2022 (the Bill).

The TIA Act protects the privacy of telecommunications in Australia, and provides a legal framework under which Commonwealth, state and territory law enforcement agencies, as well as the Australian Security Intelligence Organisation, may obtain information from communications providers to investigate criminal offences and other activities that threaten the safety and security of Australians.

The Bill would amend paragraph 110A(1)(c) of the TIA Act to transfer ACLEI's existing powers to access stored communications and telecommunications data to the National Anti-Corruption Commission (the Commission). These stored communications and telecommunications data powers will form part of the Commission's broader suite of powers to investigate serious or systemic corrupt conduct.

Subsection 110A(11) of the TIA Act requires any amendment to subsection 110A(1) to be referred to this Committee for review, consistent with recommendation 17 of this Committee's *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.*

Overview of the Commission's functions and powers

The Commission will be a specialist anti-corruption agency, with broad jurisdiction to investigate serious or systemic corruption involving Commonwealth ministers, parliamentarians and their staff, statutory office holders, employees of all government agencies and contractors. The Commission's jurisdiction will also extend to any person who engages in conduct that could adversely affect the honesty or integrity of a public official's exercise of their functions, duties or powers. The Commission will be able to investigate both criminal and non-criminal corruption.

It is common for persons engaged in serious or systemic corruption to take significant steps to conceal or obfuscate their activities. The National Anti-Corruption Commission Bill 2022 will provide the Commissioner with strong investigative powers, similar to those of a Royal Commission, to uncover the full extent of the evidence. The Bill will provide the Commission with access to covert investigative powers under the *Crimes Act 1914, Surveillance Devices Act 2004* and the TIA Act*,* including the ability to obtain stored communications warrants and to access telecommunications data. Collectively, these powers will enable the Commission to obtain information about corruption that would otherwise be unobtainable.

Amendments to the TIA Act

The Bill would amend the TIA Act to enable the Commission to use the powers that the TIA Act currently confers on the Australian Commission for Law Enforcement Integrity (ACLEI), state anti-corruption commissions and other law enforcement bodies. The Commission's access to these powers will be provided on the same basis as these bodies, including the same thresholds for the issue of warrants and authorisations, safeguards and oversight.

The Bill would also amend the *Telecommunications Act 1997* to provide the Commission, as well as state anti-corruption and investigative commissions that currently have access to Commonwealth electronic

surveillance powers,[1] access to the industry assistance framework under Part 15 of the Act. This would be consistent with Recommendation 1 of the Independent National Security Legislation Monitor's 2020 *Review of the Telecommunications and Other Legislation (Assistance and Access) Act 2018* and public statements made by the Committee in February 2019. These amendments would ensure that each agency permitted to intercept communications under the TIA Act is also able to obtain the necessary assistance from providers to ensure that encrypted communications can be accessed in an intelligible form.

The Attorney-General's Department is leading a major reform of Australia's electronic surveillance laws in response to recommendations of the *Comprehensive Review of the Legal Framework of the National Intelligence Community*. The reform aims to replace the TIA Act, the *Surveillance Devices Act 2004*, and parts of the *Australian Security Intelligence Organisation Act 1979* to address technological difficulties, inconsistency and complexity. The reform would include the Commission's access to and use of relevant powers in the same way as other agencies. The Government will continue to work with stakeholders to develop draft legislation for release and public feedback in 2022 to 2023, prior to consideration by Parliament.

Definition of 'criminal law-enforcement agency' under section 110A of the TIA Act

Item 250 of the Consequential Bill would amend subsection 110A(1) of the TIA Act, which sets out the list of 'criminal law-enforcement agencies' that may obtain stored communications warrants and access telecommunications data, to replace references to ACLEI with references to the Commission—in effect, transferring ACLEI's existing powers to the Commission.

This would enable the Commission to obtain documentary evidence that would be relevant to a criminal corruption investigation, such as contemporaneous text messages or emails held by carriers and carriage service providers (stored communications), and evidence indicating that persons of interest have, or have not, been in contact with one another (telecommunications data).

Access to such information can be critical to the success of criminal corruption investigations. Over the past three years ACLEI has made 2 applications for stored communication warrants which were both issued, 831 authorisations for disclosure of telecommunications data, and 162 authorisations for disclosure of prospective telecommunications data. During this time, the types of offences for which authorisations were made varied from fraud and bribery in 2019 to 2020, to cybercrime, illicit drug offences and people smuggling in 2020 to 2021.

Access to stored communications

This amendment would permit the Commissioner, Deputy Commissioners and staff members of the Commission authorised by the Commissioner in writing to apply for a stored communications warrant under section 110 of the TIA Act.

Under section 116 of the TIA Act, an issuing authority (a Judge, magistrate, or member of the AAT, appointed by the Attorney-General under section 6DB of the TIA Act) may grant a stored communications warrant if satisfied that, among other things, there are reasonable grounds for suspecting that a particular carrier holds relevant stored communications and that the information obtained would be likely to assist in connection

[1] The Independent Commission Against Corruption of New South Wales, the New South Wales Crime Commission, the Law Enforcement Conduct Commission of New South Wales, the Independent Broad-based Anti corruption Commission of Victoria, the Crime and Corruption Commission of Queensland, the Independent Commissioner Against Corruption of South Australia, and the Corruption and Crime Commission of Western Australia.

with the investigation of a serious contravention (including a serious offence). A serious contravention is, among other things, a contravention of an Australian law punishable for a maximum period of at least 3 years. This threshold, and the matters an eligible Judge or a nominated AAT member must consider, would apply to applications by the Commission as they currently do to ACLEI and consistently with other agencies able to apply for stored communications warrants.

Accessing telecommunications data

As a criminal law-enforcement agency under paragraph 110A(1)(c) of the TIA Act, the Commission would also be an enforcement agency under section 176A of that Act, able to authorise access to telecommunications data under Chapter 4 of the TIA Act.

An authorised officer of an enforcement agency can authorise access to historical telecommunications data if satisfied that it is reasonably necessary for, among other things, enforcing the criminal law (section 178 of the TIA Act). In relation to data that comes into existence during the period of authorisation (prospective data), an authorised officer can only authorise access if satisfied the disclosure is reasonably necessary for the investigation of a serious offence, or an offence punishable by imprisonment for at least three years (section 180 of the TIA Act). For the purposes of the Commission, an authorised officer would be the Commissioner (as the head of a criminal law-enforcement agency), or a person in a management position authorised by the Commissioner.

Where the Commission seeks telecommunications data that relates to a person who is working in a professional capacity as a journalist, or their employer, for the purpose of identifying an informant, the Commission would require a journalist information warrant under section 180T prior to making an authorisation under Chapter 4 of the TIA Act. This threshold, and the matters an authorised officer must consider, would apply to the Commission as they currently do to ACLEI and consistently with other agencies able to access telecommunications data.

The Government considers that improved protections for press freedom are needed and intends to progress further legislative reform. The Government is examining the recommendations of two completed parliamentary inquiries into press freedom being this Committee's 2020 *Inquiry into the impact of law enforcement and intelligence powers on the freedom of the press*, and the 2021 Senate Environment and Communications References Committee *Inquiry into press freedom*.

Oversight of the Commission's use of powers under the TIA Act

Consistent with existing oversight arrangements under the TIA Act, the Commission's use of powers under that Act would be subject to oversight by the Commonwealth Ombudsman. This will ensure that the Commission's use of these powers will be subject to the same, consistent standards of oversight that the Ombudsman provides for all other Commonwealth, state and territory law enforcement and anti-corruption agencies.

The Inspector of the Commission would also be able to receive information that has been lawfully obtained by another agency under the TIA Act and rely on that information as part of an investigation into serious or systemic corruption relating to the Commission. This will ensure that the Inspector is able to work in partnership with relevant Commonwealth, state and territory agencies to investigate allegations of criminal corruption relating to the Commission.