Australian Government
Department of Home Affairs

Department of Home Affairs submission to the Review of the Telecommunications and Other Legislation Amendment Bill 2025

Parliamentary Joint Committee on Intelligence and Security

22 September 2025

Table of Contents

Telecommunications and Other Legislation Amendment Bill 2025

Overview

1. The Department of Home Affairs (the Department) welcomes the opportunity to provide a submission to the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) Review of the Telecommunications and Other Legislation Amendment Bill 2025 (the Bill).
2. The Bill amends the *Telecommunications (Interception and Access) Act 1979* (TIA Act), *Surveillance Devices Act 2004* (SD Act) and the *Crimes Act 1914* (Crimes Act) to ensure key provisions operate as intended, and to support the proper administration of government, law enforcement, national security and criminal justice processes.
3. The Bill contains five Schedules:
    a. Schedule 1 permits information related to network activity warrants to be used, communicated and recorded to comply with the prosecution's disclosure obligations. It also allows the information to be admitted in evidence by the defendant when necessary to ensure they are afforded a fair trial, or to respond to any such information admitted by the defence.
    b. Schedule 2 transfers the statutory function of the Communications Access Coordinator (CAC) from the Secretary of the Attorney-General's Department to the Secretary of the Department that is administered by the Minister administering the TIA Act (currently the Department).
    c. Schedule 3 permits limited access to stored communications under development and testing authorisations issued under Part 2-4 of the TIA Act, to ensure the framework continues to achieve its intended purpose.
    d. Schedule 4 corrects a technical issue with the operation of interception international production orders in Schedule 1 to the TIA Act that was preventing United States (US)-based prescribed communications providers from being able to produce prospective content data where they do not have the technical capability to do this in real-time under the *Agreement between the Government of Australia and the Government of the United States of America on access to electronic data for the purpose of countering serious crime*.
    e. Schedule 5 amends Part IAB of the Crimes Act to clarify the threshold for authorising and varying controlled operations and subsequently the circumstances in which a participant is protected from criminal responsibility and indemnified against civil liability.
4. In relation to Schedules 1, 4 and 5, this submission reflects the joint views of the Department and the Australian Federal Police (AFP).

Schedule 1: Amendments relating to network activity warrants

Purpose and effect of amendments

5. This Schedule amends the SD Act and the TIA Act to ensure that network activity warrant information and network activity warrant intercept information can be:
    a. communicated, used and recorded for the purposes of making a decision about a criminal prosecution for a relevant offence
    b. communicated, used and recorded for the purposes of meeting disclosure obligations in a criminal prosecution for a relevant offence
    c. adduced or given in evidence by the defendant where necessary for the defendant's fair trial, and
    d. adduced or given in evidence in response to evidence given or adduced by the defendant.

6. The purpose of the amendments is to ensure that prosecutions can proceed in an ordinary and fair manner, in cases where network activity warrant information may be relevant to or disclosable in the proceedings, while preserving the intelligence-only nature of network activity warrants to the greatest extent possible. The amendments achieve this purpose, in particular, by:
   a. ensuring that the prosecution can consider any potentially exculpatory information obtained by using a network activity warrant when considering whether to institute or continue proceedings
   b. enabling the prosecution to disclose network activity warrant information to the defendant, where that information falls within the prosecution's disclosure obligations, and
   c. allowing the defendant to lead this information in the trial, if it is necessary to ensure they receive a fair trial—for example, where the information is potentially exculpatory, or may support a relevant line of questioning by the defence.
7. Consistent with the intelligence-only nature of network activity warrants, the prosecution will not be able to use information obtained by using a network activity warrant to establish its case. The prosecution will only be permitted to adduce or give such information in evidence if defendant choses to lead this evidence. This is similar to the existing restrictions on the prosecution leading character or propensity evidence and would permit the prosecution to, for example, rebut or provide context to evidence led by the defence.
8. All other strict limitations on the use and disclosure of information collected using a network activity warrant remain unaffected.

Context

9. Network activity warrants were introduced by the *Surveillance Legislation Amendment (Identify and Disrupt) Act* 2021 (SLAID Act) to allow the AFP and Australian Criminal Intelligence Commission (ACIC) to collect intelligence on criminal networks using encrypted communications platforms and networks, and operating on the dark web, to obfuscate their identities, activities and plans.
10. Network activity warrants permit access to the platforms, devices and networks used to facilitate criminal activity, enabling the AFP and ACIC to target the activities of criminal networks to discover the scope of criminal offending and the identities of the people involved. They have been used in investigations relating to serious and organised crime, and offending connected to drugs, firearms, money laundering, child exploitation and people trafficking.
11. Network activity warrants are intended to be used for intelligence purposes, rather than for the collection of evidence. As the Revised Explanatory Memorandum to the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2021 noted, at paragraph 23:

    > *There are strict prohibitions on the use of information obtained under a network activity warrant. Information obtained under a network activity warrant is for intelligence only, and will not be permitted to be used in evidence in criminal proceedings, other than for a breach of the secrecy provisions of the SD Act.*

12. Reflecting this intent, section 45B of the SD Act contains specific use and disclosure provisions for network activity warrant information that prevent such information from being used in connection with, or admitted in evidence in, criminal proceedings—with the exception of proceedings for an offence for unauthorised dealings in such information.
13. The prosecution has a duty to disclose material that, on sensible appraisal, is relevant (or possibly relevant) to an issue in the case; raises (or possibly raises) an issue that was not apparent from the prosecution case; or holds out a real prospect of providing a lead in relation to evidence concerning either

of the first two categories of material. The Commonwealth Director of Public Prosecutions *Statement on Disclosure*[1] provides:

> *In addition to fulfilling any local statutory obligations relating to disclosure, the prosecution must disclose to the accused any material which:*
>
> - *can be seen on a sensible appraisal by the prosecution to run counter to the prosecution case (i.e. points away from the accused having committed the offence); or*
> - *might reasonably be expected to assist the accused in advancing a defence; or*
> - *might reasonably be expected to undermine the credibility or reliability of a material prosecution witness.*

14. Section 45B, as currently drafted, has the unintended consequences of preventing agencies from reviewing information collected under a network activity warrant when deciding whether to commence a prosecution and determining whether the information is required to be disclosed. Section 45B would also have the unintended consequence of preventing the prosecution from disclosing such information to the defence, if it were determined to be required to be disclosed. The consequences of the prosecution being unable to determine whether disclosure obligations apply, or to comply with those obligations should they arise, could be significant—including providing a basis for an application to stay the relevant proceedings.

15. As at 31 December 2024, a total of 7 network activity warrants and 21 warrant extensions have been granted to the AFP and ACIC since 2021. Prosecutions arising from investigations that have been informed by intelligence collected under network activity warrants are now beginning to progress to trial.

16. The Independent National Security Legislation Monitor has reached a similar conclusion, in the report *Data Disruption, Network Activity and Account Takeover Powers Review of Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*, tabled in the Parliament on 1 September 2025. Recommendation 14 (e) of that report is that:

> *Potentially exculpatory material obtained under a N[etwork] A[ctivity] W[arrant] should be able to be disclosed in accordance with the usual prosecutorial duty of disclosure.*

17. The passage of this amendment would give effect to this recommendation.

Schedule 2: Amendments relating to the Communications Access Coordinator

Purpose and effect of amendments

18. This Schedule amends section 6R of the TIA Act to transfer the regulatory role of the Communications Access Coordinator (CAC) from the Secretary of the Attorney-General's Department to the Secretary of the Department of Home Affairs consistent with changes in ministerial responsibility set out in the Administrative Arrangement Order made on 13 May 2025. The CAC's functions are being performed by staff temporarily transferred to the Attorney-General's Department, pending the passage of the proposed amendments.

Context

19. The CAC performs a range of industry regulatory functions relating to the electronic surveillance framework. These include the approval of telecommunications providers' interception capability plans (under section 198 of the TIA Act) and granting exemptions or variations from the mandatory data retention scheme (under section 187K of the TIA Act). The role of the CAC has historically been vested in

[1] Commonwealth Director of Public Prosecutions, *Statement on Disclosure in Prosecutions Conducted by the Commonwealth* (20 August 2024) [3].

the Secretary of the Department responsible for the administration of the TIA Act, including following relevant Machinery of Government changes in 2017 and 2022.

20. At present, under subsection 6R(1) of the TIA Act, the CAC is the Secretary of the Attorney-General's Department, or a person or body covered by a legislative instrument made by the Attorney-General under subsection 6R(2) of the TIA Act.

21. The 13 May 2025 Administrative Arrangements Order transferred the responsibility of the TIA Act from the Attorney-General to the Minister for Home Affairs. Ordinarily, governments would request the Governor-General make a substituted references order under the *Acts Interpretation Act 1901* to reflect changes in Ministerial and departmental responsibilities following a Machinery of Government change. However, in this case, section 6V of the TIA Act prevents such an order being made, and requires Parliamentary amendments to be made.

Schedule 3: Amendments relating to developing and testing interception capabilities

Purpose and effect of amendments

22. This Schedule amends the TIA Act to ensure that agencies are able to properly develop and test technologies and interception capabilities, under authorisations given by the Attorney-General, in circumstances where stored communications are intermingled with live communications passing over the network.

23. These amendments align the development and testing framework in Part 2-4 of the TIA Act with other warrants and authorisations in the Act, by providing that a development and testing authorisation authorises access to stored communications if, and only if, the authorisation would have authorised interception of that same communication if it were still passing over a telecommunications system.

24. The amendments also clarify that the use and disclosure provision in subparagraph 31A(2)(a)(ii) permits persons authorised under a section 31A authorisation to communicate, use or record lawfully intercepted information obtained under the authorisation for the purposes of development or testing of technologies, or interception capabilities. This has been included for the avoidance of doubt and makes explicit what is implied from the condition in subparagraph 31A(2)(a)(ii).

Context

25. The *Telecommunications (Interception and Access) Amendment Act 2007* introduced the developing and testing authorisations framework in Part 2-4 to allow security authorities to seek authorisation from the Attorney-General to intercept communications passing over a telecommunications system for the purpose of that development or testing.

26. The framework is important to enable agencies to develop and test technologies and interception capabilities, before they are deployed in live, operational contexts. The framework is also important to ensure that such technologies and capabilities can be updated to keep pace with continual changes in communications technologies. These development and testing activities are critical to ensure that technologies and capabilities operate effectively and appropriately—for example, to ensure that a particular interception capability will intercept all of the communications that it should collect under a warrant, and does not intercept communications that are not authorised to be collected under that warrant.

27. At present, development and testing authorisations may only authorise the interception of live communications. However, there are circumstances in which stored communications can be inextricably intermingled with live communications—for example, where stored communications held on a server are being backed-up to another server, or are being 'synced' to an end-user device, and so are passing over the network alongside other live communications. This intermingling can prevent agencies from

undertaking development and testing activities, in circumstances where it is not possible to intercept live communications under an authorisation without also accessing stored communications.

28. The amendments in Schedule 3 align the treatment of stored communications in the development and testing provisions with their treatment in the interception warrant provisions, and the drafting draws closely on the precedent in Part 2-2 of the TIA Act (which allows for access to stored communications under interception warrants).

29. The Bill also extends all of the robust safeguards that apply to intercepting live communications under a development and testing authorisation to accessing stored communications. This includes:

    a. Applications can only be made by the head (or acting head) of a security authority, and must include details of the extent to which stored and live communications would be accessed, and the proposed development or testing activities.

    b. The Attorney-General must authorise the proposed interception or access for development and testing purposes.

    c. Information obtained under a development and testing authorisation may only be used for development or testing technologies, or interception capabilities, and it cannot be used for intelligence production or investigative activities. Of note, Schedule 3 will require any stored communications obtained under a testing and development authorisation to be handled in the same manner, and subject to the same strict limitations, as intercepted communications. The offence provision in section 105 of the TIA Act will then apply to the communication, use or recording of development and testing information in contravention of these limitations.

    d. All information obtained under a development and testing authorisation must be destroyed soon as practicable after it is no longer required for development or testing.

Schedule 4: Amendments relating to international production orders

Purpose and effect of amendments

30. This Schedule corrects a technical issue that prevented interception international production orders from being given to US-based prescribed communications providers and thereby gives effect to the original intent of the international production orders scheme.

31. The current framework assumes that data in response to an interception international production order will be returned to the requesting agency in a ‘livestream’ or ‘recording’ fashion. However, many companies within the intended scope of the framework do not have the technical capability to ‘livestream’ data in response to an order targeting prospective content, and establishing this capability would require significant technical investment by both Australian agencies and the US providers. As a result, Australian law enforcement and intelligence agencies have been unable to seek prospective content data from these prescribed communications providers.

32. The amendments in Schedule 4 to the Bill provide a technology-neutral function of what a prescribed communications provider can do in a response to an order for ‘intercepted’ communications. It allows them to transfer prospective content data to law enforcement agencies using methods other than a ‘livestream’, such as making a copy of messages from their servers and transmitting the copy to the agency.

33. These amendments do not override existing safeguards contained in the industry assistance framework under Part 15 of the *Telecommunications Act 1997,* nor do they create new powers to compel a provider to build new capabilities. The industry assistance framework explicitly prohibits agencies from requesting assistance that operates to remove, or build a capacity to remove, end-to-end encryption or other forms of electronic protection. The framework also explicitly prohibits agencies from requesting providers to

create a systemic weakness or vulnerability into a form of electronic protection, or from rectifying a systemic weakness or vulnerability in an existing system.

Context

34. Schedule 1 of the TIA Act establishes the International Production Order framework. It provides the ability for orders seeking interception, stored communications, or telecommunications to be directed at companies based in countries with which Australia has a designated international agreement.

35. Australia and the United States entered into the *Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime* (the Agreement) on 15 December 2021. The Agreement allows both nations to obtain more timely access to electronic data held by service providers to prevent, detect, investigate and prosecute serious crimes and safeguard national security.

36. The agreement became operational on 30 January 2024. As of 3 September 2025, 127 International Production Orders[2] for stored communications and telecommunications data have been sent by relevant agencies in Australia to Covered Providers under the Australia-US Data Access Agreement. These orders have related to a wide range of serious crime types, including murder, drug trafficking, terrorism, cybercrime, espionage, child abuse, and money laundering.

37. International production orders are an invaluable investigative tool to obtain the contents of communications that occur using offshore communications platforms, such as those operated by Meta, Google, Microsoft, Apple or Discord. Stored data obtained pursuant to international production orders has already been used in Australian court proceedings as evidence of serious crime. In a recent example, *DPP (Cth) v Kulendran*,[3] which involved sentencing for 43 Commonwealth child sex offences, the sentencing judge made reference to the deterrent impact of law enforcement access to communications using US-based platforms, and the value of the material to identifying additional offending, in that case, Discord and Snapchat (emphasis added):

> *It is to be noted, and as part of deterring others it should be widely known, that law enforcement could, and in this case did, secure your history of use of Discord and Snapchat. To be clear, the police secured two international production orders relating to your Snapchat and Discord accounts. These orders were authorised by the Commonwealth Administrative Review Tribunal, pursuant to the Telecommunications (Interceptions and Access) Act, and pursuant to those international production orders both Snapchat and Discord corporations produced data to the police in relation to your accounts on those platforms. A review of that data revealed additional sexualised conversations engaged by you with persons you believed to be under 16.*

38. The access to prospective communications on such platforms, in cases where it is reasonable and appropriate for such access to be authorised by an issuing person, provides Australian law enforcement and national security agencies with the opportunity to disrupt serious criminal activity in close to real time.

39. The international production order framework has provided significant efficiency benefits, as compared to the mutual legal assistance framework. International production orders have resulted in data being returned from providers in three days for high priority cases and two months for routine investigations with no particular time sensitivities. Mutual assistance, by contrast, regularly has return times in excess of twelve months, and the assessment and resolution of these cases entails a significant administrative burden for both the Attorney-General's Department and the US Department of Justice.

40. In the development of Schedule 4 the Department, with the assistance of the Attorney-General's Department as the Australian Designated Authority, consulted:

    a. the United States Department of Justice

    b. interception agencies, other agencies capable of using TIA Act powers relating to stored communications or telecommunications data, and related agencies such as the Ombudsman, and

---

[2] As at 3 September 2025.

[3] [2025] VCC 1133, [26].

c. US communications providers.

Schedule 5: Amendments relating to controlled operations

Purpose and effect of amendments

41. This Schedule amends the controlled operations provisions in Part IAB of the Crimes Act to clarify the threshold for authorising and varying controlled operations and subsequently the circumstances in which a participant is protected from criminal responsibility and indemnified against civil liability when engaging in conduct in a controlled operation.

42. The amendments make clear that a controlled operation must not be authorised or varied[4] if it is *reasonably foreseeable* that unlawful conduct of a participant will *directly*:

    i. endanger the health or safety of any person or

    ii. cause the death of, or serious injury to, any person or

    iii. involve the commission of a sexual offence against any person or

    iv. result in significant loss of, or serious damage to, property (other than illicit goods).

43. A consequence is a *direct* consequence of unlawful conduct if the unlawful conduct *causes or produces*, and is not merely a minor influence on, the consequence without any intervening conduct or events. As a result, the decision maker would not be expected to consider potential indirect effects of unlawful conduct by participants at the time of authorisation, including indirect consequences which a reasonable person may consider foreseeable as well as those that are far-fetched or fanciful.

    a. For example, an undercover operative may be seeking to infiltrate a dark web child abuse syndicate suspected of livestreaming abuse material and harming children. In this scenario, harm is occurring to children irrespective of any police action. To enable infiltration of the syndicate under a controlled operation, the undercover operative may be required trade in certain material. Without amendments, there is a risk that the operative's conduct, although it does not amount to incitement or encouragement, could not be authorised due to risk that the suspect might engage in dangerous criminal behaviour as an indirect consequence of the operative's conduct.

44. The amendments would also allow a decision maker to authorise an operative to deal with, or facilitate a person to deal with, material depicting, material describing or material otherwise involving a sexual offence against any person for the purposes of a controlled operation.

    a. The phrase 'facilitating a person to deal with' material is intended to capture conduct where a participant in a controlled operation is required to enable the actions of others for the purposes of the controlled operation. In practice, this may enable a participant to administer or moderate an online forum to infiltrate a syndicate. This aligns with the original intention of the controlled operations scheme – to allow law enforcement to infiltrate criminal organisations and target those in the upper echelons of those organisations.[5] It would not enable a participant to encourage a person to create material, because the creation of such material would, in these circumstances, be a direct consequence of such encouragement and may seriously endanger a person or involve the operative in a sexual offence.

45. Finally, the amendments clarify that a participant may be protected from criminal responsibility or indemnified against civil liability if the conduct involves the participant dealing with, or facilitating a person

---

[4] *Crimes Act 1914* (Cth) ss 15GI(2)(g), 15GQ(2)(g) and 15GV(2)(g).

[5] Revised Explanatory Memorandum, Crimes Legislation Amendment (Serious and Organised Crime) Bill 2010, 52.

to deal with, material depicting, material describing, or material otherwise involving a sexual offence against any person. These amendments are consequential from the ones above.

46. These amendments would still retain the intent of safeguards in the controlled operations regime: to not allow participants to seriously endanger, cause serious harm to others or be involved in sexual offences, and to limit unlawful conduct to the maximum extent consistent with conducting the controlled operation.[6]

Context

Current operating environment

47. Controlled operations are targeted and discrete operations performed by law enforcement both on and offline to obtain critical evidence to disrupt, charge and prosecute serious crimes. Over time, and in today's technological environment, elements of the broader legislative framework within which law enforcement operate within, including the controlled operations scheme, have become less clear. Rapid advancements in technology mean that perpetrators can commit crimes with increasing anonymity and sophistication, and in innovative ways. Anonymisation is becoming more sophisticated online and harder for police to address. Covert online investigations can take weeks or months deploying tradecraft that will result in identifying online actors. Due to a lack of clarity in the current legislation, enforcement agencies are finding it increasingly difficult to authorise and execute important powers, including controlled operations in online spaces—such as the dark web—to target such abhorrent crimes.

48. At the same time, rates of reported online child sexual exploitation have dramatically increased. Since the inception of the Australian Centre to Counter Child Exploitation (ACCCE), reports of online child sexual exploitation have increased more than five-fold, from more than 14,000 in the 2018-19 financial year, to more than 82,000 in the 2024-25 financial year. The number of reports in the 2024-25 financial year increased by 41% from the previous financial year.

49. With the proliferation of child sexual abuse and exploitation, the community has called for urgent reforms to better protect children. In June and July 2025, media reported that two men separately working in childcare industries in Victoria and New South Wales had been charged with a string of child sex offences, including in relation to the production of child abuse material. The public reporting of the alleged conduct of these two men towards innocent children in their care has caused outrage from the public, as well as calls for urgent change. This type of offending has been uncovered by police through online investigations.

Lack of clarity in existing legislation

50. The legislation does not clearly articulate the extent to which a decision maker is expected to foresee potential risks of unlawful conduct by participants when deciding whether to authorise or vary a controlled operation and not decide to authorise on the basis of these risks. This includes risks which may be indirect, far-fetched, or fanciful. In practice, it can be incredibly difficult for a decision maker to be confident that there would be no indirect effects of participant conduct that may cause one of the above outcomes, particularly before the commencement of an online investigation.

51. The Bill clarifies that a decision maker is not expected to consider any actions of persons who are not participants listed in the controlled operation authority – including, for example, people that are the target of the controlled operation. Extending conduct to the actions of suspects or people other than participants in a controlled operation, unless the conduct is in some way caused by the investigative activity of participants, would not align with the original intention of the scheme – which was to enable law enforcement to engage in unlawful conduct for the purpose of obtaining evidence about a serious criminal offence.[7]

52. In addition to this, the obfuscation of activities online means that authorising officers are not always able to foresee all the potential consequences of conduct proposed to be engaged in under a controlled operation at the time of authorising or varying the controlled operation. This is because the decision

[6] Ibid ss 15GI(2)(c), (g), 15GQ(2)(c), (g) and 15GV(2)(c), (g).
[7] Revised Explanatory Memorandum, Crimes Legislation Amendment (Serious and Organised Crime) Bill 2010, 51.

maker may not always know things such as the identity or location of offenders, or their propensity to commit serious offences, at the time of deciding whether to authorise or vary a controlled operation. For example, when considering whether to authorise a controlled operation on an encrypted site where users post sexual abuse material, the decision maker may not know the identity or criminal history of users posting or soliciting that material, nor the user's possible access to children.

53. Finally, the current legislation is also not abundantly clear as to whether a participant in a controlled operation may deal with material involving a sexual offence for the purposes of the controlled operation. Such conduct was previously intended to be permissible, based on the previous equivalent controlled operations scheme:

> *… a covert investigation may involve an investigating official assuming the identity of a paedophile. In this capacity, they may need to trade in pornography to garner credibility as a paedophile, and to progress their investigations. Should an investigation demand such drastic action, it would be necessary to remove the possibility of any illegality attaching to police trading pornography by issuing a controlled operations certificate*.[8]

Conclusion

54. The amendments to the TIA Act, SD Act and the Crimes Act set out in the Schedules to the Bill address particular issues that are preventing agencies from using the framework in the manner intended and support the proper administration of justice. The passage of the amendments is necessary to:

    a. support prosecutors and agencies to comply with disclosure obligations and to support a fair trial

    b. finalise Machinery of Government changes following the Administrative Arrangements Order made on 13 May 2025

    c. ensure that agencies can continue to undertake essential testing and development necessary to ensure that their capabilities keep pace with technological advancements

    d. give effect to the Agreement between the Government of Australia and the Government of the United States of America on access to electronic data for the purpose of countering serious crime, and

    e. provide law enforcement agencies with greater clarity about controlled operations, allowing them to better collect evidence to prosecute serious offending occurring online.

55. The Department looks forward to assisting the Committee with its Review.

[8] Explanatory Memorandum, Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill (No. 2) 2004, 53.