INDEPENDENT COMMISSION
AGAINST CORRUPTION
NEW SOUTH WALES

Submission: Reform of Australia's electronic surveillance framework

Overview

The Independent Commission Against Corruption of New South Wales (ICAC) welcomes an invitation to comment on the Department of Home Affairs discussion paper on the reform of Australia's electronic surveillance framework. We support the development of a single Act in which law enforcement and intelligence agencies have appropriate powers to investigate serious crimes and threats to security. The Commission agrees the framework requires modernisation including the removal of technology specific assumptions, so that agencies and industry have clarity on the information they can obtain, and their respective obligations. The Commission supports harmonising thresholds for the use of powers with similar levels of privacy intrusion. The Commission is extremely concerned with the recent trend to exclude some agencies from access to powers, such as in the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA Act) and the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth) (SLAID Act). This trend reduces the effectiveness of agencies and threatens their key functions. The omission of the Commission from powers afforded to other agencies produces detrimental and perverse outcomes, benefitting those who engage in serious crime and corruption.

The Commission has provided relevant commentary on Australia's electronic surveillance framework to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in their review of the mandatory data retention regime in the *Telecommunications Interception and Access Act 1979* (the TIA Act). The Commission has contributed multiple submissions to the PJCIS in their reviews of the TOLA Act and a joint submission on TOLA to Dr James Renwick CSC, SC in his capacity as the Independent National Security Legislation Monitor (INSLM). In 2019, the Commission made a submission to Mr Dennis Richardson AC in his Comprehensive Review of the Legal Framework of the National Intelligence Community. Our submissions are available on their respective websites.[1]

About ICAC

The Commission was established in 1988 in response to growing community concern about the integrity of public administration in New South Wales. The principal functions of the Commission are to investigate and expose corrupt conduct in and affecting the NSW public sector. The *Independent Commission Against Corruption Act 1988* (NSW) gives the Commission broad jurisdiction to investigate any allegation or circumstance which, in its opinion, implies that corrupt conduct has occurred or is likely to occur. In deciding to investigate a matter, the Commission may use the powers it has under legislation to gather information. Investigations are diverse in character and can range from simple to complex and embrace past and current activities. They can require the use of various covert and overt methods of investigation.[2]

The Commission is an *interception agency* for the purposes of the TIA Act. The Commission is defined as a *law enforcement agency* within s4 of the *Surveillance Devices Act 2007* (NSW) and s6A of the *Surveillance Devices Act 2004* (Cth). Delegated Commission Officers can request carrier or carriage service providers to

[1] At https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security
[2] For more information see https://www.icac.nsw.gov.au/about-the-nsw-icac/overview/functions-of-the-icac.

assist under s313 of the *Telecommunications Act 1997* (Cth) in circumstances where assistance is reasonably necessary for enforcing the criminal law and laws imposing pecuniary penalties. The Commission is not currently defined as an *interception agency* for the purposes of industry assistance in s 317B of the *Telecommunications Act 1997,* powers that were afforded through the TOLA Act.

Responses to Discussion Paper Questions

Part 1: Who can access information under the new framework?
1. Do the existing prohibitions and offences against unlawful access to information and data adequately protect privacy in the modern day?
The Commission considers existing prohibitions and offences against unlawful access and data adequately protect privacy.
2. Do the existing prohibitions and offences against unlawful access to information and data adequately allow the pursuit of other objectives of societal benefit, e.g. cyber security of networks, online safety, scam protection/reduction?
No comment.
3. Are there any additional agencies you consider should have powers to access particular information and data to perform their functions? If so, which agencies, and why?
The provisions of part 2-5, chapter 2 of the TIA Act set out its legislative intention - to meet the investigative needs of agencies to undertake interception of telecommunications in investigating "serious offences". "Serious offences" include an offence punishable by imprisonment for life, or for a period, or maximum period, of at least 7 years, and include the serious loss to the revenue of the Commonwealth, State or Territory or bribery or corruption of an officer of the Commonwealth, State or Territory. It is well recognised that widespread use of encryption has caused the degradation of TI capacity under interception warrants issued under the TIA Act. The ability of all agencies to gather evidence relating to criminal and corrupt activity is being diminished through advances in communications technology. To exclude the anti-corruption Commissions from the TOLA Act effectively deprives us of the legislatively-sanctioned use of warranted interception under the TIA Act. That outcome is contrary to the intent of that Act and to the public interest in effective law enforcement.
4. Do you agree with the proposed considerations for determining whether additional agencies should be permitted to access peoples' information and data? Are there any additional considerations that have not been outlined above?
No comment.

Part 2: What information can be accessed?
5. Are there other kinds of information that should be captured by the new definition of 'communication'? If so, what are they?
No comment.
6. Are there other key concepts in the existing framework that require updating to improve clarity? If so, what are they?

The Commission requests that reform address inconsistencies in the key concepts of *law enforcement agency* and *interception agency* caused by the exclusion of agencies from some powers and not others.
7. How could the framework best account for emerging technologies, such as artificial intelligence and information derived from quantum computing?
No comment.
8. What kinds of information should be defined as 'content' information? What kinds of information should be defined as 'non-content' information? Is there a quantity at which non-content information becomes content information and what kinds of information would this apply to?
No comment.
9. Would adopting a definition of 'content' similar to the UK be appropriate, or have any other countries adopted definitions which achieve the desired outcome?
The Commission considers the UK definition of content an improvement on the current framework.
10. Are there benefits to distinguishing between different kinds of non-content information?
No comment.
11. Should the distinction between 'live' and 'stored' communications be maintained in the new framework?
The Commission considers a distinction between live and stored communications is no longer required and privacy considerations should be consistent.
12. Do each of these kinds of information involve the same intrusion into privacy? Or should the impact of each be considered differently?
As above.
13. What type of Australian communications providers should have obligations to protect and retain information, and comply with warrants, authorisations and assistance orders under the new framework?
In the Commission's view, all communications providers servicing Australian customers should have obligations to protect and retain information. Placing obligations only on Australian based communications providers disincentivises technology companies basing their centres within our jurisdiction.
14. What are your thoughts on the above proposed approach? In particular, how do you think the information captured by surveillance and tracking devices could be explained or defined?
The Commission considers the NSW Surveillance Devices framework is robust and should be considered in the reform of Commonwealth legislation.

Part 3: How can information be accessed?
15. How could the current warrant framework be simplified to reflect the functional equivalency of many of the existing warrants while ensuring appropriate privacy protections are maintained?
The Commission supports in principle, the proposed outcomes based approach .
16. What other options could be pursued to simplify the warrant framework for agencies and oversight bodies, while also enabling the framework to withstand rapid technological change?
The Commission supports the use of technology agnostic terminology to withstand rapid change.

Part 4: When will information be accessed?
17. Is it appropriate to harmonise legislative thresholds (as outlined above) for covert access to private communications, content data and surveillance information where existing warrants are functionally equivalent?
In the Commission's view, harmonising legislative thresholds will be advantageous.
18. Are there any other changes that should be made to the framework for accessing this type of data?
No comment.
19. What are your views on the proposed thresholds in relation to access to information about a person's location or movements?
No comment.
20. What are your views on the proposed framework requiring warrants and authorisations to be targeted at a person in the first instance (with exceptions for objects and premises where required)?
No comment.
21. Is the proposed additional warrant threshold for third parties appropriate?
No comment.
22. Is the proposed additional threshold for group warrants appropriate?
No comment.
23. What are your views on the above proposed approach? And are there any other matters that should be considered by an issuing authority when considering necessity and proportionality?
The Commission's investigative outcomes may be impacted if the threshold within the proposed approach is raised. The current threshold for the interception of communications (s 46 TIA Act) is where information derived "would be likely to assist in connection with the investigation by the agency of a serious offence…". The proposed threshold represents an increase, information is "likely to substantially assist" the agency in the investigation of an offence.
24. Should magistrates, judges and/or AAT members continue to issue warrants for law enforcement agencies seeking access to this information?
No comment.
25. What are your thoughts on the proposed principles-based, tiered approach to use and disclosure?
The Commission agrees that a principled based, tiered approach to use and disclosure is appropriate.
26. When should agencies be required to destroy information obtained under a warrant?
In the Commission's view, information should be destroyed when it is no longer required for permitted purpose and all avenues of appeal have been exhausted.
27. What are your thoughts on the proposed approach to emergency authorisations?
No comment.

Part 5: Safeguards and oversight
28. Are there any additional safeguards that should be considered in the new framework?

No comment.

29. Is there a need for statutory protections for legally privileged information (and possibly other sensitive information, such as health information)?

The Commission assesses existing protections for legally privileged information sufficient. No further statutory protections are required.

30. What are the expectations of the public and industry in relation to oversight of these powers, and how can a new oversight framework be designed to meet those expectations?

No comment.

31. What, if any, changes are required to the scope, role and powers of the Commonwealth Ombudsman to ensure effective oversight of law enforcement agencies' use of powers in the new framework?

No comment.

32. How could the new framework streamline the existing record-keeping and reporting obligations to ensure effective and meaningful oversight?

No comment.

33. Are there any additional reporting or record-keeping requirements should agencies have to improve transparency, accountability and oversight?

No comment.

Part 6: Working together: Industry and Government

34. How workable is the current framework for providers, including the ability to comply with Government requests?

No comment.

35. How could the new framework reduce the burden on industry while also ensuring agencies are able to effectively execute warrants to obtain electronic surveillance information?

No comment.

36. How could the new framework be designed to ensure that agencies and industry are able to work together in a more streamlined way?

It is the Commission's view that the framework should extend industry assistance in s 317B of the *Telecommunications Act 1997* to interception agencies as defined in the TIA Act. Industry assistance allows for agencies and industry to work in a more streamlined way.

Part 7: Interaction with existing and recent legislation and reviews

37. Do you have views on how the framework could best implement the recommendations of these reviews? In particular:
    a) What data generated by 'Internet of Things' and other devices should or should not be retained by providers?
    b) Are there additional records that agencies should be required to keep or matters that agencies should be required to report on in relation to data retention and to warrants obtained in relation to journalists or media organisations? How can any new reporting requirements be balanced against the need to ensure sensitive law enforcement or security investigations and capabilities are not compromised or revealed?

c) Is it appropriate that the Public Interest Advocate framework be expanded only in relation to journalists and media organisations? d) What would be the impact on reducing the number of officers who may be designated as 'authorised officers' for the purposes of authorising the disclosure of telecommunications data?
a) No comment. b) The Commission sees reporting requirements for Journalist Information Warrants already burdensome on agencies. No further records should be required. c) The Commission sees little value in expanding the PIA framework. d) In the Commission's view, chief officers are best positioned to determine 'authorised officers' within their organisation.