LECC
Law Enforcement
Conduct Commission

Submission to the Reform of Australia's Electronic Surveillance Framework

The Law Enforcement Conduct Commission

The Law Enforcement Conduct Commission (LECC) is a statutory agency established under section 17 of the *Law Enforcement Conduct Commission Act 2016* (NSW) for the oversight of law enforcement in New South Wales (NSW). The LECC commenced operations on 1 July 2017 and replaced the Police Integrity Commission (PIC), the Police Compliance Branch of the NSW Ombudsman's office and the Inspector of the Crime Commission.

The LECC is an independent body exercising the royal commission powers to detect, investigate and expose misconduct and maladministration within the NSW Police Force (NSWPF) and the NSW Crime Commission (NSWCC). The LECC also has the power to independently oversight and monitor the investigation of critical incidents by the NSWPF, if it decides that it is in the public interest to do so. Furthermore, the LECC oversees NSWPF and NSWCC investigations of alleged misconduct by officers of those agencies.

The LECC is declared as an "Agency" for the purposes of the *Telecommunications (Interception and Access) Act 1979 (Cth)* (TIA Act) allowing it to apply for, and be issued, telecommunications interception warrants. The LECC is also a criminal law enforcement agency for the purpose of the TIA Act allowing it to access telecommunications data in support of criminal investigations.

The LECC is a "law enforcement agency" for the purposes of the *Surveillance Devices Act 2004 (Cth)* allowing it to apply for, and be issued, surveillance device and computer access warrants. In addition, the LECC is able to apply for and be issued with surveillance device warrants under the *Surveillance Devices Act 2007 (NSW).*

Not only does the LECC rely heavily on Australia's electronic surveillance framework to gather evidence for the investigation of serious offences, it also oversights law enforcement agencies deploying such powers in NSW. As such, the LECC is able to provide comment from both an operational and an integrity perspective. We would like to thank the Department of Home Affairs (the Department) for considering the LECC's input for these important reforms.

Introduction

The LECC is fully supportive of reform to Australia's electronic surveillance framework and agrees with the guiding principles for reform as stipulated in the discussion paper. Additionally, the LECC is supportive of the "future state" positions proposed throughout the discussion paper.

The LECC has reviewed the paper and respectfully submits responses to each question posed below. In addition, the LECC would like to highlight significant issues for the Department's attention and reform considerations.

Significant Issues

The LECC would like to highlight three significant issues to be considered within the reform process:

- The need for emergency use and disclosure powers to protect life, health and safety
- The proposed transfer of certain electronic surveillance oversight powers and responsibility from the state to the Commonwealth
- The exclusion of integrity agencies from Schedule 1 Powers within the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA)*

The need for emergency use and disclosure powers to protect life, health and safety

The LECC acknowledges the paper's intent to include life, health and safety as a secondary permitted purpose. The LECC wishes to reinforce the importance of this concept as currently, in certain circumstances, it is unlawful for integrity agencies to use or disclose telecommunications interception content for this purpose.

The proposed transfer of certain electronic surveillance oversight powers and responsibility from the state to the Commonwealth

Part 5 of the discussion paper articulates the current state of oversight arrangements in which Commonwealth, state and territory agencies have responsibility for the oversight of different aspects of electronic surveillance.

Part 5 of the discussion paper then states that "the Government is considering the scope and role of the Commonwealth Ombudsman, including whether the Commonwealth Ombudsman should assume greater responsibility for law enforcement agencies. This would involve the Commonwealth Ombudsman overseeing all Commonwealth, state and territory law enforcement agencies' use of electronic surveillance powers under the new framework."

The LECC would propose that the government should consider the strengths of the oversight regime within the current framework. There are strong advantages in a federated system of oversight as it can provide multiple layers of assurance to the public. The current framework incorporates a federated approach to oversight where Commonwealth, state and territory agencies have responsibility for the oversight of different aspects of electronic surveillance. Whilst oversight is dictated by the legislative instrument, multiple oversight agencies allow for innovative approaches which ultimately result in better compliance by the agencies. The LECC is better able to maintain rigorous compliance across all electronic surveillance activity by undergoing inspections from both state and federal oversight agencies and implementing procedural changes on their advice.

In the state of NSW, the oversight of telecommunication records by the Office of the LECC Inspector is intrinsically tied to the use of surveillance devices and controlled operations under state legislation. These powers are often exercised simultaneously by NSW law enforcement agencies. It is more effective to oversight these particular powers holistically within the same inspection regime. If telecommunications interception oversight was divulged to the Commonwealth, the oversight of these powers would be fragmented.

The exclusion of integrity agencies from TOLA

The paper states:

> *The current reform project will not revisit the outcome of such inquiries. Rather, developing the new electronic surveillance framework will allow the Government to work closely with affected stakeholders to appropriately implement the Government's response to those reviews, while ensuring they are consistent with the principles and thresholds outlined in this paper.*

Whilst the LECC understands that the proposed integration of multiple legislative review processes into this reform process is an effective method to ensure cohesion of the eventual legislative framework, the LECC strongly advocates for an amendment to TOLA to proceed independent of these reforms.

The LECC has submitted two independent and one co-signed joint submissions to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in support of the Committee's review of the TOLA legislation. In addition, the LECC has provided a joint submission to the Independent National Legislation Security Monitor (INSLM) in support of their review of the legislation.

Both the PJCIS and the INSLM have publically recommended that integrity agencies be included in Schedule 1 Powers of the legislation as was originally drafted. Whilst amended legislation was drafted and presented to parliament, this Bill lapsed when parliament was prorogued for the 2019 federal election. It has been over three years since the TOLA legislation was passed and despite both the PJCIS and INSLM recommending that integrity agencies be re-included, the government has yet to introduce legislative amendments.

As with other interception agencies, the LECC has been heavily impacted by encryption with well over 90% of intercepted IP communications now being encrypted. In addition, the LECC's evidence gathering through digital forensic activity has also been impacted through encryption and other security measures. The use of Schedule 1 Powers within TOLA assists agencies with the investigation of serious offences. The LECC investigates serious offences by police officers. Criminal offending by police officers has a greater impact on society. Corruption and misconduct by police officers compromises the confidence the public has in fairness, integrity and honesty in all police officers. Mistrust of police has detrimental effects on policing, as public involvement is a crucial element of law enforcement. Police often rely on members of the public to report and assist in investigations.

For the reasons stated above, the LECC strongly advocates for the inclusion of integrity agencies in Schedule 1 Powers of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA)* as soon as practicable, and independent of this reform process.

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?**
    a. **If so, which aspects are working well?**
    b. **If not, which aspects are not working well and how could the new prohibition and/or offences be crafted to ensure that information and data is adequately protected?**

    The LECC is not currently impacted by the current prohibitions and has no further comment.

2. **Do the existing prohibitions and offences against unlawful access to information and data adequately allow the pursuit of other objectives, e.g. cyber security of networks, online safety or scam protection/reduction?**

    The LECC is not currently impacted by the current prohibitions and has no further comment.

3. **Are there any additional agencies that should have powers to access particular information and data to perform their functions? If so, which agencies, and why?**

    The LECC has no objection, in principle, to the extension of powers to the agencies and circumstances indicted within this section of the discussion paper. Given the functions of the named agencies, it would seem a useful investigative tool.

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?**

    The LECC believes the considerations outlined in the discussion paper are comprehensive and appropriate to consider agency powers.

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?**

    The LECC has no further suggestions beyond what is described in the discussion paper.

6. **Are there other key concepts in the existing framework that require updating to improve clarity? If so, what are they?**

    If the concept of the telecommunications network is retained for access to certain types of telecommunications, then the LECC would suggest a better definition around this term including clarity around public Wi-Fi networks.

7. **How could the framework best account for emerging technologies, such as artificial intelligence and information derived from quantum computing?**

    Where emerging technologies can be used to communicate, the legislation should be technically agnostic as to allow their evidentiary capture. Beyond that, the LECC has no comment regarding specific technology.

8. **What kinds of information should be defined as 'content' information? What kinds of information should be defined as 'non-content' information?**

   The LECC would concur that a definition of content would be appropriate.

   The LECC would consider a simplistic definition similar to the broad description within this discussion paper as appropriate.

   Similarly, the broad description of 'non-content' within the discussion paper (being information about a communication) should be defined within the Act.

   The LECC does not agree that a URL on its own should be defined as content. The LECC would consider that a URL is not a form of content, but rather address information to the location of content. It would therefore be incorrect to expand the definition of content to include certain categories of non-content data and may cause difficulties in interpreting the legislation.

   The LECC does recognise, however, that URLs may provide the ability to replicate or provide an understanding of the content accessed. However, the Act should deal with this from an access or thr eshold perspective which is consistent with the concept of defining non-content subsets as per the UK model.

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 LECC would view the UK definition of 'content' as overly complex and would prefer a more technical definition. It would be possible to use 'non-content' data to create a form of communication thus turning it into content by using 'non-content' data as code or signals.

10. **Are there benefits to distinguishing between different kinds of non-content information? Are there particular kinds of non-content information that are more or less sensitive than others?**

    Yes. The LECC recognises that the privacy implications associated with entity and event data, as per the UK model, greatly differ. As such, defining subsets of non-content data could allow more appropriate flexibility and fairness by applying different access mechanisms and thresholds. There is a significant difference in the interference with privacy when requesting, for example, the subscriber of a service (entity data) which is information historically available in telephone directories and the detail of specific communications (event data) which would typically be provided privately within a person's telephone bill.

    Currently access mechanisms within the TIA Act do not distinguish between the two. Whilst simplicity is preferred, the requirements under s180F and subsequent oversight expectations are not proportionate to appropriate privacy protection for access to entity data. The LECC would propose that better public value could be achieved by concentrating privacy considerations on the authorisations of event data.

11. **Should the distinction between 'live' and 'stored' communications be maintained in the new framework?**

    The LECC does not support the distinction between 'live' and 'stored' communications being maintained within the new framework. Currently, the distinction causes overly complex legislation and access regimes.

12. **Do each of these kinds of information involve the same intrusion into privacy? Or should the impact of each be considered differently?**

    In the modern telecommunications environment and the way communications technologies have been embraced, there is little or no difference to the intrusion of privacy.

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?**

    The LECC would propose that providers captured under the designated communication provider definition would be appropriate for warrants, authorisations and assistance orders under the new framework. Reasonable protections for small providers could be considered, which may involve exemptions for

information retention and/or interception capability systems.

14. **What are your thoughts on the above proposed approach? And in particular, how do you think the information captured by surveillance and tracking devices could be explained or defined?**

In principle, the LECC supports the proposed approach to define types of information for appropriate warrants or authorisations. This could potentially reduce complexity of the Act and better align warrant considerations to interference of privacy. It could also provide multiple operational solutions for the sought information dependant on the operational environment, which may change during the period of the warrant.

Information captured by surveillance and tracking devices could be defined simplistically using principles such as:

- Public activity/private activity
- Location information
- Private communication/public communication
- Electronic communication/electronic information

Legislative clarity would be necessary relating to public and private activity.

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 protections are maintained?**

The LECC agrees in principle with the proposed outcomes based approach as outlined in the discussion paper. The LECC agrees that authorising access to the type of information, as opposed to the access method, would achieve simplification of the warrant framework. In addition, the proposed approach would also reflect the functional equivalency of warrants and allow more effective assessment of the interference with privacy.

The new framework needs to be carefully worded to avoid the following risks:

- An unintended outcome of warrant applications requiring overly complex technical explanations
- Warrant applications requiring complex explanations of techniques and systems
- A requirement for an issuing authority to consider privacy implications where some of the information is not known. For example, the type or volume of information being accessed may not be known because it is intrinsic to the individual(s) behaviour

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?**

Rapid changes to technology are likely to impact electronic information/communications. Types of electronic information (including communications, metadata, files, text, symbols, audio, media content, identification information etc.) may be difficult to categorise definitively as technology evolves. In addition, accessing subsets of electronic information and excluding others is likely to become more technologically difficult. A simplified warrant framework able to withstand rapid technological change should authorise access to broad categories of electronic information.

The current ability to authorise multiple services under a named person warrant including the ability to add services within the warrant period has provided significant simplification of the current warrant framework. A similar principle should transition to the new framework. Where an information based warrant is in place based on anticipated access methods within the warrant application, the warrant should also authorise newly identified sources of the same type of information including non-significant modification of the access method.

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?**

Yes, it simplifies the regime. The LECC considers, however that the proposed legal threshold to be issued with a warrant of "likely to substantially assist" would be exceptionally difficult to substantiate within a warrant application in most instances. There is often unknown factors which may be behavioural or specific to service usage which cannot be established pre-warrant.

18. **Are there any other changes that should be made to the framework for accessing this type of data?**

The authorisation of entity data could differ from the authorisation requirements to event data as per response to Question 10. Some of the record keeping requirements should be simplified where there is little or no accountability gains.

19. **What are your views on the proposed thresholds in relation to access to information about a person's location or movements?**

The LECC supports the principles proposed in the discussion paper. The LECC concurs that there is greatly reduced interference in privacy for location information as opposed to more intrusive surveillance devices. The ability to internally authorise certain tracking devices, in addition to being able to include such authorisations within a warrant, would provide an effective operational environment proportionate to the interference of privacy.

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)?**

In principle, the LECC is supportive of targeting criminal activity by a particular person. The legislation needs to contain sufficient flexibility however for the technical practicalities of evidence collection which involves deploying methods external to the person.

21. **Is the proposed additional warrant threshold for third parties appropriate?**

An issuing authority in the current regime must consider the interference of privacy when authorising a third party warrant. The LECC is not opposed to additional mechanisms to assist an issuing authority in making that decision.

22. **Is the proposed additional threshold for group warrants appropriate?**

It would be important to restrict warrants to specific criminal activity to ensure that evidence collection remains targeted.

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 considerations proposed in this section currently exist in the current regime. The issuing authority is able to scrutinise these issues.

If a key objective of the new regime is reduce complexity, then the proposed reforms within this section may be counterproductive. The majority of these considerations are currently considered by issuing authorities and clear legislative guidance is given via thresholds. The LECC does not see the value in complicating this aspect of the legislation.

24. **Should magistrates, judges and/or AAT members continue to issue warrants for law enforcement agencies seeking access to this information?**

Yes, any restrictions to the current lists may produce resourcing issues within the justice system.

25. **What are your thoughts on the proposed principles-based, tiered approach to use and disclosure?**

The LECC supports the proposed principle-based, tiered approach to use and disclosure.

The LECC specifically supports a secondary disclosure for the prevention of a serious risk to life, health and safety. Within the current regime, it is unlawful in certain circumstances for the LECC to disclose information for this purpose. This is a significant deficiency within the current legislation.

26. **When should agencies be required to destroy information obtained under a warrant?**

In principle, content should be destroyed where a criminal investigative or judicial purpose ceases to exist.

The destruction requirements relating to restricted records provide technical practicality to the destruction regime. Destruction requirements as they apply to protected information for stored communications content are problematic. Evidence is often used in various aspects of an investigation. In many instances, information is used within various investigative reports and records which are covered by state destruction requirements. It is impractical to track specific information across all records of an investigation for destructive purposes. In essence, the collected evidence can be, and should be, destroyed as soon as practicable. However, information derived from such evidence is very difficult to track for destruction purposes.

27. **What are your thoughts on the proposed approach to emergency authorisations?**

The LECC supports the proposed approach as outlined in the paper.

28. **Are there any additional safeguards that should be considered in the new framework?**

The proposed framework would provide a comprehensive system of safeguards.

PART 5: SAFEGUARDS AND OVERSIGHT

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

The LECC currently restricts access to electronic surveillance information to a small number of investigative staff. This includes further restrictions for certain information including legal professional privilege. The application of legislative restrictions would be difficult to define and effectively apply given the nature of electronic surveillance product.

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

The use of electronic surveillance powers is vitally important in the investigation of criminal offences, however, the use inevitably results in significant interference of privacy for the targeted suspects. As such, the public should expect that there is no tolerance for intentional misuse of these powers. In addition, the public should expect that a rigorous governance and oversight framework is in place to significantly reduce any risks of human or system errors which may result in unintentional breaches of privacy.

A new oversight framework would better meet those expectations by focusing less on prescriptive record-keeping requirements and focusing more on the operational deployment of powers. The review of key records is a fundamental requirement to verify warrants are applied for, issued and complied with. The current regime requires an extraneous amount of additional records be produced and maintained by agencies. The current oversight framework significantly focuses on the inspection of these records, providing a diminished public value in compliance.

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?**

The LECC currently supports a federated model of oversight for the future electronic surveillance regime. The federated model has worked extremely well for the deployment of telecommunications interception. Please refer to previous comments in response.

The role and scope of oversight bodies in the new framework should shift from a record-keeping focus to a less prescriptive regime which includes an overview of operational deployment of powers. A more productive regime would also include the ability to live monitor operational activity as opposed to inspecting records created over a year ago.

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

The record-keeping and reporting requirements within the existing electronic surveillance framework is complex and prescriptive. The practical application of the framework and the expectations of oversight bodies, however, add a further layer of complexity around what records are required and the specific format and content of each record. Subsequently, to properly understand and streamline record-keeping for a new framework, it would be important to engage subject matter experts from within the compliance departments of agencies and representatives from the oversight agencies such as the Commonwealth Ombudsman. By doing so, the public value of current record-keeping and reporting requirements could be properly assessed before designing the new governance framework.

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

The LECC believes that the record-keeping and reporting requirements could be completely redesigned with the goal of providing more meaningful public information. The LECC would welcome input into this process.

PART 6: WORKING TOGETHER: INDUSTRY AND GOVERNMENT

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

The LECC works closely with the major Australian telecommunications carriers when executing warrants and authorisations. The assistance received from these carriers is professional and of high technical standard. The LECC is, however, unable to comment on the challenges that carriers or other providers face within the current framework.

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?**

As per Question 34, the LECC is unable to provide comment relating to the burden experienced by industry.

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

The LECC has expressed through multiple submissions to government that it could work in a more streamlined way with industry assistance through inclusion within the Schedule 1 Powers of TOLA. Please refer to previous comment.

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?

As a small agency, the LECC's investigative interest is currently limited to data generated by devices which have an alignment to electronic surveillance.

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?

The LECC has not applied for a journalist information warrant to date and is therefore, not able to provide informed comment relating to this type of record-keeping. Sensitive law enforcement investigations are critical and may be affected by public reporting. There may be scope to delay reporting in some instances until certain investigations are at overt stages without limiting oversight of these investigations.

c. Is it appropriate that the Public Interest Advocate framework is expanded only in relation to journalists and media organisations?

The LECC does not see a need to expand the Public Interest Advocate framework.

d. What would be the impact on reducing the number of officers who may be designated as 'authorised officers' for the purpose of authorising the disclosure of telecommunications data?

Depending on the type of reduction, this may have a substantial impact on senior officer resources for all agencies. The LECC would support a reduction if the resource impact were to be offset by the authorisation requirements of entity data as discussed above.