NSW Government Submission

Australian Government's Reform of Australia's Electronic Surveillance Framework Discussion Paper

3 March 2022

Contents

Introduction

The NSW Government welcomes the opportunity to provide feedback on the Reform of Australia's Electronic Surveillance Framework Discussion Paper and looks forward to continued engagement with the Australian Government on this important issue, particularly with the release of the exposure draft legislation later this year.

The NSW Government Submission includes feedback from a number of NSW Government agencies (noted below) and is organised around the questions listed in the Discussion Paper, followed by additional comments.

General comments

While NSW welcomes opportunities to improve and streamline aspects of electronic surveillance mechanisms, it is NSW's position that existing capacities to undertake operational activities be maintained under the new model, and not be diluted. This is of particular importance in the case of monitoring and intercepting telecommunications for law enforcement purposes. NSW looks forward to continued discussion with the Australian Government on operational, as well as legislative and policy alignment.

NSW notes that at this stage, the exact mechanism proposed for the reform, and interactions with existing NSW legislation, remain unclear. For all matters impacting legislation and key functions that require ministerial and Cabinet-level consideration, NSW notes the Australian Government should engage with jurisdictions through relevant ministers, either directly or through ministerial forums like Meetings of Attorneys General.

Contributing NSW Government agencies
NSW Department of Premier and Cabinet (DPC)
NSW Police Force (NSWPF)
NSW Department of Communities and Justice (including Corrective Services NSW) (DCJ)
NSW Crime Commission
NSW Department of Customer Service (DCS)

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?

Current NSW legislation has provisions explicitly relating to the protection of privacy. For example, s19(2) *Surveillance Devices Act 2007* (NSW) (NSW SD Act) states "*the extent to which the privacy of any person is likely to be affected*". New South Wales Police Force (NSWPF) submits that this provision adequately protects individuals' privacy by ensuring the police officer considers alternative means to obtain the information, as well as the privacy impacts of the target and third parties against the utility and necessity of the warrant. NSWPF supports forms of digital consent implemented by industry and required by users of applications that track someone's geolocation.

The NSW Crime Commission supports, conceptually, attempts to achieve consistency across State and Commonwealth Surveillance Device legislation, but considers that further discussion at the ministerial level would be required.

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?

Nil 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?

Emerging legislation and legislative amendments in the electronic surveillance space have afforded powers to some agencies and not others, creating significant disparity between interception agencies with similar functions to investigate serious crime. The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA Act) and *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (SLAID Act) exemplify this disparity, the former not proposed to be extended to investigative Commissions and integrity agencies and the latter only affording powers to Commonwealth agencies, but not their state-based equivalents. TOLA was originally proposed to be extended, with legislation to do so being drafted but was never enacted. The NSW Crime Commission targets sophisticated criminals who are well versed in traditional law enforcement investigative techniques. Without access to powers required to properly investigate emerging criminal threats, the NSW Crime Commission simply cannot achieve its functions effectively.

NSW Department of Communities and Justice (DCJ) notes and recommends the implementation of Recommendation 78 of the Richardson review to the new legal framework. The Recommendation proposes corrective services authorities should be granted power to access telecommunications data if the state or territory government considers it to be necessary. Implementing this Recommendation into the framework will assist protecting correctional centre security as well as the monitoring of criminal offenders in custody and in the community. The review observed that corrective services agencies play a frontline role, not only in managing offenders in custody, but also in contributing to the detection and prevention of serious and organised crime at a local, state and national level. The review noted statistics about Corrective Services NSW's (CSNSW's) and

Corrections Victoria's use of telecommunications data from 2010-2015, which indicated that the power was heavily relied on in criminal investigations.

DCJ submits that the new legal framework for electronic surveillance should implement the Richardson review's recommendation by giving corrective services agencies powers to access telecommunications data for the purposes of monitoring criminal offenders in custody and in the community and protecting correctional centre security.

The Richardson review noted that, before the introduction of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) (2015 Amendment Act), corrective services agencies were permitted to access telecommunications data, as they fell within the definition of an 'enforcement agency' under the *Telecommunications (Interception and Access) Act 1979* (Cth) (Commonwealth TIA Act) responsible for enforcing the criminal law. The introduction of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) limited access to telecommunications data to a smaller range of law enforcement agencies, which did not include corrective services agencies. This meant that corrective services agencies could no longer access, use, store or share telecommunications information. Other law enforcement agencies could not share telecommunications data they obtained under the Commonwealth TIA Act with corrective services agencies.

Corrective Services NSW (CSNSW) is concerned that the consolidation of the legislation may impact its existing capacity to lawfully monitor and intercept telecommunications for law enforcement purposes. CSNSW emphasises that any existing capacity to undertake these activities be maintained in full in the new Act, and not be diluted. CSNSW's capacity to monitor and intercept telecommunications, including via its own Offender Telephone System, is essential to maintaining the good order and security of the correctional system, and in disrupting criminal activity which threatens the safety of the community.

In particular, when preparing new legislation, careful consideration should be given to the role of existing definitions in the *Telecommunications (Interception and Access) Act 1979* (Cth) (Commonwealth TIA Act), such as 'enforcement agency' and carriage service provider'. These definitions play a key role in conferring capabilities on CSNSW and other law enforcement agencies. Any change in, or addition to, definitions relating to telecommunications service providers, or lawful reasons for agencies to interact with telecommunications information, must account for the very specific and significant role that agencies., including CSNSW, undertakes in enforcing the criminal law. Traditionally, the work undertaken by CSNSW in this regard supports the management of offenders in custody and in the community, and does not always result in the laying of charges or the prosecution of individuals for offences. The capacity for CSNSW to continue to undertake its activities for investigative and intelligence-collection purposes must not be disrupted by any proposed changes to the legislation.

See Annexure A for further information.

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 NSW Government supports the considerations outlined in the discussion paper. Additional considerations, not outlined above, could include:

- Whether the agency has met particular offence thresholds for use of devices to access information and data. Thresholds will need to be defined in the legislation, to ensure there is a consistent standard

- Whether an agency with the powers to access certain information would be able to lawfully share it with officers of an agency who ordinarily do not have these powers. The NSW Crime Commission operates as part of joint investigations and taskforce arrangements with other law enforcement and regulatory agencies and the current information sharing provisions are complex. Specifically, the NSW Crime Commission routinely works in partnership with the Australian Transaction Reports and Analysis Centre (AUSTRAC), the Australian Tax Office (ATO), Australian Border Force (ABF) and CSNSW and it would be advantageous to be able to share electronic surveillance content and / or data with these agencies. The NSW Crime Commission supports a streamlined, principals-based approach to sharing of information.

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 definition for 'communication' is outdated and requires clarification. Consideration should be given to all hybrid elements of data, including data held on storage devices, real-time data in motion and cloud storage, as well as other signals like sign languages (e.g. AUSLAN).

Consideration should also be given to 'Internet of Things', the collective network of connected devices and the technology that facilitates communication between each of these devices and between the devices and the cloud. For example, vehicle telecommunication modules or 'Black Box Event' recorders. At this stage it is unclear whether they will just be static recorders or if they will transmit data back to the manufacturer.

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

Many of the current challenges relevant to the existing framework relate to the difficulty in obtaining data or communications from providers who are non-traditional and therefore potentially fall outside the definition of carrier service provider. It is crucial that any new or revised framework incorporates a concept of 'carriage service provider' which effectively captures the full range of entities involved in the communications process. For example, clarity around the access and ownership of data stored on Cloud services could be improved.

See Annexure A for further information.

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

NSW supports a technology-neutral and a 'technology agnostic' approach focused on targeting types of information sought to obtain rather than the technology used to obtain the information.

Importantly, the issue exemplifies the critical nature of having all persons being able to understand the legislation, its purpose and limitations. References to complex technologies in detail that would be unintelligible to legal and investigative staff would be ineffective. It is also important that the framework acts as a facilitator for industry to agency (or agency to agency) collaboration and information sharing. It is only through the sharing of knowledge and expertise that best practice can be established with regards to the ongoing challenges inherent in emerging technologies.

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?

NSW supports unambiguous definitions for 'content' and 'non-content' data.

The NSW Crime Commission notes recent Commonwealth Ombudsman inspections of the agency's telecommunications data have identified challenges in distinguishing between content and non-content information. NSWPF is cognisant of ensuring a broad enough, technology-neutral definition to ensure the evolution of technology doesn't render definitions outdated.

The NSW Crime Commission supports submissions to expressly permit non-content Interception Related Information (IRI) or Call Associated Data (CAD) to be delivered in conjunction with a lawful interception under a warrant.

See Annexure A for further information.

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 UK definition of 'content' focusing on the meaning of the communication is useful and appropriate. NSW supports a variation of the UK definition in-principle as long as it is specific enough to ensure 'non-content' is not captured unintentionally.

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?

NSW does not see benefit from distinguishing between types of 'non-content' information.

Different levels of authorisations to cover different types of non-content information would be particularly onerous and could also duplicate work. A requesting officer might require two different authorisations to permit access to the same material currently obtained under one which detracts from the overall purpose of the reform focusing on the person and their criminality, not the technological means through which they undertake such activities.

See Annexure A for further information.

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

There is a distinction between 'live' and 'stored' communications as it relates to an individual's privacy expectations. Compared to 'live' communication, a person would likely have a greater expectation that a 'stored' communication would be retained, either with the Carrier, application provider or on the handset of the intended recipient.

However, it should be noted that the distinction between 'live' and 'stored' communications is becoming blurred by new types of communication that are not just permanent or temporary, but also semi-permanent. Consider evolving technology such as speech-to-text messages, automatically disappearing messages, an over the top (OTT) application which deletes automatically at a set point in time dependent on user preferences, an Instagram story or a Snapchat. These semi-permanent communications may be live when initially recorded and stored for a limited period before being set for removal. In such semi-permanent communications, the premise that the communication would be more 'considered' and less spontaneous than a live communication such as a phone call, as suggested on p26 of the Discussion Paper, no longer holds.

The privacy impact is just as significant for both 'live' and 'stored' communications. However, if the proposal is to remove the distinction between live and stored communications and the threshold is harmonised between interception and stored communications, consideration should be given to ensure access does not become more difficult for investigators.

See Annexure A for further information.

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

See response to question 11.

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?

All Carriers, carriage service providers (CSPs), email, Cloud Storage and OTT application providers that offer services to Australian users should be captured under a warrant or authorisation framework. This includes foreign owned entities, such as Google, Microsoft, Facebook and other entities whose purpose is to facilitate communications, particularly if these providers have storage infrastructure in Australia. It is important that the new framework explicitly addresses the question of whether law enforcement agencies are even permitted to request the information from these foreign providers.

See Annexure A for further information.

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?

A tracking device authorisation should be technology-neutral to allow for new technologies as they appear on the market. To avoid ambiguity, a practical approach would be to regulate the type of information being obtained rather than the kind of device used to target the information.

See Annexure A for further information.

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?

NSW supports attempts to simplify the current warrant framework to streamline processes. NSWPF suggests that a cascading warrant framework could be implemented. For example, if a warrant is obtained that authorises a high level of intrusiveness or significant privacy implications, then the framework would provide that lower threshold law enforcement activities (which would usually be granted under a separate lower threshold warrant) would also be allowed. This approach will eliminate the unnecessary and administrative burden in obtaining a lower threshold warrant.

In addition, the NSW Crime Commission notes agencies currently may be required to seek a telecommunications interception warrant, a stored communications warrant, a surveillance devices warrant and a controlled operation in order to access particular types of information which have functional equivalency. If the definition of the 'serious offence' / 'relevant offence' etc. is consistent, this would simplify the functional equivalency and therefore reduce administrative burdens. The product use provisions could reflect the intended limitations depending on the manner by which the product was derived.

See Annexure A for further information.

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 NSW Crime Commission notes use provisions may be simplified for agencies and oversight bodies while also being resilient to technological change.

In order to reduce the administrative burden on agencies and oversight bodies, consideration should also be given to the ways in which warrants are sought to ensure that these procedures can survive technological change and accommodate organisational realities in an increasingly dynamic environment. Specifically, consideration should be given to the legislation expressly addressing (and allowing) authorisation by electronic means, such as a warrant issued via a digital platform (e.g., Dekko). The legislation should make clear that electronic authorisation of warrants and datasets, electronic file management and electronic inspection is acceptable. Any references in the legislative framework to ink signatures should be removed and it should be made abundantly clear that signatures include digital signatures. Provision should be made for the destruction of physical files in favour of electronic originals.

The number of steps currently required to obtain a warrant, use the material in evidence and report on its use and effectiveness are substantial and should be streamlined. For example, the current process in obtaining evidentiary certificates for warrants and data authorisations could be made redundant if the certificate, or a version of it, was issued as a matter of course at the time the warrant or authorisation request was actioned.

See Annexure A for further information.

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?

NSWPF notes it is appropriate to harmonise legislative thresholds. However, the threshold should be set based on the investigation of an indictable offence, or at the '3-year offence' level currently adopted by most Commonwealth legislation, rather than the proposed '5-year offence'. This would ensure serious offences such as 'use of a carriage service to menace/harass/offend', being a precursor to many domestic violence offences, are covered by the legislation. Further, NSW surveillance device legislation allows for a warrant to be obtained to assist in the investigation of any indictable offence.

The NSW Crime Commission notes that consideration should be given to the anticipated impact of the proposed changes on the surveillance device requirements, given the NSW SDA shadows the *Surveillance Devices Act 2004* (Cth) (Commonwealth SDA).

See Annexure A for further information.

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

The NSW Crime Commission strongly opposes additional reporting and record-keeping requirements to bolster transparency on the basis that the 2015 metadata amendments already additionally created significant oversight and reporting obligations that did not previously exist,

although access to that data, if accessible (accepting it was not required to be retained by the carriers) was available to law enforcement agencies prior to such amendments. Further, expanding the role of the Public Interest Monitor (PIM) will inevitably increase costs and delay for law enforcement agencies, which would require significant justification.

See Annexure A for further information.

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

NSWPF supports in-principle the proposed thresholds.

The NSW Crime Commission cannot currently use a tracking device without a warrant and does not currently have any internal authorisation to use such devices. The NSW Crime Commission welcomes proposals to allow for tracking to take place pursuant to an authorisation rather than a warrant and considers the proposed threshold of an offence punishable by a maximum period of three years to be appropriate.

See Annexure A for further information.

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)?

The NSW Crime Commission considers this proposal to be appropriate in the Commonwealth TIA Act context, but it could pose a real problem in the SD context, if the changes affected State laws, and depending on the proposed exceptions.

Specifically, limiting applications to be referable to persons at first instance, and by exception objects or premises, seems to exclude the other options currently permitted under State SD legislation (vehicle, about the bodyof a person who is not involved in the offence).

See Annexure A for further information.

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

As per the response to question 20 above, this may have an impact on the NSW Crime Commission in relation to surveillance devices, if the State law is affected. It could be managed, but clearly creates additional legislative hurdles in seeking a warrant.

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

Proposed additional thresholds for group warrants are likely to create additional burden on law enforcement, but are appropriate due to the potential of targeting multiple people under one warrant.

See Annexure A for further information.

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 Discussion Paper notes that current federal legislation does not include a clear requirement that powers only be used where necessary and proportionate and undertakes to consider how best to incorporate a clear, express requirement to that effect in the new framework. DCJ recommends that the review have closer regard to the authorisation test provided in the Commonwealth SDA, which is mirrored in the NSW SDA, and which, in the view of DCJ, provides a useful platform for the establishment of a clear and consistent authorisation test.

The authorisation framework for the reform regime that is discussed in the Discussion Paper and in Richardson review report divides the authorisation decision making process into two stages. Firstly, there are threshold legal tests. These require the issuing authority to be satisfied of specified matters. If satisfied of these matters, the issuing officer may proceed to the second stage, which is to assess whether s/he should exercise their discretion to issue the warrant. The officer is guided in this second stage determination by specified mandatory considerations.

The Commonwealth SDA and the NSW SDA are structured so that they deal with the issue of necessity in the first stage. Only if the issuing officer is satisfied that necessity requirements are met, does the officer move on to consider the issue of proportionality in the guided exercise of his or her discretion.

The key threshold test, incorporating the requirement of necessity, is established in the Commonwealth SDA by section 14(1).

Section 16(1) cements the threshold test by providing that the issuing authority:

"***may*** *issue a surveillance device warrant if satisfied … that there are reasonable grounds for the suspicion founding the application for the warrant*" [emphasis added].

The use of the word *"may*" leads to the second stage issue of whether the officer exercises his or her discretion to issue. The exercise of the officer's discretion is guided by section 16(2), which specifies mandatory considerations that the officer must have regard to.

DCJ considers that this delineated approach, dealing with necessity and proportionality distinctly, with necessity being a prerequisite to consideration of proportionality, would provide a clear and balanced test that promotes explicit, consistent and appropriate application of necessity and proportionality principles. In addition, by mirroring the approach taken in the Commonwealth SDA, which is based on uniform model SDA legislation that has been adopted by jurisdictions, the new Act will harmonise with the existing national approach to issuing warrants for surveillance devices.

The reform should avoid a test that blurs consideration of the concepts of necessity and proportionality. An example of this is the threshold posed on page 40 of the Discussion Paper that the issuing officer be satisfied: "*the exercise of powers under the warrant is likely to substantially assist the agency in the investigation of the offence*". This can militate away from the issue of necessity.

In the circumstances of a very serious offence, such as murder or kidnapping, the use of a surveillance device may not be *likely to substantially assist … the investigation of the offence*, however, in the context of the gravity of the circumstances use of a surveillance device must necessarily be attempted. The issue of whether use is likely to assist the investigation may usefully be incorporated into the second stage of the test, affecting the issue of proportionality, but its inclusion in the initial threshold stage is inappropriate and may have significant adverse operational implications.

The NSW Crime Commission welcomes the proposed "necessity and proportionality test" but considers that it may create issues for repeat interception. It seems common that 'renewal' interception is often most useful for the associated data that comes with it. In such cases, it would be difficult to prove that the benefit to the investigation of intercepting a person's private conversations, which primarily do not relate to the commission of the investigated offence, outweighs the intrusion on that person's privacy, when there are other options available to the NSW Crime Commission that are less intrusive, such as s.180 Commonwealth TIA Act.

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

NSW is supportive of requiring authorisation by an appropriate independent authority. However, currently, law enforcement agencies are not permitted to access the delegations of nominated AAT members, on the basis of their personal privacy. As such, agencies are unable to check that the members hold the appropriate authority to issue warrants before they do so. Historically, the NSW Crime Commission used to receive copies of the declarations made by the Attorney General for NSW, of the persons who were made eligible Judges under subs. 5 (3) NSW SDA.

See Annexure A for further information.

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

In any re-drafted legislation, NSWPF suggests the inclusion of a general disclosure provision permitting the use or communication of intercepted or accessed information where the disclosure is necessary to prevent serious injury or death to a person, or serious damage to property belonging to any person. In this respect, consideration should also be given to the exigent nature of the circumstances.

The NSW Crime Commission welcomes the proposed approach to disclosure for a permitted purpose rather than nominating acceptable recipients. The NSW Crime Commission considers that this will assist in addressing the current challenges associated with sharing electronic surveillance material as part of multiagency taskforces and joint investigations.

See Annexure A for further information.

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

When it is no longer required for the purpose for which it was obtained or in the exercise of the Agency's functions and powers and after it is no longer required for oversight purposes, and or when the information is no longer considered a *State record* for the purposes of the *State Records Act 1998*.

Regarding the destruction of documents, the expression 'not likely to be required' is open to interpretation. NSWPF suggests providing additional clarification on how this is to be interpreted in the legislation.

While the Discussion Paper repeatedly references concerns about privacy, if the privacy impost has already occurred via the collection and review of the private information, the NSW Crime Commission does not consider that the length of time that the material is retained has an impact on the privacy if it can only be used in appropriate circumstances.

Many investigations conducted by the NSW Crime Commission jointly with its partner agencies are extremely protracted, with prosecutions and appeals extending for years or even decades. Any legislation regarding the destruction of information obtained under a warrant must contemplate these delays.

See Annexure A for further information.

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

NSWPF is supportive of the proposed approach to emergency authorisations. Consideration should be given to:

- allowing a commissioned police officer[1] to approve an interim emergency authorisation for a surveillance device request in a specific and limited number of circumstances to prevent imminent threats, such as terrorist attacks or kidnappings.
- to the circumstances and manner of interception that can be conducted in an emergency. For example, allowing police to directly intercept information under s30(2) TIA Act, rather than 'an employee of a carrier'.
- creating provisions to enable law enforcement to utilise technologies in search and rescue operations

NSWPF supports maintaining the current arrangements for a law enforcement officer to provide internal authorisation to access data and information to locate a missing person.

The NSW Crime Commission very rarely meets the threshold required for urgent warrants and authorisations. When this does occur, the warrants are usually sought by the NSW Crime Commission's law enforcement or intelligence partners.

Part 5: Safeguards and oversight

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

NSW supports the safeguards as listed in the proposed future state. Beyond that, each law enforcement agency is responsible for ensuring staff awareness and diligence.

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

NSW notes the new framework should contain statutory protections for legally privileged information, health information, and other types of sensitive information, such as Cabinet-sensitive information. However, NSWPF notes that existing legislation to protect legally privileged information should be considered to reduce duplication.

The NSW Crime Commission notes the warrant regime could incorporate specific criteria that law enforcement agencies need to consider when reviewing and evidencing certain product. However, as has always been the case, the legislation cannot seek to stop agencies from obtaining the product first, and then assessing it for such claims; the consideration of such claims can only be made after the product has been obtained.

NSW welcomes the opportunity to further discuss this aspect with the Australian Government

See Annexure A for further information.

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?

NSWPF is committed to meeting public and industry expectations of the use of police powers and working with relevant oversight bodies to meet these expectations.

[1] of or above the rank of Inspector. Section 3 *Police Act 1990 (NSW)*.

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?

NSWPF supports maintaining the NSW Law Enforcement Conduct Commission as the NSWPF's primary oversight body, especially for matters relating to NSW legislation.

DCJ considers that this proposal, if implemented, could have significant implications for the effective oversight of all law enforcement agency activities in NSW. Centralising oversight of the exercise of powers under the new Act may seem to be an attractive and tidy arrangement, but in a federated system of government where the states and territories have primary responsibility for law enforcement, it could result in a less effective oversight system that does not respond to and take account of local needs.

DCJ understands from discussions with NSW oversight agencies and law enforcement agencies that the current system of oversight of the exercise of powers under the Commonwealth TIA Act works well in NSW. Any proposal to change current arrangements should be very carefully and thoroughly canvassed with NSW oversight and law enforcement agencies through the responsible NSW Ministers.

The NSW Crime Commission notes the current effective regime where both the Commonwealth Ombudsman and the Office of the Inspector of the Law Enforcement Conduct Commission (OILECC) provide oversight to the agency's use of powers. Any proposed changes to the oversight arrangement should involve further discussion with state-based agencies and at the ministerial level as these will impact on state-based legislation, particularly the NSW TIA Act.

A potential challenge may stem from the oversight of the NSW SDA. It appears unlikely that the NSW SD legislation will be subsumed by this reform. Therefore the NSW Crime Commission and its state-based partners will still need to be oversighted by State representatives and State legislation Even in the absence of any such applications, agencies are obligated to advise the overseer of that, and report, as required by each legislation.

See Annexure A for further information.

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

DCJ considers that there needs to be close consideration of what "meaningful transparency" countenances, what measures will best meet these aspirations, and what measures involve a disproportionate administrative burden or an unnecessary disclosure of operational practices in this sensitive area of law enforcement operations.

NSWPF notes current reporting requirements can be extremely onerous on law enforcement agencies and take months to prepare and compile without offering ways to assist meaningful transparency. These can be streamlined by taking the following actions:

- Ensure reporting obligations is not duplicated where possible.
- Ensure the time period given for agencies to assess the usefulness or resolution of a warrant is long enough for relevant court proceedings to have occurred. For example, within 3 months after a telecommunications service warrant is issued to the agency is often not enough time to determine the warrant's usefulness in terms of arrests or prosecutions.
- Ensure that reporting obligations do not require the exposure of technical details and protected methodology of law enforcement capabilities.

NSWPF supports not requiring reporting against matters relating to expenditure for the stated reasons outlined in the Discussion Paper. Other reasons for this position include the fact that expenditure matters are generally subject to strict internal regulation and policy and frequently inspected by internal auditors.

The NSW Crime Commission questions the efficacy of any proposal to remove the role of state-based oversight bodies.

The NSW Crime Commission's Warrant Administration Team has identified irregularities in reporting that could benefit from being streamlined. For instance, there are questions in the Home Affairs Annual Report – Interception Questionnaire which don't appear to have any meaningful operational, regulatory or public interest function other than their requirement under existing legislative frameworks. For example, agencies are required to calculate the actual duration of all warrants sought versus the length of time for which a warrant was issued, distinguishing between renewal and non-renewal warrants. Conversely, matters that might be of more significant public interest such as the acquisition of telecommunications data or content in error, are not reportable outside of the inspection framework.

The NSW Crime Commission notes the following processes around reporting and oversight may also be streamlined:

- Effectiveness reports;
- 6B NSW TIA Act / 94B Commonwealth TIA Act reporting to Attorney General compared with annual reporting to Minister
- Special register of warrants s81C does not appear to serve any real public interest purpose as the information is contained within the annual report

From recent Commonwealth Ombudsman inspections, the NSW Crime Commission recommends increasing effective engagement between agencies and oversight bodies to manage expectations and requirements, rather than altering oversight arrangements.

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

The NSW Crime Commission is of the view that additional reporting or record-keeping obligations should not be imposed.

Part 6: Working together: Industry and Government

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

While the NSW Crime Commission is unable to comment on the workability, NSWPF notes the current framework is workable from an operational perspective.

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?

A key issue in the current operating environment is the proliferation of resellers and on-sellers (e.g., Lebara, Lycamobile etc) subsidiary to a 'parent' provider such as Telstra, Optus or TPG. It is often difficult for law enforcement agencies to identify the entity closest to the source of the information,

or the owner of the information in order to effect service of the warrant or authorisation on the correct entity. This is particularly challenging with emerging technologies such as Cloud servers.

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

Industry should be encouraged to employ more dedicated law enforcement liaison officers. This would ensure a closer relationship between law enforcement and industry, as well as foster a greater understanding by industry of its obligations under the legislation. Additionally, further engagement with industry to assist law enforcement in identifying capabilities, types of information that are accessible and the relevant entities on which to serve warrants and notices would beproductive.

See Annexure A for further information.

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 with 'communications' more broadly, the retention of data generated by the Internet of Things (IoT) comes with both opportunities and risks. Although the temptation is to assume that there is no such things as too much information (especially if it can be analysed with advanced analytics or AI), there is a clear risk that the sheer quantity (or complexity) of data generated by the IoT with regards to 'machine-to-machine' interactions will potentially mean that it becomes unworkable and an impediment to its usability. The best case outcome would be for the framework to be sufficiently flexible to allow for a level of negotiation between industry and agencies and in turn the formulation of a compromise which broadly satisfies the objectives of both sides (noting that compromises would be required). Through a process of negotiation and collaboration, industry and agencies would be able to determine what subsets of IoT data is of most value in terms of its contribution towards agencies' objectives, which in turn would ensure that the obligations placed on providers in terms of the storage (and transfer) of IoT is not too great a burden.

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 NSW Crime Commission notes no additional records should be kept or recorded.

See Annexure A for further information.

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

Nil comment

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?

The NSW Crime Commission would oppose a reduction of 'authorised officers'. The NSW Crime Commission's authorised officers have intimate knowledge of the investigations relevant to the authorisations they make. This provides suitable oversight and assurance that information is being properly accessed in a manner required to assist the investigation. Reduction in the number of authorised officers would have the effect of authorisations needing to be made by more senior staff who do not have operational knowledge of the investigation.

See Annexure A for further information.

Additional feedback

Harmonising State and Commonwealth laws

The Discussion Paper notes that prohibitions on the use of surveillance devices are governed by state and territory legislation, with each jurisdiction having its own legislation that prohibits the use of certain surveillance devices in certain circumstances (Pages 13-14). The Discussion Paper states that in developing the new framework, the Australian Government will consider the appropriateness of existing prohibitions on the use of surveillance devices and whether any additional protections are necessary.

The NSW Government has no plans to change how Part 2 of the NSW SDA currently regulates and restricts the use of surveillance devices. If the Commonwealth develops any proposal to legislate to override NSW laws in this space, or to harmonise federal, state and territory laws, it should be raised and discussed at ministerial level, through forums like the Meeting of Attorneys-General.

No direct or indirect degradation of powers

The NSW Crime Commission supports proposals to streamline legislative thresholds and does not object to the proposed issue of warrants for offences punishable by a maximum of five years imprisonment. However, the NSW Crime Commission considers that requiring law enforcement agencies to demonstrate that exercise of the powers under a warrant will "substantially assist" may result in a degradation of powers in limiting the ability of agencies to utilise electronic surveillance warrants as part of a multifaceted investigative strategy.

See Annexure A for further information.

Ensuring consistency in availability of warrants that authorise remote access to electronic devices for federal and state offences

Currently, Part 2 Division 4 of the Commonwealth SDA provides that computer access warrants may be issued for federal offences punishable by imprisonment for 3 years or more. Computer access warrants authorise remote and covert access to electronic devices and are a valuable tool for criminal investigations.

However, computer access warrants are not available to investigate serious state offences without a federal aspect, such as murder and other serious violence and sexual offences.

This contrasts with warrants and authorisations under the Commonwealth TIA Act to intercept telecommunications and access metadata, which are available to support the investigation of state offences that do not have a federal aspect.

The Discussion Paper discusses establishing a streamlined and technology-neutral warrant framework that focuses on authorising access to the full range of information and data and moves away from regulating access to devices. However, it is not clear from the paper that the new framework will resolve the current inconsistency in the capacity for law enforcement agencies to apply for warrants to authorise remote access to electronic devices when investigating federal and state offences.

The Commonwealth could consider adopting an approach that does not disqualify the availability of warrants to investigate offences simply because they are state offences. In principle, warrants that authorise remote access to electronic devices should be available for serious offences regardless of whether they are state offences or federal offences. DCJ requests that if the Commonwealth adopts such an approach, that it consults with NSW about which state offences should be amenable to investigation by a warrant that authorises such access.

See Annexure A for further information.

Relationship to digital Identity data and information

DCS recommends the Commonwealth give further consideration with how Australian jurisdictions are managing digital identity and digital credentials, and the data that is created and stored using these artifacts.

The Commonwealth recently released the Trusted Digital Identity (Exposure Draft) Bill 2021 to enable a digital identity system used by state and territory governments and the private sector. This Bill proposes to restrict law enforcement access to any form of biometric data, and it is unclear how the Framework will align to this approach and the policy positions established in this Bill.

Data created in the system potentially facilitates a scenario whereby a person's day-to-day activities can be monitored using identity to purchase or obtain goods and services, including the use of biometric data. The Framework should consider how new identity data, previously not utilised by law enforcement, will be accessed.

As part of the delivery of the NSW Digital Identity Roadmap in 2022, NSW will be considering the issue of law enforcement access to information created in the NSW digital identity exchange. NSW will consult closely with the Commonwealth and other Australian jurisdictions on the approach.

Promoting public trust

DCS recommends the framework reflect the importance of maintaining public trust and confidence in the digital systems citizens are asked to use, as recently demonstrated in enacting legislation regarding the personal and health information collected under a Public Health Order in relation to COVID-19.

Impact on NSW Telco Authority

There is likely to be minimal impact to the policies or operations of the NSW Telco Authority (NSWTA) with the reform of the national electronic surveillance framework. The operations of NSWTA are not within the main scope of the focus areas of the reforms. NSWTA has existing obligations under the *Telecommunications Act 1997* (Cth) and *Telecommunications (Interception and Access) Act 1979* (Cth) to support the investigations of these agencies if required and will not be adversely, materially affected by the indicated reforms.

Cyber NSW

State cyber security bodies should be able to download and handle information resulting from credential and data breaches, including PII, in order to investigate the scope of potential impact to government and effectively mitigate the risks from the public availability of that data.

Cyber Security NSW is unable to download data available on dark web sites to investigate whether or not it poses a threat to NSW citizens. This ability would allow for much more effective intelligence gathering, and a carve-out should be made for state government cyber security organisations.

No increased administrative and / or compliance burdens on agencies

As noted in responses to question 16 and 31, the NSW Crime Commission considers its current oversight regimes to be sufficient and appropriate and opposes any proposals that would lead, directly or indirectly, to increased reporting, inspection or administrative burdens on agencies Existing reporting requirements should be reviewed and streamlined to remove duplication and focus areas that demonstrate the extent of use of the powers, the agency's compliance and focus on areas likely to be of public interest.

The NSW Crime Commission considers that streamlining and harmonising reporting requirements and oversight regimes may reduce, rather than increase the requirements on agencies without limiting oversight and public confidence.

Further consultation with the Commonwealth

Currently, both Home Affairs and the Digital Transformation Agency are consulting on a range of interrelated issues, such as digital identity, National Proofing Guidelines, and privacy. NSW requests the Commonwealth present a clear timeline for the year ahead to ensure appropriate and meaningful consultation can be conducted.