CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

CSCRC SUBMISSION: Response to the Department of Home Affairs – *Reform of Australia's electronic surveillance framework discussion paper*

cybersecuritycrc.org.au

Dear Sir/Madam,

Submission: *Reform of Australia's electronic surveillance framework* – Discussion Paper

I am pleased to submit the Cyber Security Cooperative Research Centre's (CSCRC) response to the Department of Home Affairs regarding its Discussion Paper into *Reform of Australia's electronic surveillance framework*. The Discussion Paper is an important first step in these important, once-in-a-generation reforms, which aim to ensure Australia's electronic surveillance framework remains fit for the digital world.

About the CSCRC

The CSCRC is dedicated to fostering the next generation of Australian cyber security talent, developing innovative projects to strengthen our nation's cyber security capabilities. We build effective collaborations between industry, government and researchers, creating real-world solutions for pressing cyber-related problems.

By identifying, funding and supporting research projects that build Australia's cyber security capacity, strengthen the cyber security of Australian businesses and address policy and legislative issues across the cyber spectrum, the CSCRC is a key player in the nation's cyber ecosystem.

We look forward to answering any queries about this submission and welcome the opportunity to participate in any future consultation regarding these landmark reforms.

Yours Sincerely,

Rachael Falk
CEO, Cyber Security Cooperative Research Centre
ceo@cybersecuritycrc.org.au

Introduction

Electronic surveillance capabilities are essential for intelligence gathering, policing and crime detection in our tech-reliant world. And over the last several decades, internet-facilitated communications and activity have replaced traditional telephony as the new normal. But while the technology has rapidly evolved, the legislation that governs electronic surveillance powers has struggled to keep pace. As a result, Australia has been left with a complex patchwork of laws governing the use of electronic surveillance and a more streamlined, tech-neutral and less complex regime is required.

This reform process will ultimately help Australians better understand how electronic surveillance powers operate, what these powers entail and their potential impacts on privacy. Transparency must be baked-in to the reformed regime and is essential not only to the future effectiveness of the extraordinary powers these laws enable – it is also essential for public trust. As noted in the *Comprehensive Review of the Legal Framework of the National Intelligence Community*: "Complex laws also undermine public trust and confidence. It should be clear to the Australian public what intrusive powers are available to NIC agencies, the circumstances in which they may be used, and the limits, controls, safeguards and accountability mechanisms that apply".[1]

In an increasingly complex operational environment, these reforms will play a key role in helping Australian authorities effectively and efficiently counter serious crime and threats to Australia's national security committed domestically and offshore. While there is no doubt electronic surveillance powers are extraordinary and intrusive, they play a key role in the investigation of some of the most grave crimes, like terrorism, child sexual abuse, cybercrime and drug trafficking. The rich content and evidence electronic surveillance provides in investigations cannot be understated, and this review is crucial in ensuring that these powers continue to be proportionate and appropriate in relation to the scale and seriousness of the threat posed.

Ultimately, the reform process presents a clear opportunity for Australia to ensure domestic electronic surveillance laws – laws with real-world consequences – are properly aligned with contemporary and future technological developments, allowing lawful, targeted access to data and devices where appropriate. Given the extraordinary nature of these powers, it is essential that the reform process is not rushed and that adequate consultation is provided with industry, academia, civil society organisations, and the Australian public more broadly, to help ensure new legislation does not have adverse unintended consequences, especially as it comes to privacy.

[1] volume-1-recommendations-and-executive-summary-foundations-and-principles-control-coordination-and-cooperation.PDF (ag.gov.au), P33

The Cyber Security Cooperative Research Centre (CSCRC) contends the reforms must clearly express to Australians why such extraordinary powers are required and (where possible) provide real-life examples of their application. This means highlighting the serious crimes or threats to national security that have been thwarted and the role that electronic surveillance played in preventing these crimes. Furthermore, several key concepts must remain front-of-mind during the reform process:

- Reforms must develop an effective and less complex warrant structure that targets individuals and, specifically, individuals suspected of committing serious crimes. These powers are ultimately about targeting people who are doing the wrong thing – they should not intrude on the privacy of innocent citizens.
- The new regime must be tech-neutral, easier to understand, transparent and avoid duplication.
- The public must be reassured the reforms do not seek to introduce additional powers and that the powers that currently exist will not be extended.
- Effective oversight mechanisms governing the appropriate and proportionate use of electronic surveillance powers must be maintained and, where needed, further enhanced.

This once-in-a-generation reform process provides Australia with an opportunity to establish an enduring electronic surveillance regime to stand the test of time. And Australians must be brought on this journey. As technology and communications continue to evolve and become even more central to the lives of Australians – as well as economic and national security – clarity, transparency and oversight of electronic surveillance legislation must be paramount.

Part One: 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?*

There is no doubt the increasing use of electronic surveillance by intelligence agencies and law enforcement bodies has posed emergent challenges to the protection of human rights, in particular, the right to privacy. While current protections in place across Australia's complex patchwork of electronic surveillance-related legislation are adequate and fit for purpose, there is no doubt that touted reforms have the potential to harmonise such provisions and offences and create less ambiguity as to how and when they would apply. Such a goal is especially pertinent in a global environment in which technological advances far outpace legislative changes and where threat vectors continue to evolve and globalise.

It is also important to note that, as part of the social contract upon which modern democracies like Australia are based, there must be limits to privacy. These limitations are clearly expressed in the United Nations' International Covenant on Civil and Political Rights

(ICCPR), to which Australia is a signatory.[2] In particular, Articles 17 and 19 of the ICCPR enumerate Australia's commitments to protect, respect and fulfil the right to privacy and the right to freedom of expression. These rights are related and mutually reinforcing—for instance, an individual's privacy facilitates their freedom of expression.[3]

The ICCPR clearly articulates situations in which limitations on human rights are permissible, noting that some human rights cannot legitimately be subject to any limitation, including the right to freedom from torture or cruel, inhuman or degrading treatment or punishment. According to the ICCPR, human rights may be limited where is necessary and proportionate to achieving a legitimate aim. [4] The protection of the human rights of individuals endangered by serious criminal activity, such as the general public, is a legitimate aim, as is surveillance on the grounds of national security or for the prevention of terrorism or other crime may be a measure that serves a 'legitimate aim'.

There is a risk that electronic surveillance legislation could limit human rights to a greater degree than is necessary through 'legislative creep'. That is, intrusive and extraordinary law enforcement powers can quickly become normalised through successive legislation and practice, and used as a precedent to justify even more invasive future measures. Hence, as part of this reform, strict oversight and compliance measures must be 'baked in' to help prevent legislative creep and ensure such extraordinary powers are not subject to misuse.

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, scam reduction or protection)?***

Existing prohibitions and offences against unlawful access to information and data adequately still allow for the pursuit of other objectives, such as cyber protections, online safety and scam reduction and protection. There are significant safeguards in place regarding the misuse of electronic surveillance powers and penalties exist for activities that cause damage to computers, networks and servers.

It should be noted that the lack of harmonisation across Australia's states and territories as it comes to what constitutes electronic surveillance and electronic surveillance devices creates confusion about where and when prohibitions and offences against unlawful access may apply. Hence, jurisdictional consistency has a role to play in the reform process.

The CSCRC notes the Comprehensive Review cautioned against Commonwealth legislation to replace state and territory surveillance device laws, which would significantly add to the

[2] OHCHR | International Covenant on Civil and Political Rights
[3] International Covenant on Civil and Political Rights - Human rights at your fingertips - Human rights at your fingertips | Australian Human Rights Commission
[4] OHCHR | International Covenant on Civil and Political Rights

complexity of the reform process.[5] Therefore, working closely across jurisdictions to harmonise surveillance device laws would be a prudent approach to achieving consistency and clarity and reducing greater complexity in the reform process.

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?***

Electronic surveillance powers are extraordinary and, as outlined in the Discussion Paper, in many investigations are necessary for the detection of serious criminal activity. Hence, strict controls must be upheld to ensure such powers are not used inappropriately or abused.

While the CSCRC supports additional powers as outlined being granted to AUSTRAC, the Australian Border Force (ABF) and the Australian Criminal Intelligence Commission (ACIC), we believe there is not a case for such additional powers to be extended to the and the Australian Taxation Organisation (ATO) and state and territory corrective services. AUSTRAC, ABF and the ACIC all play a significant role in protecting Australians from serious domestic and transnational crimes. Hence, they must be endowed with appropriate intelligence gathering tools to fulfil their missions, including adequate and enhanced electronic surveillance powers.[6] That said, more detail and greater clarity is required in relation to the expansion of these powers, especially in relation to the ACIC, with the information in the discussion paper significantly vague.

In seeking additional powers, the ATO, in particular, would have to provide ample evidence to illustrate operational necessity. The expansion of ATO powers could – understandably – cause alarm to members of the public in relation to potential invasions on the confidentiality of their private taxation and financial details. The CSCRC submits that for greater transparency and oversight, a better approach is for the ATO to work with other agencies (e.g. AFP), when seeking such warrants.

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?***

As noted above, the CSCRC agrees with the determinations provided in relation to AUSTRAC, ABF and the ACIC. However, the CSCRC believes the expansion of powers to the ATO and state and territory corrective services, as outlined in the discussion paper, are unnecessary.[7]

[5] The Department of Home Affairs Reform of Australia's electronic surveillance framework discussion paper
[6] Ibid 5, P17
[7] Ibid 5, P17

The CSCRC has outlined above its reasons as to why caution should be exercised in relation to the expansion of powers to the ATO. The CSCRC submits the expansion of powers for state and territory corrective services is fraught with potential for misuse and could create significant issues as it comes to oversight. The CSCRC submits that at the state and territory level, adequate mechanisms already exist for the monitoring of serious criminal offenders, for example, parole and probation mechanisms and the use of tracking devices such as ankle bracelets.

Part Two: 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 CSCRC submits the range of considerations noted in the Discussion Paper as it comes to redefining 'communications' in the TIA Act is sufficiently broad and, importantly, take a tech-neutral approach. Given the unrelenting pace of global digital development, it is vital the new definition is future-proof and broad enough to capture new developments, but also tight enough to help prevent unintended consequences or overreach.

The definitions of 'communication/s' in New Zealand's *Intelligence Security Act 2017 (NZ)*[8] and the United Kingdom's *Investigatory Powers Act 2016 (UK)* both provide good guidance for a new definition. Both are sufficiently broad and tech-neutral to be future-proof, while also being prescriptive in what they capture.

Section 7 of the NZ *Intelligence Security Act 2017 (NZ)* defines communication as "signs, signals, impulses, writing, images, sounds, information, or data that a person or machine produces, sends, receives, processes, or holds in any medium".[9] The use of the words "any medium" is especially useful in this definition.

Section 261 of the UK's *Investigatory Powers Act 2016 (UK)* defines communication as "anything comprising speech, music, sounds, visual images or data of any description" and "signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus".[10] This definition, while more complex in its wording, is also fit for purpose.

For ease of interpretation, the CSCRC submits the wording of the *Intelligence Security Act 2017 (NZ)* definition more useful.

6. ***Are there other key concepts in the existing framework that require updating to improve clarity?***

[8] Intelligence and Security Act 2017 No 10 (as at 28 October 2021), Public Act – New Zealand Legislation
[9] Ibid 8
[10] Investigatory Powers Act 2016 (legislation.gov.uk)

The CSCRC submits that other key concepts may need to be reviewed after a new definition of 'communications' is developed to help ensure consistency and operationalisation, as well as to reduce the potential for unintended consequences. Such work would have to occur as a flow-on effect of changes to the definition of 'communications'.

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

As previously noted, language in the definition of 'communications' must be kept sufficiently broad to capture evolving and future digital and technological developments, such as AI and quantum computing. Incorporation of the words "any medium" or similar, as applied in the *Intelligence Security Act 2017 (NZ)*,[11] could be useful in this regard. In relation to AI, precautions should be taken to ensure its ethical applications and that issues related to selection bias do not arise.

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 this would apply to?***

As noted in the Discussion Paper, clarity regarding the definitions of content and non-content information will be essential to the success of a new regime. The CSCRC believes the approach taken by the UK in its definition of 'content' is sensible and sufficiently clear,[12] and that it would be prudent to take a similar approach to definitional clarity of communications in Australian reforms. The UK definition also succinctly and simply defines what is *not* content.

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?***

Please refer to Question 8.

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?***

Non-content information is a vital tool in investigating alleged serious crime but is not in and of itself evidentiary, because without content there can be no context. What non-content information does is help build a picture of when, who with and where a person may be communicating from and, for example, the types of websites they have visited.

[11] Ibid 8
[12] Ibid 10

There has been significant controversy regarding the use of metadata and its privacy implications. While privacy should always be a primary consideration as it comes to surveillance activity, the CSCRC submits that the sensitivity of metadata has often been overstated as being more materially sensitive than, in reality, it is. What is of concern, however, is the ease with which metadata can be accessed via the mechanisms of the *Telecommunications Act*, which has significantly less clarity in regard to who and who cannot access this information than the TIA Act, which limits the use of metadata to 20 agencies. There is scope to tighten the provisions of the *Telecommunications Act* to abrogate such valid concerns and ensure use, access and retention of metadata and the privacy intrusions it causes are more tightly protected.

Metadata is information about a communication that does not include the contents or substance of that communication. Examples of metadata include (but are not limited to):

- subscriber information (for example, the name, date of birth and address of the person to whom the service is subscribed)
- the date, time and duration of a communication
- the phone number
- the location of a mobile device from which a communication was made[13]

What sets metadata apart is that unlike other intrusive powers, agencies can internally authorise a carrier to disclose metadata, meaning access does not require a warrant. This requires an authorised officer to consider the use and relevance of the metadata against intrusions on an individual's privacy. However, as noted above, such data is not in and of itself evidential. Rather, it can act as a useful part of the puzzle when it comes to investigating serious crime.

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

Given the rapidly evolving nature of communications and the significant changes to the ways people communicate have altered since provisions for 'stored' communications were introduced to the TIA Act in 2006, the CSCRC agrees that the distinction between 'live' and 'stored' communications is no longer relevant. In the current environment, and as noted in the Discussion Paper, the result is inconsistent protections for information that could be classified as either live or stored, even though the content remains the same.[14]

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

[13] Australian Federal Police's (AFP) use and administration of telecommunications data powers 2010 to 2020 (ombudsman.gov.au), PP3-4
[14] Ibid 5, P27

As outlined in the response to Question 11, given the evolution of communications, it is no longer useful to distinguish between live and stored communications. Both involve the same intrusion to privacy, noting much of the same information could be sought via either means (with the notable exception of a telephone conversation), and should not be differentiated.

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?

While this particular issue was not explored as part of the Comprehensive Review, there is scope to broaden the definitions of 'carrier' and 'carriage service provider' to capture 'new communications' like social media and over-the top-messaging services. Such applications are increasingly being used by Australians to send and receive messages as opposed to traditional telecommunications providers (e.g. Telstra, Optus), who are bound by the provisions of the *Telecommunications Act* and the TIA Act. Key examples include Apple and its iMessage service; Meta and its various platforms including Facebook, Messenger, WhatsApp and Instagram; and other platforms that can be used for messaging, like TikTok and Snapchat.

The CSCRC submits that the law as it currently exists does not adequately capture new and emerging forms of communications, such as those noted above, and that the new framework must capture a much broader range of communications providers. As noted in the discussion paper, Part 15 of the *Telecommunications Act* and its definition of 'designated communications providers' for the purposes of the industry assistance framework,[15] captures a much wider range of communications providers. There is merit in better aligning the definitions of 'carrier' and 'carriage service provider' with the definition of 'designated communications provider' for greater consistency and clarity and to keep pace with the current and future communications landscape. A potential approach to carving out entities that could be captured is by setting a minimum annual worldwide revenue threshold or by mandating a threshold related to the number of Australian subscribers. This would help ensure only entities with significant market share would be captured by such adoption.

The CSCRC stresses that such a move would not be overly burdensome to entities captured under a minimum annual revenue or minimum number of subscribers scheme. Rather, such an approach would even the playing field with telcos and recognise the rapidly altered nature of what constitutes a 'carrier' or 'carriage service provider' in the current (and future) environments. In taking such an approach, however, the willingness of companies not based in Australia to comply should be considered, given the extra-territorial nature of many of these organisations.

[15] Telecommunications Act 1997 (legislation.gov.au)

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 CSCRC supports reforms that focus on the information captured by a surveillance device as opposed to the type of device. This would help ensure future legislation is more tech-neutral and able to better withstand the test of time.

In defining or explaining such information, the CSCRC submits that descriptions should be kept suitably broad. For example, high-level concepts such as data, online communications, audio and visual recordings, stored data, intercepted telecommunications data and location data, would be appropriately broad and tech neutral concepts to consider in formulating a definition for this type of captured information.

The CSCRC notes that a key consideration of such a change must take state and territory definitions of surveillance and tracking devices into account, given the significant variations that currently exist. For the regime to work effectively, steps towards federal, state and territory definitional harmonisation should be considered.

Part Three: 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?

and

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?

In an operational environment that continues to grow in complexity, a simplified warrant system would significantly reduce complexity, provide greater clarity and transparency and reduce administrative burden.

The current patchwork of legislation and the multiple areas of overlap across the regime creates significant confusion. Consolidation of similar and overlapping warrants would help achieve more outcomes-focussed results. As noted in the Discussion Paper, such an approach would also promote greater attention to privacy in the warrant application process, with the least intrusive method of surveillance required for issuance.[16]

[16] Ibid 5, P35

Finally, a more streamlined warrant regime would enhance oversight by the Commonwealth Ombudsman and the Inspector General of Intelligence and Security (IGIS). Ultimately, a more streamlined and consolidated approach – and the greater clarity it will provide – will likely reduce room for administrative error in the warranting process, ultimately helping drive down accidental misuse of powers.

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?***

    and

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

It is appropriate for legislative thresholds to be harmonised for covert access to private communications, content data and surveillance information where existing warrants are functionally equivalent. While there may be exceptions where the threshold is lower, like as is currently the case for computer access warrants, harmonisation in this regard would significantly reduce complexity in the regime.

One way that effective harmonisation could be achieved is via a tiering system, essentially ranking the level of access that could be granted in line with seriousness of offending. For example, and in line with the current regulatory regime, more intrusive warrants may be permitted for crime that carry a minimum sentence of seven years' imprisonment.

The availability of other evidence should also be a consideration, noting that in a world increasingly reliant on internet-based communications, the only evidence available to actually prove a crime has been committed may only be found online. Hence, emerging and increasing phenomenon should be reflected in warrant thresholds.

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

The CSCRC supports reforms that would see tracking information regulated separately to more intrusive surveillance information. Such a change should retain the existing threshold that use of a tracking device be permitted for offences attracting a maximum period of three years' imprisonment. Likewise, the ability of agencies to internally authorise the use of particular tracking devices in particular circumstances should also be retained.

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 CSCRC supports the principle that, in the first instance, electronic surveillance powers be targeted and 'person-based', which would help protect the privacy of people not directly engaged in suspected serious criminal activity. Noting that in an increasingly complex operational environment such an approach may not always be possible, the CSCRC supports the addition of third-party and group warrants to the reformed regime.

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

Reforms that standardise the thresholds and purposes for which third-party powers can be used by both law enforcement agencies and ASIO are welcomed by the CSCRC. The additional warrant threshold as proposed, and its consistent application, would provide an appropriate additional safeguard to third-party privacy in all cases.

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

The introduction of group warrants where a warrant in relation to individual members of a group would be impractical or ineffective makes sense in an increasingly complex operational environment and would also help agencies delegate resources more efficiently. The addition of higher thresholds for group warrants would also act as a safeguard. In particular, the prerequisite requirement that application of such a warrant only be considered where it would be impossible to obtain a warrant for all individuals that are members of a group is a proportionate solution to a complex problem.

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 CSCRC broadly supports the approach as outlined in the Discussion Paper. As noted above, the additional safeguards proposed for warrant thresholds are appropriate and would help ensure that minimum standards are met in proving why different warrants may be sought in different situations. This would also help ensure that some warrants would not be sought as investigatory shortcuts.

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

Concerns have been raised in various inquiries in relation to the adequacy of AAT members issuing warrants for electronic surveillance.

In discussions with agencies that rely on these powers to investigate serious crime, the CSCRC has been told that the removal of the AAT as a key issuing authority would be a

significant blow to operations due to the AAT's capacity to consider such warrants more quickly than magistrates and judges. It is also worth noting that many members of the AAT have at least five years' experience as lawyers, legal qualifications or relevant knowledge or skills.[17]

One way this issue could be approached in the new regime is also via a tiered approach. That is, judges or magistrates be required to issue warrants for applications seeking the most intrusive level of powers, while warrants not requiring the same level of intrusiveness to be issued by AAT members.

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

The CSCRC supports the proposed principles-based, tiered approach to use and disclosure of information collected under warrant. Such an approach would help streamline the patchwork of inconsistent controls that currently exist across different legislative regimes and ultimately support enhanced information sharing between agencies.

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

As a general principle, the CSCRC recommends information obtained under warrants be destroyed as soon as practicable if no longer required for legal proceedings or ongoing investigations, and within five years. It is vital such information is stored securely and is not accessible to agencies or other government departments who have no legitimate basis to access the information.

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

In rare and extreme situations, especially in instances where there is imminent risk to life, it is appropriate that ASIO and law enforcement agencies have access to emergency authorisation of warrants.

The CSCRC supports the tiered approach outlined in the discussion paper, which would allow the issuance of warrants orally, without the provision of a written warrant. Such an application would rarely be required and could only be sought in extreme, time-sensitive situations.

As outlined in the discussion paper, a tiered authorisation framework comprising oral issuance (by the Attorney-General for ASIO and a judge for other law enforcement agencies), followed by a written authorisation after the fact, would be suitable in particular circumstances. Furthermore, it is a necessary mechanism that should be available in extraordinary situations.

[17] Chapter 2 – The role of the tribunals : AAT Annual Report 2016–17

Part 5: Safeguards and oversight

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

The safeguards as outlined in the discussion paper are sufficiently broad for inclusion in the new framework.[18] The CSCRC does not propose further safeguards beyond those stated are necessary.

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

The CSCRC submits that the principle that no party in legal proceedings is able to obtain an advantage by accessing legally privileged communications of another is deeply enshrined in our common law system. Conversations between lawyers and their clients for the purposes of obtaining legal advice are by their very nature deeply private and, subject to exceptions, should remain so.

There should be statutory protections for legally privileged information incorporated into the new framework as a safeguard mechanism, in line with Australia's democratic process and in the interests of natural justice.

However, it is vital to remember there are thresholds that must be met to invoke legal professional privilege (LPP) and there are also exceptions to LPP. Notably, the principle that privilege does not apply to communications made for the purpose of facilitating illegal or improper purposes, which applies regardless of whether a legal representative was a party to, or unaware of, the improper purpose.

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?

Both members of the public and industry expect independent and robust oversight mechanisms are in place as it comes to ensuring the lawful and appropriate use of electronic surveillance powers.

The CSCRC submits that the oversight currently provided by the Commonwealth Ombudsman and the IGIS remain effective oversight bodies for the future electronic surveillance regime. The Independent National Security Legislation Monitor (INSLM) should continue to play a central role in ensure the new framework contains appropriate protections for individual rights, is proportionate to national security threats and is necessary.

[18] Ibid 5, P62

These mechanisms are further bolstered by parliamentary oversight, notably the Parliamentary Joint Committee on Intelligence and Security (PJCIS) and the Parliamentary Joint Committee on Law Enforcement (PJCLE).

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 CSCRC submits the scope, role and powers of the Commonwealth Ombudsman remain fit-for-purpose in terms of effective oversight of the new framework.

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

As noted in the discussion paper, it makes sense that reporting requirement that do not assist meaningful transparency be removed, for example, reporting on annual expenditure on electronic surveillance or reporting on warrant registers. However, reporting requirements that enhance transparency should be included. For example, information regarding the use of electronic surveillance information by integrity agencies, including the number people of that have been subject to electronic surveillance, the number and type of warrants that were used and instances where an issuing authority has requested additional information or amendments in relation to a warrant.

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

As is stands, reporting of the use of electronic surveillance by agencies is subject to vigorous reporting and record-keeping requirements. The CSCRC submits that adding to such requirements would create unnecessary administrative burden. However, steps to make such reporting as publicly available as possible (noting operational and confidentiality restraints) would help improve public understanding on the frequency and scope of the use of these powers.

Part 6: Working together: Industry and Government

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

Anecdotally, the CSCRC is aware that the vast majority of industry works hard to comply with government requests when they are sought. This can prove to be a cost and resource impost on industry so, where possible, reducing the burden on industry in the new framework would be welcomed.

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?

While this question is difficult to address in the absence of a new framework, the CSCRC submits that a more streamlined and condensed warranting system would help reduce industry burden.

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

Communication is key to ensuring that government and industry work more effectively together in the new framework. Potential changes to interception capability plans (ICPs), as noted in the discussion paper, would serve to enhance communication between government and industry and could also help provide greater clarity for industry in terms of ICP update obligations.[19]

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?

The Internet of Things (IoT) continues to expand at a rapid rate, with new products for a range of different applications, from the mundane to the complex, constantly flowing into the market. For this reason, the CSCRC cautions against the new framework being prescriptive about what devices and their data should not be retained by providers. Such an approach would contradict the aim of the new framework to be tech-neutral, as many of the IoT devices of the future are yet to be invented.

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?

While the protection of journalists and their sources is a fundamental cornerstone of democracies, there must be limitations to the information they can receive and publish. Notably, there must be recourse for serious disclosures relating to sensitive matters of national security, which could compromise the safety of Australians and Australian interests.

[19] Ibid 5, P71

While the number of warrants obtained in relation to journalists and media organisations should be publicly reported annually, there should be no requirement to report on the target of the warrant or the type of warrant obtained.

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

The Public Interest Advocate Framework could potentially be expanded to government whistle blowers.

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 CSCRC submits that an increasingly complex operational environment, teamed with a growing volume of investigations that require access to telecommunications data, means that reduction to the number of 'authorised officers' able to authorise disclosure of telecommunications data could have a deleterious effect to the investigative process and ultimately the service of justice.