8 February 2022

Electronic Surveillance Reform Branch
Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

Dear Sir/Madam,

RE: AUSTRALIA'S ELECTRONIC SURVEILLANCE FRAMEWORK DISCUSSION PAPER

We thank you for the opportunity to make submissions in relation to the Reform of Australia's electronic surveillance framework discussion paper ("**the Discussion Paper**"). Given the rapid expansion of Australia's electronic communications surveillance legislation[1], we acknowledge the recommendations contained within the Comprehensive Review of the Legal Framework of the National Intelligence Community ("**the Richardson Review**") are being considered for reform of the legislative framework governing access to telecommunications in Australia via the repeal of all existing surveillance legislation and the introduction of a consolidated *Electronic Surveillance Act*.

We commence with two (2) primary submissions and recommendations before addressing the questions posed in the discussion paper. It is important to note that we have made submissions to each of the substantive national-security focused legislative developments since the metadata retention scheme was introduced in 2015 and have attended numerous hearings before the Parliamentary Joint Committee on Intelligence and Security (PJCIS), Parliamentary Joint Committee on Law Enforcement (PJCLE) and the Independent National Security Legislation Monitor (INSLM).

We respectfully request an invitation to any hearing or further consultation regarding the Discussion Paper.

We trust that the submissions contained in the following pages are of assistance and please do not hesitate to contact the below named should you require any further information.

[redacted]
Angus Murray
For and on behalf of the
Queensland Council for Civil Liberties

[redacted]
Dr Monique Mann
For and on behalf of the
Australian Privacy Foundation and
Liberty Victoria

[1] Mann, M., & Murray, A. (2021). *Striking a balance: Legislative expansions for electronic communications surveillance*. Precedent (Sydney, N.S.W.), (166), 44–51.

Submissions

At the outset, national security is fundamentally important to Australia. We recognise the importance of ensuring security of Australians' and their freedoms. The rationale for (indeed the very existence of) national security comes from the importance of ensuring that freedoms are protected. We are concerned to ensure that the 'forest isn't lost for the trees' in this reform process and that the guiding and predominant principle in this reform is that our national security framework serves to protect the freedoms that ought to be enjoyed by all Australians.

Whilst we appreciate and, in principle, have broad agreement with the proposals expressed in the Discussion Paper, we look forward to substantively considering an exposure draft of any proposed legislative reform in the form of a consolidated *Electronic Surveillance Bill*.

We emphasize that the Australian government has recently introduced a broad range of significant powers enabled by, *inter alia*, the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* ("**the Data Retention Act**"), the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* ("**the TOLA**"), the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2020* ("**the ID Act**") and the *International Production Orders Act 2021* ("**the IOP Act")**. The reform processes underway represent an opportunity to ensure that the exercise of these powers are necessary, proportionate, consistent with the rationale supporting their introduction, transparent, and subject to enhanced oversight and reporting requirements.

In recognition of the desire to rapidly reform the legislative framework governing telecommunications surveillance in this country, we submit that this ought to be undertaken in a substantive, transparent and consultative manner.

Recommendation One: The timeframe for introduction of a Bill repealing the *Telecommunications (Interception and Access) Act 1979* ("the TIA"), the *Surveillance Devices Act 2004* ("the SD Act") and aspects of the *Australian Security Intelligence Organisation Act 1979 Act* ("the ASIO Act") be delayed by at least twelve (12) months to allow for comprehensive consultation with experts, stakeholders and the community.

National security and surveillance powers in Australia ought to follow the introduction of a Federal and enforceable human rights framework, recommended by a succession of law reform commissions and bringing Australia into line with other democratic nations. The protection of Australians' human rights and associated freedoms is the rationale for the existence of national security legislation and therefore must be the paramount consideration for the use of intrusive powers. Adopting the text and spirit of the guiding principles for reform contained within the Discussion Paper, we consider that it would be appropriate to have the objects of a simplified *Electronic Surveillance Act* coupled with clear requirements for the use of national security and surveillance powers expressly reflecting Australia's obligations pursuant to the *International Covenant on Civil and Political Rights* and the *Universal Declaration of Human Rights*. This would instill public confidence by requiring law enforcement agencies (and Court's issuing

warrants) to have an express object of human rights compliance together with a decision making criteria that directly requires contemplation of human rights implications. In the context of substantive reform to national security and surveillance legislation it would be remiss to avoid due consideration of Australia's human rights obligations as established under international law.

Recommendation Two: The objects of a simplified Act ought to be coupled with clear requirements that the use of national security and surveillance powers are expressly balanced with Australia's obligations pursuant to the *International Covenant on Civil and Political Rights* and the *Universal Declaration of Human Rights*.

We now respond to each question posed in the Discussion Paper with our recommendations:

Part 1: Who can access information under the new framework?

Question 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?*

A Commonwealth prohibition on surveillance devices could be introduced. This would achieve a harmonisation of Federal, State and Territory law and make clearer the circumstances and requirements for the lawful use of surveillance devices. However, we note that harmonisation of laws requires consultation, political will and involvement of the State and Territory Information and Privacy Commissioners (where they exist). In particular we note concerns regarding under-resourcing of these Commissioners.

We do not consider that the penalties prescribed for unlawful access to information and data are adequate. Adopting the example contained in the Discussion Paper, s. 108 of the *Telecommunications (Interception and Access) Act 1979* creates an offence where a person accesses, authorises access or does anything that enables access to a stored communication that is punishable by two (2) years imprisonment or 120 penalty units. While we agree that that penalty is appropriate for unlawful access by a citizen, it pales in comparison to the penalty of up five (5) years imprisonment for disclosure by a designated communication provider contained at s. 317ZF of the *Telecommunications Act 1997* or failure to comply with a Notice issued pursuant to Division 3, Part 15 of the *Telecommunications Act 1997* which incurs, for a body corporate, 47,619 penalty units or 238 penalty units for a designated communications provider that is not a body corporate.

There is an important need for ensuring that citizens are not unlawfully accessing stored information and data of other citizens; however, given the significant power vested in law

enforcement, the penalties for misuse of that power ought to be severe and subject to strict liability. There should be significant penalties for misuse of power and an oversight mechanism that enables transparent and accurate reporting regarding when power and how power is used and the consequence that flows from misuse of said powers. This is relevant, for instance, when law enforcement access journalists' metadata without obtaining the required Journalist Information Warrants.

Recommendation Three: A Commonwealth prohibition on surveillance devices be introduced following consultation with State and Territory stakeholders.

Recommendation Four: Greater penalties for misuse of power vested with law enforcement ought to be introduced that include strict liability.

Recommendation Five: Increased transparency should apply to the use of law enforcement powers to ensure accurate oversight and prosecution of misuse.

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

As per our response to **Question 1** above.

Question 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?

We disagree with widening the range of agencies that have access to intrusive surveillance powers. The justification for intrusive surveillance powers is said to arise from the need to prevent and investigate human trafficking, child sexual exploitation and terrorism. These powers are acceptable in that, and only that, justification. It is inappropriate to widen access to these powers beyond agencies that respond to these most serious crimes. Electronic communication surveillance powers in Australia ought to be limited to the most serious of offences - namely terrorism, human trafficking and child exploitation. In our submission, a "serious criminal offence" ought to be specifically defined at a higher threshold that presently exists.

Recommendation Six: The use of surveillance powers be expressly limited to the investigation and prosecution of serious criminal offending and further consultation is required to establish that threshold, including evaluation of the historical exercise of powers with regard to the justification provided for their introduction.

We also note that, for example, the Commissioner of Taxation already has extensive investigation powers (such as the power to issue notices pursuant to s. 353-10 of the *Taxation Administration Act 1953*) coupled with a reversed burden of proof in relation to taxation decisions pursuant to s.14ZZK of the *Taxation Administration Act 1953.*

The only additional agency that ought to have access to intrusive surveillance powers and capabilities would be an Independent Commission Against Corruption at the Federal level. We also object to the proposal that corrective services have access to information for the purposes of monitoring individuals in the community. Such forms of surveillance would be pre-emptive and offend the rule of law.

Recommendation Seven: There be no additional agencies granted access to surveillance powers aside from a Federal Independent Commission Against Corruption (in the event that one is established).

Question 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 stated in response to Question 3, we do not consider that any additional agency(ies) should have access to information and data other than a Federal Independent Commission Against Corruption (in the event that one is established).

In this event this recommendation is adopted, we submit that the consideration ought to flow from the seriousness of the crime with the incorporation of a new definition of "serious criminal offence" (refer to **Recommendation Six**) and that the use of powers ought to be balanced against an express requirement that the use of national security and surveillance powers are consistent with Australia's obligations pursuant to the *International Covenant on Civil and Political Rights* and the *Universal Declaration of Human Rights* (**Recommendation Two**).

This approach to the consideration for the use of surveillance power is simplified and clearer than applying complex assessments about the technical mechanisms for the powers. This approach would also align with the justifications provided in the recent amendments made by the Data Retention Act[2], TOLA Act[3] and the ID Act[4].

Part 2: What information can be accessed?

Question 5. Are there other kinds of information that should be captured by the new definition of 'communication'? If so, what are they?

'Communication' is currently defined at s. 5 of the *Telecommunications (Interception and Access) Act 1979* as "a conversation and a message, and any part of a conversation or method whether in the form of speech, music or other sounds, data, text, visual images whether or not animated, signals or any other form in combination or in any combination of forms". Although that definition is capable of broad construction, we consider that a simplified definition of

[2] Revised Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015*, [2].

[3] Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, [2].

[4] Explanatory Memorandum, *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (ID Bill), [2]

communication could be introduced as “any exchange or record of information in any form between two or more locations”.

We also submit that the inferences that can be drawn from aggregate data should also be incorporated into any definition of ‘communication’ as these may be more revealing than the content or metadata itself.

In this way, the definition of ‘communication’ would be less about communication and more about the transmission of information, including activities such as web browsing, tracking and accessing data stored at rest in one’s computer or Cloud services. This would ensure that the definition of ‘communication’ is technology neutral.

In this context, and of critical importance to this submission, we submit that the key to creating a simplified national security regime as regards to electronic surveillance is a very broad definition of the key term - being communication (or another relevant term / concept that is used to capture this revised concept).

This is not to say that law enforcement should be given open access to the wider class of information under our recommended definition for ‘communication’. Rather, we consider that it is no longer relevant (or indeed helpful) to attempt to define elements of a communication (i.e., ‘content’ versus ‘non-content’ or ‘live’ versus ‘stored’) other than the fact of a record or exchange of information occurring.

Significantly enhanced judicial authorisation of law enforcement operations is appropriate in the form of increased warrant requirements for collection, judicial control of access *and analysis* (including aggregation and the drawing of inferences) of retained and intercepted ‘communications’ as are enhanced reporting obligations arising from the exercise of surveillance powers. We deal further with these points in our responses to the questions below.

Recommendation Eight: a simplified definition of communication be introduced as “any exchange or record of information in any form between two or more locations”.

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

We consider that the definition suggested in response to **Question 5** addresses issues with the existing framework.

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

In our view, a broader and simplified definition for “communication”, as proposed above in response to **Question 5**, would encapsulate emerging technologies and it is important to ensure that the principle of human rights protection as the fundamental basis for the existence of

national security measures remains at the forefront of any surveillance legislative framework. Further, it is important that the framework is created with a principle based approach that is founded in human rights as this serves to ensure a technology neutral framework. We note that such a recommendation exists in the Human Rights Commission's Human Rights and Technology Project[5].

Recommendation Nine: A simplified definition for "communication" as proposed at Recommendation Eight be introduced and that any framework that accounts for emerging technologies be informed by a human rights based approach as per Recommendation Two.

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

The distinction between 'content' and 'non-content' information is no longer meaningful. In our submission, a revision to the definition of 'communication' as per our response to **Question 5** above would make the concept of 'content' and 'non-content' irrelevant. A judicially authorised warrant ought to be required for any access to any 'communication' and the threshold for the issuance of such a warrant would and should not be more or less burdensome regardless of whether the information contained within a communication is "content" or "non-content" information. 'Non-content' information can be more revealing than 'content', especially in the context of metadata and drawing inferences from aggregate data.

Recommendation Ten: A simplified definition for "communication" as proposed at Recommendation Eight be introduced and that judicially authorised warrants be required for law enforcement access to information.

Question 9. Would adopting a definition of 'content' similar to the UK be appropriate, or have any other countries adopted definitions that achieve the desired outcome?

Please refer to our response at **Question 8** above.

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

Please refer to our responses at **Question 5** and **Question 8** above. This question is addressed in its simplest form by amendment to the definition of "communication" and the positioning of that term as the fundamental definition in relation to electronic surveillance.

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

[5] See: Human Rights Commissioner, *Human Rights and Technology Final Report (2021)* available at URL https://tech.humanrights.gov.au/?_ga=2.154928895.616985201.1643691567-165464140.1643691567.

Please refer to our responses at **Question 5** and **Question 8** above. This question is addressed in its simplest form by amendment to the definition of "communication" and the positioning of that term as the fundamental definition in relation to electronic surveillance.

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

Please refer to our responses at **Question 5** and **Question 8** above. This question is addressed in its simplest form by amendment to the definition of "communication" and the positioning of that term as the fundamental definition in relation to electronic surveillance.

Question 13. What type of Australian communications providers should have obligations to protect and retain information, and comply with warrants, authorisations and assistance orders under the new framework?

The substantive powers introduced by the TOLA Act were predicated on the new and broadly defined concept of 'designated communications provider' (DCP), created pursuant to s317C of the TOLA Act. A DCP can, through a technical assistance request (TAR), technical assistance notice (TAN) and/or technical capability notice (TCN) (collectively 'Notices') introduced into Part 15 of the *Telecommunications Act 1997*, be required to do a broad list of 'acts or things' defined in s317E of the TOLA Act. The amendments pursuant to the TOLA Act also had several potential extraterritorial effects. First, it allows for Australian law enforcement agencies to request or compel assistance from offshore DCPs and for foreign law enforcement to request that Australian agencies exercise surveillance powers to enforce foreign laws (including those involving the death penalty)[6]. This opens the possibility for foreign agencies to funnel requests through Australia in order to exploit its weaker human rights protections, rather than targeting other nations with stronger constitutional protections[7].

While we not our disagreement with the industry assistance powers under the TOLA Act[8] potential reform could alleviate concerns with the TOLA Act and its operation by an adoption of the definition of 'communication' provided at **Question 5.**
Moreover, any Australian DCP may be ordered by a Court to retain communications (as defined at **Question 5**) for a limited period and for the limited purpose of prosecuting serious offences (as per **Recommendation Six**). These powers should only be exercisable within the sovereign jurisdiction of the Australian Courts or subject to bilateral or multilateral agreements (also noting our concerns with the IPO Act and circumvention of mutual legal assistance treaty processes[9]).

---

[6] See: D Ford and M Mann, 'International implications of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, Australian Privacy Foundation (4 June 2019). <https://privacy.org.au/wp-content/uploads/2019/06/APF_AAAct_FINAL_040619.pdf>.

[7] See: M Mann, A Daly and A Molnar, 'Regulatory arbitrage and transnational surveillance: Australia's extraterritorial assistance to access encrypted communications', *Internet Policy Review*, Vol. 9, No. 3, 2020, 1–20.

[8] See: Mann, M. and Murray, A. (2021) 'Striking a balance: Legislative expansions for electronic communications surveillance', Precedent (Sydney, N.S.W.). *Australian Lawyers Alliance*, (166), pp. 44–51.

[9] Ibid.

Question 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?

We agree that the framework should be focused on regulation of the type of information (as per **Question 5**) that can be obtained rather than the types of surveillance devices. We agree that the Government ought to work closely with States and Territories to ensure that definitions are harmonized across Australian jurisdictions. We repeat Recommendation Two and our response to **Question 1, Question 5** and **Recommendation Three**.

In our view, the definition of 'communication' provided at **Question 5** could be incorporated into the definition of a 'surveillance device' as "any technology capable of recording a communication".

Recommendation Eleven: a definition of a 'surveillance device' be introduced as "any technology capable of intercepting, accessing or recording a communication".

Part 3: How can information be accessed?

Question 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?

Question 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?

We have addressed Questions 15 and 16 collectively and agree with the proposals contained in the Discussion Paper. Provided that the primary principle supporting the proposed framework is human rights based, we consider that *judicially* issued warrants are the appropriate means to authorising access to information.

There should be no circumstances where warrants are authorised by the Heads of Interception Agencies, the Attorney-General or Ministers (i.e., Executive authorisation). It is axiomatic that authorisation by a Court provides necessary independence, addressing concerns about one executive hand washing the other. Submissions by civil society organisations have recurrently noted that warrant issuing by courts does not involve inordinate delays. We reiterate concerns regarding issuing of warrants by members of the Administrative Appeals Tribunal.

These warrants should be the subject of judicial oversight to ensure compliance with human rights and **Recommendation Two**. On this condition, warrants could reasonably be outcome-focused provided that they are subject to legislative restriction that detail the powers that can be exercised under warrant, and including general descriptions of the ways agencies access

information, and on the basis that the authorisation of power provided in a warrant is based upon the least intrusive means available to the agency.

Part 4: When will information be accessed?

To briefly recap, it is our submission that the predominant and primary purpose of a simplified *Electronic Surveillance Act* ought to be the protection of human rights (**Recommendation Two**). Collection, access and analysis of communications (as broadly defined and discussed in response to **Question 5** and **Recommendation Eight**) should only be authorised in circumstances of the investigation of a serious crime with amendments to that definition as expressed in **Recommendation Six**.

Question 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?

We submit that under a broad and technologically neutral definition of "communication" (as per **Question 5** above), any access ought to be controlled by a warrant issued only by the Federal Court of Australia or a Supreme Court of a State or Territory of Australia. This ought to be achieved in a tiered approach of "collection warrants" and "access and analysis warrants". In effect, law enforcement ought, on grounds of reasonable suspicion or belief and with primary regard to the human rights implications of such an authorisation being granted, to be required to obtain a warrant to collect communications and, separately, obtain judicial authorisation to access *and analyse* communications. This approach could alleviate the need to define specific technologies being the subject of a warrant authorisation.

Recommendation Twelve: any collection of communications ought to be controlled by a warrant issued only by the Federal Court of Australia or a Supreme Court of a State or Territory of Australia.

Recommendation Thirteen: A "collection warrant" ought to be introduced which, on application to the Federal Court of Australia or a Supreme Court of a State or Territory of Australia on grounds of reasonable suspicion or belief and with primary regard to the human rights implications of such an authorisation being granted, to be required to obtain a warrant to collect an individual's communications.

Recommendation Fourteen: An "access and analysis warrant" ought to be introduced which, on application to the Federal Court of Australia or a Supreme Court of a State or Territory of Australia on grounds of reasonable suspicion or belief and with primary regard to the human rights implications of such an authorisation being granted, to be required to obtain a warrant to access and analyse an individual's communications collected under a validly issued "collection warrant".

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

Issues and concerns regarding reasonableness and proportionality in the authorisation of access to metadata are resolved by vesting authorisation with the Federal Court of Australia or a Supreme Court of a State or Territory of Australia.

As regards to journalistic information, this concept ought to be expanded by further consultation as to what constitutes information that justifies a higher threshold, such as information that engages lawyers' client-legal privilege, academic freedom, and a broadened class of what constitutes "journalism" (i.e., beyond the current definition of 'a person working in a professional capacity as a journalist'). We refer to this class of information, for convenience alone, as "special information". We consider that, where law enforcement reasonably suspects or ought to be aware that, communications collected under a "collection warrant" would include information within this class of "special information". We will return to matters concerning journalists' information further in **Part 7** below.

Recommendation Fifteen: The concept of "journalist information warrants" ought to be expanded by further consultation as to what constitutes information that justifies a higher threshold, such as information that engages lawyers' client-legal privilege, academic freedom and a broadened class of what constitutes "journalism".

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

This question should be deferred for further consultation both prior to and in connection with the public release of an exposure draft of the proposed framework.

Question 20. What are your views on the proposed framework requiring warrants and authorisations to target a person in the first instance (with exceptions for objects and premises where required)?

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

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

A collection warrant ought only be authorised in relation to *an individual under investigation* and the issue as regards to third party or group warrants are alleviated by an ability to seek additional collection warrants authorised by the Federal Court of Australia or a Supreme Court of a State or Territory of Australia.

Question 23. What are your views on the above proposed approach? Are there any other matters that should be considered by an issuing authority when considering necessity and proportionality?

We agree that a simplified *Electronic Communications Act* should require the Federal Court of Australia or a Supreme Court of a State or Territory of Australia to be satisfied of the matters contained in the Discussion Paper (p. 52) being the following non-exhaustive list of factors:

- the gravity of the matter under investigation – is the crime or security matter, and the resulting likely harm, serious enough to justify the use of the power?
- the intrusion on privacy – how much will the use of the power intrude on the privacy of the target or any other person?
- the likelihood the surveillance will achieve the warrant objective – will the use of the power actually provide the information that the agency is seeking?
- the likely relevance and usefulness of the information – is the information likely to further the agency's investigation, including preventing further criminal activity or threats to security?
- whether there are less intrusive means of achieving the purpose of the warrant – could the agency use some other less intrusive power to obtain the information it is seeking?
- what other intrusive powers have been, or are being, used in relation to the target?

We additionally consider that, as recommended, the Court also ought to be satisfied that other human rights (i.e. freedom of association, political opinion, anti-discrimination etc) are not disproportionality impacted by the issue of a warrant.

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

Authorisation of access to information should vest with the Federal Court of Australia or a Supreme Court of a State or Territory of Australia.

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

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

In relation to the sharing of information collected under warrants, we submit that any sharing or disclosure of information collected by an agency only occurs with leave of the Court and is destroyed as soon as it is no longer required which is an expressly defined concept that occurs at either a fixed period of time after collection or a fixed period of time after the conclusion of any prosecution of an individual the subject of such warrants.

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

In certain, and limited circumstances (as they are contained in the Discussion Paper), we agree that a warrant may be authorised with retrospective effect by the Federal Court of Australia or a Supreme Court of a State or Territory of Australia. We submit that an application for

retrospective authorisation requires evidence of notice and approval provided that the activity contemplated in such an application was expressly authorised by either the Director-General of ASIO or the Attorney-General prior to activity being undertaken by law enforcement.

Part 5: Safeguards and oversight

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

Refer to **Question 17** above.

We also support existing requirements in, for example, the ASIO Act that require the Director-General to report about instances where warrants issued under s.25, 25a, 27a, 27c, or 29, which have "materially interfered with, interrupted or obstructed the lawful use by other persons of a computer or other electronic equipment or a data storage device", including the addition of associated "concealment activities" (34(2)(b)). However, reporting should be made directly to the Inspector-General of Intelligence and Security (IGIS) as well as the Parliamentary Joint Committee on Security and Intelligence (PJCIS). This recommendation aligns with the PJCIS' similarly framed recommendation contained at, for example, Recommendation 2 of the PJCIS *Advisory report on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*[10].

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

Legally privileged information (and possibly other sensitive information, such as health information) should be not accessible and we refer to **Question 18** above and **Recommendation Fifteen**.

Question 30. What are the expectations of the public, including industry, in relation to oversight of these powers, and how can a new oversight framework be designed to meet those expectations?
We agree with the implementation of the *Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020* to provide greater oversight by the PJCIS and INSLM.

Intrusive surveillance powers should be limited to exceptional and significant circumstances and used sparingly with full regard to the fundamental freedoms that ought to be enjoyed by all Australians. In addition to **Recommendation Two**, an independent and Court appointed "Human Rights Advocate" from a judicially established panel of legal practitioners ought to be required to make submissions on any warrant application. We consider that public confidence

[10] Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (August 2021), [6.26].

will be increased if selection is made by an independent judicial panel, rather than by a ministerial advisor.

Recommendation Sixteen: the simplified Act prescribes a role of an independent and Court appointed "Human Rights Advocate" from a judicially established panel of legal practitioners ought to be required to make submissions on any warrant application.

Question 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 Commonwealth Ombudsman investigates, publicly reports, and makes *actionable referrals* to the Australian Commission for Law Enforcement Integrity (ACLEI) for the enforcement of penalties for law enforcement misuse or unlawful exercise of surveillance powers (e.g., when accessing journalists' metadata without the required Journalist Information Warrant or failing to obtain the correct authorisations for the exercise of surveillance powers). This process of referral should enable significant penalties for misuse of power and an oversight mechanism that enables transparent and accurate reporting regarding when power and how power is used and the consequence that flows from misuse of said powers. Consistent with preceding comments, we emphasise the importance of appropriate resourcing of the Ombudsman, given the increasing range of tasks assigned to the Ombudsman, questions about the expertise of the Ombudsman's office, and balkanisation of privacy oversight responsibilities across an increasing range of agencies.

Recommendation Seventeen: the simplified Act requires that the Commonwealth Ombudsman investigates, publicly reports, and makes *actionable referrals* to the Australian Commission for Law Enforcement Integrity (ACLEI) for the enforcement of penalties for law enforcement misuse or unlawful exercise of surveillance powers.

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

This question requires further consultation with the benefit of an Exposure Draft of the simplified Act and reserve our response to that point.

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

A redacted form of judicial decision records for the issue of warrants ought to be published. In our submission, transparency, accountability and oversight of the operation of warrants is possible by publicizing the legal principles (rather than the specific facts) of warrants issued and would enhance public confidence in the oversight of such a regime.

Recommendation Eighteen: A redacted form of decision records for the issue of warrants ought to be published.

Part 6: Working together: Industry and Government

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

Question 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?

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

A principled human-rights approach to these submissions ought to be the predominant focus of this consultation rather than considerations regarding industry collaboration or co-opted assistance with law enforcement. The recommendations made in this submission address a balance between the expectations of the Australian community and national security.

Part 7: Interaction with recent existing and recent legislation and reviews

Question 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?

Considerable industry concern was expressed in response to the *Data Retention Act* and the commercial and financial burden this regime placed upon industry and consumers. We reject that communications and information ought to be retained other than as required by a judicially authorised warrant. However, we accept that this forms an important aspect of a simplified *Electronic Surveillance Act* and respectfully reserve response to this question when an Exposure Draft of a Bill is made public.

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?

Refer to **Question 37(a)**.

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

Refer to **Question 37(a)** together with our **Recommendation Sixteen**.

Further, we contend that the position of the Public Interest Advocate under the *Data Retention Act* should be a representative of media organisations or the profession of journalism rather than an appointment of the Prime Minister. This advocacy process should be more transparent rather than covert with regard to the interests of the journalist and the freedom of the press.

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?

Judicial oversight and authorisation is the only appropriate mechanism for authorisation of communications data and we refer to our response to **Question 16** and **Recommendation Twelve**.

We trust that our responses to the questions posed in the Discussion Paper have been of assistance in this initial consultative process. We look forward to the publication of an Exposure Draft of the consolidated *Electronic Surveillance Act.*

Please do not hesitate to contact the writers should you require any further assistance.