February 14, 2022

The Hon Karen Andrews MP

Minister for Home Affairs
Parliament House
Canberra ACT 2600

Dear Minister,

We are a diverse group of organisations representing a range of perspectives including both the internet industry and civil society in Australia. We support the work of the government in seeking to reform and rationalise Australia's electronic surveillance framework which is undoubtedly outdated and overly complex in its current state. We welcome the Discussion Paper opening the opportunity to consult on this matter and look forward to continuing to work with you in the establishment of a modernised, coherent and effective legal and regulatory framework.

We believe, however, that the proposed framework may fail to balance its objectives of better protecting individual information and data, as well as providing a clear and transparent Act that will facilitate industry's compliance, in favour of extending powers for law enforcement agencies and ASIO to investigate crimes and threats to security while expanding the burden on industry by imposing or increasing the application of regulatory requirements.

Responses to Electronic Surveillance Reform Discussion Paper
Author: Name Name

We also note the increased importance and evolution of capability in surveillance tools which combined with societal change and the advances in artificial intelligence and analytical capabilities provide useful and accurate information from large data sets. From the outset, we emphasise that it is essential that any framework be founded on the key principles of real need, proportionality, reasonableness, and accountability, and the utmost respect for human rights, including the importance of maintaining personal freedom with minimum state supervision and surveillance. Any exceptions to the general prohibition of electronic surveillance must properly consider the seriousness of the privacy intrusion involved. Furthermore, the review must be appropriately coordinated to achieve harmonisation across Federal and State or Territories to ensure consistency and ease of compliance. It is also important that ordinary citizens can understand the basis for use of the powers and have confidence regarding the integrity of the system that permits their use. We believe that adherence to these principles is critical to maintain trust in the organisations and government that underpin Australia's democratic society.

Key terms and definitions

Communications

We recognise the fundamental need to clarify the definition of *'communications'* to keep up to date with changes in how individuals and systems interact, and how information and data are transmitted online.

We note that the changes proposed in the Discussion Paper seek to extend the kinds of data and information that will be captured under the new definition. While we acknowledge such an expansion may be necessary to ensure agencies are able to access the required relevant information and data for gathering of intelligence and evidence, we raise concerns that such a change would give rise to increased risks and problems.

For example, the proposal to capture information generated from Internet of Things (IoT) devices potentially raises a two-pronged issue. On one hand, this will result in substantial costs and burdens for industry in having to comply with the likely requisite data retention obligations. Simultaneously, this will increase the risk of such entities being subject to cyber attacks as many businesses operating IoT currently likely lack the requisite ability to implement safeguard measures to ensure the privacy of individuals.

We recommend that the definition for *communication* be de-coupled from data disclosure so that not all communications are subject to the same requirements. We view that the current proposal is too broad and thus the onus is on the government to demonstrate what information will be retained and disclosed, and why.

Any changes to the definition for *communication* will have significant implications on various other elements of the framework's operation. As such, we believe it is critical that this be considered in conjunction with principles of reasonableness and practicality.

Non-content data

We note that the distinction between content and non-content information and the resulting requisite level of authorisation for information for each type is highly contentious. Industry is still eagerly awaiting the government's response to the PJCIS' report on its review of the mandatory data retention regime which made recommendations to clearly define *the content or substance of a communication*.

Metadata can be extremely revealing and can constitute personal information depending on the surrounding circumstances. As such, the warrantless system for accessing metadata is an issue often raised by industry and civil society groups and we believe that it is not suitable to remain in the new framework. In this context, we also note that the PJCIS in its report on its review of the mandatory data retention regime expressly recommended "whether some information that is currently treated as telecommunications data should now be regarded as content given what that information can reveal about an individual."[1]National security and offence threshold

The currently existing framework and the proposal under the Discussion Paper make extensive reference to national security as one of the core justifications for electronic surveillance. However, we note that this definition is used inconsistently across different legislation and circumstances. We recommend that 'national security' also be clearly defined for the purpose of the Act.

Furthermore, given that electronic surveillance is an extreme intrusion of individual privacy, we recommend the application of the definition of 'serious offences' in line with the *Telecommunications (Interception and Access) Act 1979* (TIAA).

[1] p, 95, para 5.17, Recommendation 2, Parliamentary Joint Committee on Intelligence and Security, *Review of the mandatory data retention regime*, Oct 2020

Technology neutral

We agree in principle with the proposal to make the new Act technology neutral. We recognise the rationality in ensuring that new legislation not face similar issues as the current framework lagging behind the constant evolution of technology. However, we emphasise that technology neutral wording must not result in all-encompassing unclear thresholds and definitions which render the Act a catch-all legislation that avoids appropriate nuance and distinctions. It is imperative to ensure that any new framework is clear, practical, efficient and effective whilst also remaining current with technological change.

Potential overreach in government powers

Agencies given electronic surveillance powers

The Discussion Paper notes that the government will consider which bodies should have access to telecommunications data or metadata in line with the PJCIS review of the mandatory data retention scheme. However, we recommend that the government should go further to directly implement an equivalent of the recommendation that was made in that report so that only ASIO and the list of agencies listed under s 110A of the TIAA, and only through one legislative means, should be able to access such data. Agencies focusing on revenue protection should not be able to directly access data. We also recommend that there not be an equivalent of section 280(1)(b) of the *Telecommunications Act (1997)* which can enable other agencies to obtain access to data in the new legislation.

In the event this is not possible, we believe that the proposed future state as set out in the Discussion Paper is too vague and that the government should establish clear thresholds for a definite list of agencies with access that includes a much higher threshold for the inclusion of any additional agencies.

How information can be accessed

Part 6 of the Discussion Paper notes the possibility of the Government requiring selected members of industry to develop and maintain attribute-based interception capability. We are concerned with the extreme breadth of power this would provide the Minister or Attorney-General, in addition to the great costs to industry as noted in the Richardson Review. Therefore, we oppose the inclusion of any powers concerning attribution-based interception.

Moreover, as above, we again emphasise the need to harmonise the process of how agencies can access information, and that the warrantless system for metadata be abolished.

Oversight and accountability

We acknowledge the consideration of safeguards and oversight by the Government and appreciate the commitment to ensuring the accountability of the new framework. However, we believe that greater oversight is required than the current state and the proposed future state. We are particularly concerned over the limited oversight for those operating under a warrantless regime.

The Richardson Review discusses a ‘double lock’ system and its various benefits. While the report ultimately recommended against the implementation of such a system, we believe that such a system is necessary for warrants and other investigative powers conducted by ASIO and other agencies. Furthermore, the authorisation powers should be vested external to the Executive of any

single agency. We believe that this is crucial to ensuring stringent oversight and accountability and such benefits recognised by the Review should not be discarded lightly.

We also note that the INSLM in its review of Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018 and related matters found the argument for independent approval of TCNs and TANs, external to the requesting agency, similar to that of a double-lock system, "compelling".[2]

Potential issues with compliance

We note the broader list of entities who will be subject to obligations, and recognise the need to reassess the range of entities who will need to be captured to ensure the efficacy of any new Act. However, we emphasise the need to consider this in the context of the principles of reasonableness and practicality so as to avoid the resulting issues which are likely to arise.

At the current stage, it is difficult to respond on the potential issues regarding what sort of data will be required and its implications for industry due to the lack of clarity in defining *communication*s. However, we believe that the currently proposed breadth of scope overreaches and is at risk of creating a catch-all framework.

We also recommend the obligations be accompanied by clear and timely guidance so that they can be practically implemented.

Conclusion

We believe that these recommendations and considerations will significantly enhance the discussion of the new electronic surveillance framework by ensuring greater focus on the paramount protection of individual privacy and mitigate barriers to compliance. We are committed to the building of a new framework that will appropriately balance all objectives to better protect all parties and the citizenry at large.

Again, we thank you for the opportunity to respond on this matter and look forward to continuing to work with the government in resolving these concerns as consultations continue in the process to create Australia's new electronic surveillance framework.

Yours faithfully,

Representatives of the following organisations (overleaf)

[2] pp. 196-197, paras 10.18-10.19, Independent National Security Legislation Monitor, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, June 2020.

Internet Association of Australia	
Communications Alliance	
Internet Of Things Alliance Australia	
Australian Information Industry Association	
Internet Australia	
Digital Rights Watch	
Electronic Frontiers Australia