INTERNET ASSOCIATION OF AUSTRALIA
ABN 71 817 988 968
ACN 168 405 098
PO Box 8700
Perth Business Centre WA 6849
Phone: 1300 653 132

11 February 2022

To: Department of Home Affairs

By submission: www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers

INTRODUCTION

Thank you for the opportunity to express the Internet Association of Australia (IAA) perspective on the Discussion Paper concerning the reform of Australia's electronic surveillance framework. We welcome the extensive review of the current system which is undoubtedly due for comprehensive reform. IAA supports the efforts to establish a new framework that is proportionate, reasonable and effective to ensure Australia maintains a robust electronic surveillance framework that is able to balance the objectives of permitting law enforcement agencies to carry out their functions in keeping the community safe from harms whilst still upholding the privacy of individuals.

We note that this review forms part of an overarching overhaul of the security regime in Australia undertaken in recent years. While we acknowledge that it is critical the government stays on top of the ever evolving technological landscape to ensure the protection of Australia, we also raise concerns that on the whole, such reforms may be at risk of, or at least the serious perception of, transforming Australia into a surveillance state with overreaching government powers that endanger the freedoms and privacy of its citizens and inhibits the operation and growth of industry.

IAA is signatory to the joint letter submitted by various stakeholders from industry and civil society organisations in relation to this review. While that joint letter expressed the general high-level concerns which we believe must be considered by the government at the minimum, this submission will go into greater detail about our perspective on the Discussion Paper. Many of IAA's members are small to medium sized internet service providers (ISPs). Therefore, this submission is

written from the perspective of our members with a focus on the impact on smaller internet businesses, as well in promotion of the general well-being of the internet and civil society.

PART I: WHO CAN ACCESS INFORMATION

A MORE COMPREHENSIVE REGIME

IAA welcomes the proposed efforts to harmonise the regulations between the Commonwealth and States or Territories. We note that this will however result in more changes being made at different levels and thus greater work will need to be undertaken by industry and other entities in order to meet their obligations under the new framework. IAA requests that consultation continues and is prioritised during this period so that all stakeholders will have a chance to have a say on what this comprehensive regime will look like and what the implications will be.

AGENCIES PERMITTED ACCESS

At the outset, IAA emphasises that electronic surveillance is a substantial power and not one that should be simply handed over. The intrusion to the individual right to privacy is extreme and should not be dismissed lightly. As such, IAA believes that the proposed future state on which who should be able to access information or data is too broad and vague.

We extend our support to the stance that was taken in our joint letter. We believe only ASIO and the list of agencies under s110A of the *Telecommunications (Interception and Access) Act (1979)* should be able to access information and data, and only through this legislation. As such, we agree with the recommendation by the PJCIS's review of the mandatory data retention scheme that the exception to this rule under s280(1)(b) of the *Telecommunications Act (1997)* be repealed.

At the very least, we believe that the Discussion Paper is too vague in its proposal regarding what sort of information will be required for what reason and for which specific agencies. While IAA supports the list of questions that the government will be required to consider before permitting additional agencies access, there needs to be further clarity and transparency as to why such agencies should be granted access.

For example, the Discussion Paper notes that ACIC will be able to use its powers for a "slightly wider range of investigations." This does not provide sufficient information to ascertain whether it is in the public interest to grant powers which contravene the fundamental right to privacy. Similarly, clarification should be provided regarding State and Territory corrective services agencies which will be granted access for the purpose of monitoring criminal offenders.

Thresholds regarding the type and seriousness of crime to warrant surveillance should be established.

PART II: WHAT INFORMATION CAN BE ACCESSED

IAA welcomes the efforts of the government to clarify the definition of various key terms to fit the modern way in which people interact. For this part, we request you refer to the stance expressed on this matter in the joint letter. In addition, we will emphasise and share our perspective on some key points raised in the Discussion Paper.

COMMUNICATIONS

We emphasise the increased burdens that will be particularly experienced by small businesses. It is likely that they will face the greatest challenge with the implementation of changes in policy and infrastructure in order to comply with the likely new obligations that will be introduced with the amendment to the definition. As such, we reiterate that the definition of communications be de-coupled from disclosure so that only the relevant entities are captured by any new obligations. Where smaller providers will be subject to the legislation, we request that the government provides support and guidance to assist with compliance.

NON-CONTENT INFORMATION

While the distinction between content and non-content data has always been conflicting and complex, we believe this is being further confounded with the addition of the term 'personal information' and how this intersects with non-content data. As such, we believe that clarification regarding the definition of non-content data is critical in the modern age, and particularly in the context of the great number of reviews being conducted in the area of privacy and digital data or information.

In addition to the points raised in the joint letter, we stress that while definitions should remain technology neutral, the government should look at the layer at which the communication is occurring to distinguish between content and non-content data. While we maintain the stance that the warrantless system for non-content data should be abolished, if this is not possible, we believe that a distinction similar to the 'entity data' and 'events data' as followed in the UK could be useful so that accessing 'events data' at the very least is subject to a warrant. We believe this is crucial in order to ensure protection against unfettered government access to individuals' data. This will also allow greater consistency as to the intentions and recognition by the government

that even non-content data can be very revealing about an individual's personal information. As this was a key point raised in the Attorney-General's Privacy Act Review, we believe it is a principle that should also be applied to the government in accessing such data.

LIVE AND STORED COMMUNICATION

IAA recognises that the way in which we communicate has changed so as to blur the significance of the distinction between live and stored communication. While that is true, it is our belief that there are still norms and understanding that is held by individuals which influence how they communicate. People still prefer not to leave sensitive information in stored format. For example, it is heavily advised that people do not send their passwords to themselves through an email or text as this is information that increases their risk of being exposed to hackers.

Therefore, we believe it is critical that the distinction between live and stored information is retained in the new framework. In addition, we believe this is necessary so as to provide clarity on which entities will be subject to the obligation to provide live interception.

CARRIERS AND CARRIAGE SERVICE PROVIDERS

IAA recognises the need to clarify the definitions surrounding 'carriers' and 'carriage service providers' for the purposes of the surveillance framework, and whether new terms are necessary to appropriately capture the relevant entities who are part of the telecommunications supply chain. It is our understanding that the amendment could see a substantial expansion in entities who would be subject to the electronic surveillance regime. However, we raise concerns that this would not only cause significant burdens for industry, it will also likely stifle investment and innovation in Australia's telecommunications sector. We emphasise the need for continued consultation with industry in this process so as to mitigate the likely adverse implications raised by such changes.

PART III: HOW INFORMATION CAN BE ACCESSED

In principle, IAA supports the focus of a framework that prioritises privacy over the method of access. However, we believe that the proposal outlined in the Discussion Paper will actually undermine this objective. In practice, it seems that an outcome-based warrant will obscure transparency and instead result in overreaching powers of the Executive. A broad warrant that permits any method of obtaining information indeed obfuscates transparency.

We propose a double-system of outcome-based warrants where agencies will still need to satisfy particular thresholds to be able to use different methods they propose to use. The onus should be on the agencies to prove why they should be allowed to use such methods as well addressing additional matters including, but not limited to, of the seriousness of the crime being investigated, whether being limited to certain types of methods would not be sufficient, how this method will assist in their investigation, the likelihood of success in their investigations by using this method, and the impact on privacy.

Therefore, this could still remove the existence of multiple warrants for each particular type of information. However, there will still be appropriate checks and accountability so as to prevent agencies having unfettered access.

PART IV: WHEN INFORMATION WILL BE ACCESSED

In general, IAA supports the principle of applying real life standards for the electronic landscape when it comes to warrant systems. However, we raise some key issues with points outlined in the Discussion Paper. It is noted that the government will consider expanding agency powers to access information for the purpose of developing, testing, maintaining and evaluating electronic surveillance and cyber capabilities and technologies. We are concerned that information is being accessed and, in line with the Comprehensive Review, potentially retained despite there being no immediate threat of crime or issue of national security. Moreover, if these powers are necessitated by the fact that agencies lack the ability to develop and test their capability in simulated environments due to limitations in their technological capacity, there is a real risk of agencies not possessing the requisite ability to ensure any information being accessed and/or retained will be secure. Thus, given the great intrusion on privacy that is being imposed – in the absence of any real risks – IAA believes that the most stringent limitations and regulations must be established. If such powers are to be expanded, there must be full transparency into the access and retention of information. In addition, strict policies concerning the destruction of data must be implemented and adhered to.

ACCESS TO INFORMATION ABOUT COMMUNICATIONS

IAA raises concerns about the proposed two-year retention period. Industry expressed its views on this term during previous consultations and use this opportunity to again note that this causes substantial burdens for organisations. This is particularly so for the small businesses that we represent.

ACCESS TO INFORMATION ABOUT PERSONS' LOCATION OR MOVEMENT

IAA disagrees with the proposal that access to tracking information will retain the lower threshold of offences attracting a maximum penalty of three years' imprisonment. We believe that the threshold of five years' imprisonment be proposed as the general standard that should apply. We oppose the justification that tracking a person's location or movement amounts to a lesser imposition into one's privacy. In addition, consistency should be achieved wherever possible.

SPECIFIC TARGET, THIRD PARTIES, AND GROUPS

We support the Comprehensive Review's recommendation that all electronic surveillance powers should be 'person-based' in the first instance. IAA acknowledges that this will not always be possible. Where exceptions arise, we believe that they must be subject to a high threshold. Onus must be on the agencies to prove why non-person-based powers are necessary and required to make considerations including, but not limited to, the seriousness of the crime, how this will assist in their investigation, the likelihood of success in their investigations by obtaining information through this power, and the intrusion on privacy. Furthermore, this should not be allowed by just internal authorisation, and should always require a warrant.

IAA supports the standardisation of third party warrants across different agencies. However, we disagree with the proposal that agencies would only need to demonstrate other methods would be impractical or ineffective. The threshold which should apply is that methods to obtain information through an ordinary warrant was exhausted, or at the least, that it would not otherwise be possible. Lowering the threshold altogether removes the impetus on agencies to maintain the privacy of individuals as a priority that must be heeded and balanced. Again, it must be emphasised that intruding on one's privacy is no small matter, and this should be reflected in the regulation of powers which would see potentially unrelated individuals or those not the subject of an investigation having their privacy breached.

Similarly, IAA opposes the blanket group warrant which could see agencies gaining surveillance powers over entire messaging platforms. Such an approach raises various concerns. On one hand, given the substantial volume of data that would be attracted by such a warrant, this would give rise to serious burdens on industry whilst simultaneously seeming inefficient for agencies to have to investigate such large quantities of information. Moreover, this seems to be an overreach in the government's powers that would again, intrude on the privacy of unrelated individuals. There is a myriad of reasons why individuals may use anonymising apps. To encroach upon individual

freedom to do so amounts to a serious breach of their privacy. However, IAA supports that there should be harmonisation for agencies to have the same access for the same type of warrants as above in the case of third-party warrants.

APPROPRIATE AUTHORISATION OF POWERS

IAA welcomes the proposed requirement that agencies will need to satisfy the issuing authority that the use of a particular power would be necessary and proportionate. We believe that the authorising authority should be a judicial magistrate or judge for agencies with the exclusion of ASIO. With regard to ASIO, we believe that they should be subject to some additional judicial or other independent authorisation. We view this as necessary for various reasons including, but not limited to, achieving harmonisation with international production orders, ensuring appropriate oversight, and increasing public trust in the operation of government agencies.

We note that the concept of a 'double lock' was considered in the Comprehensive Review. Although the report ultimately deemed the system unnecessary, as stated in the joint letter, we emphasise that the benefits of a double lock approach should not be dismissed lightly.

DISCLOSURE AND ERASURE

IAA supports the principle of the tiered approach. However, it is critical that transparency and oversight remain core priorities throughout this process. In addition, there must be clear and limited circumstances when disclosure should be allowed. Prior to disclosure, agencies should be required to consider similar matters as when they are applying for a warrant. This includes, but is not limited to, the seriousness of the crime, how likely the information would help the other agency, how likely the disclosure would help the other agency, and the intrusion on privacy.

Agencies should be required to destroy any information that is not relevant to their specific investigation, and where relevant, following any sharing of information that is subject to disclosure for primary or secondary purposes.

EMERGENCY AUTHORISATIONS

IAA recognises the need for emergency authorisations where the usual process of obtaining a warrant may not be possible. However, we believe there must be strict adherence to transparency to this process. This includes clarity over definitions of what constitutes an emergency to warrant such a process, as well as clear reporting so that the effectiveness of the process can be assessed appropriately and thoroughly.

In addition, while we acknowledge that emergency authorisation powers should exist, adequate attention should be heeded to the note in the Comprehensive Review that the current system has not prevented ASIO from obtaining information in urgent situations so as to prevent them from achieving their objectives. As such, while we support the streamlining of the process it is our view that emergency authorisation is not an area in need of greater expansion of its scope of power.

PART V: SAFEGUARDS AND OVERSIGHT

IAA welcomes the government's commitment to ensuring that an appropriate system of safeguards and oversight will be built into the new framework. We support the harmonisation in oversight between the Commonwealth and States and Territories. Following that principle, we believe that independent oversight is also critical over the AFP and the Department of Home Affairs. We believe one recourse to ensure this accountability would be to expand the scope of the INSLM's functions from its current ad-hoc application.

However, noting that the INSLM's scope is limited to matters of national security, we do believe that an independent body with consolidated powers over all relevant agencies would be best suited to achieve the necessary level of harmonised and comprehensive oversight over the use of the surveillance powers under the new framework.

Moreover, this could also mitigate the current issue of reporting to the Minister for Home Affairs as serving no useful function as raised in the Discussion Paper. Reporting is a critical element of ensuring accountability and thus should serve a meaningful purpose. In that respect, it is our view that reporting on annual expenditure should be retained in the new framework, contrary to the proposal to remove this obligation in the future. Annual expenditure is inherently a matter of public interest as it concerns expenditure using the public's money and can be used to assess whether the amount spent on electronic surveillance is justified by the outcome. Thus, it is important to maintain transparency in this matter.

PART VI: INDUSTRY AND GOVERNMENT

IAA emphasises our commitment to working with the government in this process of reforming Australia's electronic surveillance framework. However, we believe that this must be measured so as to not impose unnecessary burdens on industry. In that light, we oppose the attributions-based interception which would likely result in great cost to industry, particularly for smaller businesses. Moreover, in line with concerns raised in the joint letter in addition to points made above, we believe that all obligation requirements should be kept at the appropriate level. For example, CSPs

should not be made responsible for content data which occurs through over the top messaging platforms.

IAA welcomes the effort of the government to seek ways in which agencies and industry will be able to work together in a more streamlined way. We believe that the Trusted Information Sharing Network groups which has recently been expanded to the telecommunication sector could be a good model that could similarly be adopted for electronic surveillance. IAA would be more than happy to run such a discussion and networking forum for the telecommunications sector, or help the government facilitate such a forum.

In general, the establishment of a harmonised framework which is measured in its approach so that it is not too onerous on business, not overreaching in permitting and enabling access nor intruding on the individual right to privacy, should set a streamlined foundation through which industry and agencies will be able to work together constructively and securely.

CONCLUSION

Once again, IAA appreciates the opportunity to contribute to the reform of Australia's electronic surveillance framework. We look forward to representing our members and the broader public interest in the continued engagement with the Department of Home Affairs, as well as other stakeholders, to ensure the creation of a new measured, effective and practical electronic surveillance framework that will best serve Australia.

ABOUT THE INTERNET ASSOCIATION OF AUSTRALIA

The Internet Association of Australia (IAA) is a member-based association representing the Internet community. Founded in 1995, as the Western Australian Internet Association (WAIA), the Association changed its name in early 2016 to better reflect our national membership and growth.

Our members comprise industry professionals, corporations and affiliate organisations. IAA provides a range of services and resources for members and supports the development of the Internet industry both within Australia and internationally. Providing technical services as well as social and professional development events, IAA aims to provide services and resources that our members need.

IX-Australia is a service provided by the Internet Association of Australia to Corporate and Affiliate members. It is the longest running and lowest cost Internet Exchange in Australia. Spanning six

states and territories, IAA operates over 30 points of presence and operates the New Zealand Internet Exchange on behalf of NZIX Inc in New Zealand.

IAA is also a licenced telecommunications carrier, and operates on a not-for-profit basis.

Yours faithfully,

Narelle Clark

Chief Executive Officer
Internet Association of Australia