COMMUNICATIONS
ALLIANCE LTD

Communications Alliance Submission

to the Department of Home Affairs
in response to the

Reform of Australia's electronic surveillance framework
Discussion Paper

18 February 2022

CONTENTS

Communications Alliance

Communications Alliance is the primary communications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, platform providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to be the most influential association in Australian communications, co-operatively initiating programs that promote sustainable industry development, innovation and growth, while generating positive outcomes for customers and society.

The prime mission of Communications Alliance is to create a co-operative stakeholder environment that allows the industry to take the lead on initiatives which grow the Australian communications industry, enhance the connectivity of all Australians and foster the highest standards of business behaviour.

For more details about Communications Alliance, see http://www.commsalliance.com.au.

1. Introduction

Communications Alliance welcomes the opportunity to make a submission to the Department of Home Affairs (Department) in response to the *Reform of Australia's electronic surveillance framework* Discussion Paper (Discussion Paper).

This submission has been endorsed by the Digital Industry Group Inc. (DIGI).

We support a general review of the surveillance framework and recognise opportunities for modernisation, harmonisation, clarification, consolidation and updating of various pieces of legislation that currently form Australia's electronic surveillance framework. Consequently, in principle, we support the intention to streamline the existing legislation and replace it with a single, technology-neutral, consistent Act that provides sufficient clarity and certainty for all organisations bound by its provisions. However, the new framework must be developed in close consultation with industry to minimise the risk of unintended consequences and to ensure the new framework does not impose unnecessary additional cost on industry.

Communications Alliance members have a long history of closely cooperating with law enforcement agencies under different pieces of legislation and legislation, including:

- Data Retention Regime (*Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*);
- Telecommunications Sector Security Reform (TSSR) requirements in Part 14, Division 3 of the *Telecommunications Act 1997;*
- *Telecommunications (Interception and Access) Act 1979* (TIA Act);
- Section 313(3) of the *Telecommunications Act 1997,* which requires carriers and carriage service providers (C/CSPs)(among other things) to "give help as reasonably necessary" to assist authorities with enforcing the criminal law and laws imposing pecuniary penalties.
- All communications member organisations (i.e. C/CSPs, platforms, search engines, hardware and software manufacturers, etc.) may also assist LEAs through the workings of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Assistance and Access Act 2018).
- They may also provide far-reaching assistance via the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021.*
- Moreover, our members will assist agencies through any legislated measures that will flow out of the *Telecommunications Legislation Amendment (International Production Orders) Act 2021* and any associated international treaties.

All C/CSPs, digital platforms, search engines, app distribution services and other members of the online industry will also continue to lend their assistance under formalised existing and new arrangements in the recently enacted *Online Safety Act 2021* (OSA).

Communications Alliance – in cooperation with other relevant industry associations – is currently in the process of developing industry codes to underpin the OSA, to further strengthen online safety. The codes will be released for public consultation, to enable registration by July 2022/December 2022. Once registered, these codes become enforceable by the Commissioner.

The OSA and the industry codes have recently been complemented by the *Online Safety (Basic Online Safety Expectations) Determination 2022,* which sets out expectations to uphold online safety for Australian end-users for social media services and other sections of the industry.

All C/CSP, digital platforms and search engines also provide assistance, both voluntary and legislated, for example through compliance with the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 (AVM Act)*.

Communications Alliance and its relevant members will also comply with the recent national security reforms as a result of the *Security Legislation Amendment (Critical Infrastructure) Act 2021* and those that are yet flow from the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022*.

Communications Alliance has represented the communications industry through formal and informal engagement with all relevant stakeholders during the development and, where applicable, review processes of the relevant legislation over the past 15 years (and earlier).

Communications Alliance is also a member of the Interception Consultative Committee, chaired by the Department of Home Affairs.

On this basis, we offer the following feedback in response to the Discussion Paper.

2. Guiding principles

2.1. The Discussion Paper appropriately begins by listing the objectives of the new Act which can be summarised as follows:

- better protection of individuals' information and data in today's data societies;
- ensuring law enforcement agencies (LEAs) and ASIO have the powers they require to fulfil their respective functions;
- clarity, transparency and practicality for those that need to work and comply with the new Act;
- technology-neutrality, updating of definitions, updating of the list of LEAs; and
- appropriate thresholds, effective and consistent controls, limits, safeguards and oversight.[1]

The Discussion Paper also notes that the safeguards listed in the last objective must "reflect the importance of accountability, transparency, the rule of law, privacy and other applicable rights" and the necessity to balance those against LEAs and ASIO's needs to effectively pursue their enforcement and investigative activities.[2]

The Discussion Paper goes on to say:

> *"The framework will have some impact on industry. The need to protect the integrity and security of communications and networks will be front of mind. Industry assistance will continue to be required – for example, in intercepting communications and accessing telecommunications data. However, it is intended that streamlining the existing framework will ultimately lead to a reduced regulatory burden."*[3]

2.2. While we recognise that the Discussion Paper acknowledges the need to protect the integrity and security of communications and networks, we are concerned that this need has not been identified as a key objective of the reform and given equal weight to other objectives. **Given the importance of the integrity and security of communications and networks – as evidenced in the recent Critical Infrastructure Reforms – it difficult to understand why this criterion would not, in and of itself, be an objective of the new Act.**

[1] p. 6, Department of Home Affairs, *Reform of Australia's electronic surveillance framework* Discussion Paper, Dec 2021

[2] ibid

[3] ibid

We highlight that the Parliamentary Joint Committee on Intelligence and Security (PJCIS), in its recent report on the Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms, expressly made the following recommendation:

> *" 3.112 The Committee recommends that section 3 of the Telecommunications Act 1997 be amended to add an object of the act ensuring the security of telecommunications networks and their architecture from cyber and other security threats."*[4]

While the Committee made a recommendation in relation to the *Telecommunications Act 1997*, we believe that the principle is equally true in the context of the broader surveillance framework.

Consequently, we strongly recommend the inclusion of an express objective of preservation of the integrity and security of communications and networks, in the new Act.

2.3. We also note that a significant set of broad powers beyond the scope of this reform (including the ability to search personal digital devices and copy electronic information without a warrant) are afforded to the Australian Border Force (ABF). Therefore, we believe that the ABF should also be subject to these reforms.

3. Who can access information?

Agency access to information

3.1. Part 1 of the Discussion Paper raises the question as to who can access information under the electronic surveillance framework.

However, the first question posed under this Part, namely

> *"Do the existing prohibitions and offences against unlawful access to information and data adequately protect privacy in the modern day?"*[5]

goes to a much broader context and ought to sit outside this Part, or at least ought to be equally considered in the context of thresholds, effective and consistent controls, limits, safeguards and oversight.

Consequently, at this stage our focus in response to this question is with regards to the 'who', i.e. which agencies, have access to information.

3.2. Overall, the current framework, with its protections provided by section 276 of the *Telecommunications Act 1997* and the subsequent exception in sections 290 and 280, is confusing, complex and difficult to apply.

3.3. As detailed in numerous submissions, including the statutory review of the Data Retention regime in 2020, section 280(1)(b) in combination with the requirement of section 313(3) of the *Telecommunications Act 1997* to *"give officers and authorities of the Commonwealth and of the States and Territories such help as is reasonably necessary"* have led to more than 80 agencies making requests for metadata, over and above the 22 Criminal Law Enforcement Agencies that were originally intended to be the only agencies vested with such powers.

3.4. In its October 2020 report, the PJCIS, which led the Inquiry into the review of the mandatory data retention regime, made the following recommendation

[4] p. 46, para. 3.112, Recommendation 2, Parliamentary Joint Committee on Intelligence and Security, Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms, Feb 2022
[5] p. 16, Department of Home Affairs, *Reform of Australia's electronic surveillance framework* Discussion Paper, Dec 2021

5.100 The Committee recommends that section 280(1)(b) of the Telecommunications Act 1997 be repealed.

Moreover, the Committee recommends that the Government introduce any additional amendments to Commonwealth legislation that are necessary to ensure that:

- *only ASIO and the agencies listed in section 110A of the Telecommunications (Interception and Access) Act 1979 [TIA Act] be permitted to authorise the disclosure of telecommunications data; and*
- *those agencies can access telecommunications data only through Part 4–1 of the Telecommunications (Interception and Access) Act 1979 and through no other legal mechanism.*

3.5. We are disappointed and bewildered by the fact that Government has not responded to this important report, more than one and half years after its release.

3.6. We strongly recommend that the new Act respond to the above recommendations, to ensure only a narrowly defined list of law enforcement agencies and ASIO be granted the powers to request access to metadata, and only through one specific legal mechanism.

3.7. The Discussion Paper also proposes considerations for determining whether additional agencies should be permitted to access peoples' information and data. The Paper specifically suggests giving consideration as to whether the *"the agency typically deal[s] with the investigation, prevention or enforcement of crimes that merit access to such information?"*[6]

3.8. As noted above, we believe that the recommendation by the PJCIS to limit the number of agencies that have access to metadata to those listed in section 110A of the TIA Act (and also those that have powers to intercept communications) ought to be implemented.

3.9. If further agencies must be added, we believe that the aforementioned criterion, in and of itself, is not sufficient, as it does not entail any threshold, nor include any form of proportionality test. In our view, there ought to be a uniform (well-defined) threshold for the crimes that warrant access to metadata – also noting that access to metadata is currently a warrantless regime.

We note the recent PJCIS recommendations[7] to revisit the definition of 'serious offence' more generally and apply consistently across Australia's security legislation. (Also refer to sections 6.4 to 6.6 further below.)

The threshold of serious offence, as currently defined in section 5D of the TIA Act (where serious offence, by and large, is an offence punishable by imprisonment for life or for a period, or maximum period, of at least 7 years), ought to be the threshold for agencies to be able to apply for the use of these powers, i.e. only agencies that typically deal with 'serious offences' ought to be considered; to ensure the use of the powers is proportionate to the offence.

3.10. Furthermore, the scheme should be explicit regarding the extent to which information is being used for surveillance and analysis, as well as the extent to which prospective collection is allowed. Access to metadata, including by means of a technical assistance notice, should not be allowed to generally assist the mission of an agency, but instead should only be requested or sought when specifically required in relation to a known offence.

[6] p. 18, ibid

[7] p. 135, para 6.71, Recommendation 12, Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*, Aug 2021 and p. 53, para 4.93, Recommendation 7, Parliamentary Joint Committee on Intelligence and Security, *Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, Dec 2021

3.11. In any case, we believe that providers responding to requests for metadata must be given certainty that the agency requesting the data has the requisite powers to do so. It must not be incumbent on providers to verify the validity of requests or the legal basis on which those are made.

3.12. Related to the question of the threshold for agencies to access information, is the question of use of the information obtained through surveillance, interception or as part of access to communications data. The information so obtained ought only to be used for the specific purpose for which it was obtained (and which entitles the agency to obtain the information).

Pursuit of other objectives of societal benefit

3.13. Generally speaking, Part 13 of the *Telecommunications Act 1997* prohibits carriers and carriage services providers (C/CSPs) from disclosing and using the contents and substance of a communication, as well as affairs and personal particulars of a person.

3.14. In the recent past, this has prevented C/CSPs from taking some measures in relation to identifying and blocking malicious SMS messages.

This specific issue has been addressed through the *Telecommunications (Interception and Access) Amendment (2021 Measures No. 1)* Regulations 2021 (made in November 2021 upon 'request' by Communication Alliance).

3.15. However, the issue highlights the difficulty in interpreting the scope of the relevant exceptions.

3.16. The future Act should include a coherent principle-based regime for communications security, access and use of communications for technical service delivery reasons, including network security, permissions for access to communications, and access to communications for LEAs and national security agencies. Any exceptions need to be clearly defined and widely understood.

3.17. We also note, consistent with our opening remarks, that the pursuit of other objectives of societal benefit must include the integrity and security of networks, as well as the privacy of communications. Both of those require, to a significant extent, encryption and, therefore, the new Act ought to be seen as an opportunity to give encryption the positive attention that it deserves.

3.18. Similarly, we caution against an overly legalistic approach to the new framework with regard to lawful access to information.

For example, the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Assistance and Access Act 2018)* and the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* both created far-reaching powers for LEAs and investigative agencies.

While those Acts do not create a regime of unlawful access or disclosure of information, a perception of undue intrusion is not helpful for businesses nor the general reputation of the interception and access regime with the Australian public more generally.

3.19. We also encourage global interoperability with the new framework, and in particular welcome efforts being made by the Australian Government to enter into an agreement with the US Government for access to electronic communications under the US enacted *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act). The CLOUD Act enables companies to disclose data to LEAs subject to an appropriate consenting official being satisfied about the maintenance of robust procedural protections for privacy and human rights. We note that the agreement signed by the United States

and Australia in December 2021 must now undergo Parliamentary and Congressional review processes in both countries.[8]

3.20. The US Department of Justice has previously emphasised the importance of privacy in Designated International Agreements under the CLOUD Act with foreign partners.

> *"The Act permits our foreign partners that have robust protections for privacy and civil liberties to enter into executive agreements with the United States to use their own legal authorities to access electronic evidence in order to fight serious crime and terrorism. The CLOUD Act thus represents a new paradigm: an efficient, privacy-protective approach to public safety by enhancing effective access to electronic data under existing legal authorities. This approach makes both the United States and its partners safer while maintaining high levels of protection of privacy and civil liberties"*[9]

These high standards under US law must be reflected in the updated Australian framework. Otherwise, there is a risk of Australian law diverging from the robust protections for privacy and civil liberties required to enter into a CLOUD Act agreement under US law.

4. What information can be accessed?

4.1. The Discussion Paper proposes the clarification and/or re-definition of some key terms and concepts, such as 'communications', 'content' and 'stored communications'.

4.2. In principle, we agree that these terms and concepts would benefit from clarification and further debate as they are, as defined or used/applied/given meaning in their current form, not practical for operational purposes.

However, we disagree or raise concern with some of the proposals and notions put forward in the Paper, as further discussed below.

Definition of 'communication'

4.3. The Discussion Paper proposes a broadening of the definition of 'communication' to now include, among other things, a person's internet activity, electronic documents created by a person (regardless of whether they have been transmitted), and, importantly, interactions between persons and machines and machine-to-machine interactions/signalling, including all data generated by the applications of the Internet of Things (IoT). It also envisages that the definition includes quantum computing and information derived from machine learning.[10]

4.4. In fact, the data sets listed for inclusion in the definition are so extensive that is hard to think of important data sets in existence that are excluded. Indeed, it appears that this is the approach intended by the Richardson Review:

> *"In line with the Comprehensive Review's recommendation, the core definitions in the new framework will aim to:*
>
> *[…]*

[8] As accessed at https://minister.homeaffairs.gov.au/KarenAndrews/Pages/united-states-australia-enter-cloud-act-agreement.aspx on 16 Feb 2022

[9] US Department of Justice (2019) FAQ, *Promoting Public Safety, Privacy, and the Rule of Law Around the World*, as accessed at: https://www.justice.gov/dag/page/file/1153466/download on 16 Feb 2022

[10] p. 22, Department of Home Affairs, *Reform of Australia's electronic surveillance framework* Discussion Paper, Dec 2021

ensure there are no gaps in the types of information that agencies may access or obtain under warrants and authorisations"[11]

4.5. The Discussion Paper proposes to make this broad range of information available under warrant or authorisation. However, we note that the Discussion Paper does not indicate which of the new sets of the broader information would be made available under warrant and which ones are being proposed to be made available under authorisation.

4.6. While we agree that the definition of 'communication' requires clarification so as to reflect modern communication technologies and societal changes, we believe that the proposed scope is overly broad, in the absence of any evidence or argument as to why this scope would be required.

The proposed scope includes, among other extensive data sets, data generated by the usage of non-messaging applications, person-to-machine data (including, for example, interactions with a customer service chat-bot), machine-to-machine content and IoT-generated data.

Beyond the technical difficulty of collating certain categories of the data captured here (such as machine to machine data), the sheer volume of data implicated in the proposed scope is of serious concern. It is predicted that the average Australian household will have 36 internet-connected devices in 2024.[12]

The volume of additional data that is proposed to be retained and the systems required to make it available to agencies is potentially astronomical. The challenges to keep this data secure could also be substantial.

With the world's IoT devices alone expected to generate close to 80 zettabytes[13] (10^{21}) or 1 zettabyte represents about as much information as there are grains of sand on all the world's beaches[14]) of data by 2025, it appears that retention of this data alone would already be impractical, if feasible at all. Adding all the other data sets to the above estimate amplifies the problem to an even greater scale. It is also important to understand that in many cases, IoT devices act as 'black boxes' which, in many cases, will only provide very limited useful data and/or the data cannot easily be captured and/or the data is captured by third party operators, thereby further complicating access arrangements.

4.7. Therefore, we request that any definition of 'communication' be guided by an initial analysis as to which information ought to be made available <u>following a stringent cost-benefit analysis</u>.

4.8. We also ask Government to provide a clear outline, prior to the enactment of the new Act, as to how it intends to compensate providers for additional expenses incurred in order to make changes to processes and systems to comply with the new Act. For example, any change to the definitions of what data must be retained or what communications must be intercepted will require providers to undertake significant work to revisit and update existing processes and systems.

This could be similar to the Data Retention Industry Grants Programme that partially compensated providers for expenses incurred for the implementation of the Data Retention regime.

4.9. If an all-encompassing, or at least very broad, definition of 'communication' is indeed being contemplated, it may be necessary to decouple (as is currently the case) the

[11] p.20, ibid
[12] Reference as accessed at https://www.statista.com/statistics/1202887/australia-average-number-of-internet-connected-devices-per-household/ on 4 Feb 2022
[13] Reference as accessed at https://www.iotaustralia.org.au/2019/06/19/iot-facts-and-forecasts/idc-says-by-2025-41-6b-iot-devices-will-be-generating-79-4-zettabytes-of-data/ on 4 Feb 2022
[14] Reference as accessed at https://www.eecis.udel.edu/~amer/Table-Kilo-Mega-Giga---YottaBytes.html on 4 Feb 2022

requirement to protect communications from the retention requirements and only require the retention of certain data sets from within that definition. Anything else appears impractical from a data storage, retrieval and security perspective, and may also be undesirable from a human rights perspective.

'Content' vs 'non content'

4.10. The Discussion Paper correctly indicates that the existing framework does not contain a definition of 'content and substance'.

The Discussion Paper also usefully points to the PJCIS's recommendation to define 'content and substance of a communication'.[15]

4.11. Our members agree that the current framework lacks such a definition, and that the introduction of a definition may be beneficial. The UK model represents a sound starting point for thinking regarding the definition of 'content'.

4.12. However, the definition of 'content' proposed in the Discussion Paper is overly broad. The Discussion Paper makes no reference to the second part of the same PJCIS recommendation which says that "in defining the term "content or substance of a communication", Home Affairs should specifically consider 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."[16]

It is also key to note that the PJCIS did not confine the purpose of a definition of 'content and substance of communication' to greater certainty for those who have to work with the definition, but recommended the definition be amended "for the purpose of providing greater certainty and enhancing privacy protections" [emphasis added].[17]

4.13. Particularly in aggregation, metadata can reveal information more important than what would be considered the 'classical content of a communication'. This becomes even more true through algorithmic analysis and tools that artificial intelligence offers and the inferences that now will be able to be made and which were previously unavailable to LEAs.

4.14. Our members echo the PJCIS's sentiment and disagree with the notion put forward in the Discussion Paper that non-content information (or metadata) is, per se, less revealing than content information. Metadata can be very revealing and can constitute personal information, depending on the surrounding circumstances. As such, the distinction between content and non-content information and the resulting requisite level of authorisation for information for each type is highly contentious. We believe that the warrantless system for accessing all metadata may not be suitable, in its current form, for the new framework and ought to be re-worked.

4.15. It is also key to understand that the distinction between content information and so-called non-content/metadata of communications is critical for operational and implantation purposes of any proposed solutions and could substantially impact the type of technical solutions that providers would be able to offer. Therefore, extensive and timely consultation is required.

4.16. Irrespective of the categorisation of any information, a clear obligation ought to be placed on LEAs, to not use and to destroy, as soon as practicable, any information that they receive either inadvertently or as part of their requests, where information that was not requested cannot be separated from information that was requested.

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

Definition of 'national security'

4.17. As previously noted in the context of the Critical Infrastructure reforms, the current national security framework does not adopt a single consistent definition of 'national security'. This is problematic and ought to be rectified.

4.18. The requirement to "do the carrier's best […] to protect the telecommunications networks and facilities owned, operated or used by the carrier or provider from unauthorised interference or unauthorised access […]" contained in section 313 of the *Telecommunications Act 1997* has been seen by our members in the context of 'classical' national security risks such as espionage, sabotage and foreign interference. Our members have not raised any concern about the inclusion of 'politically motivated violence' as one of the examples of national security risks.

4.19. However, our members are concerned that different pieces of legislation that strongly relate to or the sole purpose of which it is to strengthen national security, do not adopt a single, well-defined definition of 'national security'.

4.20. How are critical infrastructure organisations across different sectors supposed to implement a risk-based approach to national security compliance, when the definitions of 'national security' in different pieces of legislation that these organisations are subject to are not identical, let alone consistent?

4.21. Any additional confusion or ambiguity introduced due to variations in definitions unnecessarily adds to risks that need to be managed by industry and ought to be eliminated.

4.22. We have previously commented (in our submission to the PJCIS in Feb 2021) on the proposed definition of 'national security' in the SoCI Act and have reproduced our response below for your convenience:

> *Section 5 of the SOCI Act defines national security as "Australia's defence, security or international relations". This definition is broad and does not limit national security to any specific activities. However, the definition of national security is key to the operation of the draft legislation, including the rule-making powers, the Ministerial declaration powers and the far-reaching directions powers. Importantly, the Explanatory Document cites national security concerns as the primary reason for exempting the Ministerial authorisations under Part 3A of the draft legislation from judicial review under the Administrative Decisions Judicial Review Act 1977.*[18]
>
> *Given the wide scope of the current national security definition and the intrusive nature of the powers (and attendant penalties for non-compliance), we urge Government to adopt a more narrow definition which ties national security to specific activities, conducts and interests. The current definition of national security under section 90.4 of the Criminal Code Act 1995 might provide a useful approach. Alternative, it is also worth noting that section 5 of the SOCI Act already includes a definition of security which references the definition of the Australian Security Intelligence Organisation Act 1979 (ASIO Act). The latter, in turn, includes more specificity on the activities that could be considered a threat to Australia's security. Therefore, the ASIO Act definition of security would also be preferable to the definition of national security of section 5 of the SOCI Act. In fact, it is hard to see why a separate definition of national security is required given the existing (and referenced) definition of security in the ASIO Act.*
>
> *If the definition of national security was to be retained, at the very least the individual terms that make up the definition of national security, i.e. 'defence', 'security' and 'international relations', should be defined within the legislation rather*

[18] p.65, Department of Home Affairs, *Explanatory Document, Security Legislation Amendment (Critical Infrastructure) Bill 2020,* Nov 2020

than be left to their ordinary meaning. In this context, section 10 of the National Security Information (Criminal and Civil Proceedings) Act 2004 may offer a useful reference point which would also provide consistency with Australia's commitments to the United Nations Norms of Responsible State Behaviour in Cyberspace.[19]

'Stored' vs 'live' communications

4.23. The Discussion Paper considers the distinction between 'stored' and 'live' communications to be less important than it once has been. It is not clear whether it proposes to no longer make any form of distinction between those types of communications in the future.

4.24. While we tend to agree with the general principle that the distinction between the two types of communications is less important today, it will require careful consideration and consultation with the sector to get definitional aspects of the context right.

4.25. Furthermore, 'live' and 'stored' communications should be subject to heightened safeguards as both forms of content can be highly personal and revealing.

Emerging technologies

4.26. Emerging technologies often evolve faster than legal frameworks. As technologies, and data collection tools evolve, surveillance often takes entirely new forms. Therefore, a technology neutral framework will reform efforts to avoid becoming either obsolete or overly broad. For this reason, the framework should remain neutral in language, avoiding calling out specific technologies.

However, this must not result in the adoption of all-encompassing, unclear thresholds and definitions, so as to render the Act a catch-all piece of legislation that avoids appropriate nuance and distinctions.

4.27. With the increasing prevalence of artificial intelligence, the new framework will need to set clear boundaries as to how inferences and intelligence gained from surveillance data at scale can be used, if such use is permissible at all. It will be especially important to be transparent and accountable with respect to technologies that are not easily understood from a technological perspective by the community, in order to gain and maintain the requisite level of trust in the surveillance framework.

Which providers ought to be covered?

4.28. The Discussion Paper indicates that the current framework only applies to carriers and carriage service providers (C/CSPs), but also notes that a number of other legislative options exist to compel a large range of organisations operating in the communications supply chain to provide assistance.

4.29. Indeed, the *Telecommunications Other legislation Amendment (Assistance and Access) Act 2018* applies to such a wide scope of organisations that almost any entity operating in this space, including the operator of a single website, is bound by its provisions to assist ASIO and LEAs.

4.30. The Discussion Paper hints at the possibility (or even likelihood) that the future electronic surveillance framework will extend to all organisations that facilitate communication:

"The new framework will aim to provide greater clarity about which kinds of communications service providers must execute, or assist with the execution of,

[19] As accessed at: https://www.dfat.gov.au/international-relations/themes/cyber-affairs/international-security-and-cyberspace) on 26 Nov 2020

electronic surveillance warrants, authorisations or assistance orders. In developing the framework, the Government will consider what kinds of entities involved in the communications supply chain, in addition to traditional carriers and carriage service providers, must meet these obligations. Changes may be needed if existing or potential future providers the community would expect to be subject to these obligations are not captured. The question of which obligations should apply to which providers is further discussed in ***Part 6****."*[20]

Unfortunately, the Discussion Paper does not provide any further information as to what Government's considerations will involve or which criteria it will apply to limit the scope of providers that could be subject to obligations. Part 6 also does not give any further indication of how the issue may be addressed but instead only lists three legislative reviews (Assistance and Access Act, Data Retention, TSSR) and other areas for reform (Interception Capability Plans and attribute-based interception) on which we comment further below.

4.31. We agree with the Discussion Paper's assessment that "Any change to the range of providers that must provide communications or technical assistance to agencies should avoid placing unnecessary additional burdens on Australian industry. Any change would also need to consider jurisdictional limitations."[21]

Speaking from our members' experience, even so-called 'targeted' data retention schemes are often broadly scoped, very complex and very burdensome to implement.

4.32. The Discussion Paper mentions data centre (DC) operators as one category of providers currently not captured under the framework, that may be of potential interest for the future surveillance framework.[22]

4.33. **We believe that DC operators ought not have any obligations, including data retention, lawful interception and complying with warrants, authorisations and assistance orders under the new framework.** A DC operator does not have any visibility or insight into what, if anything, might be stored or processed on its customers' servers, let alone any ability to identify or distinguish the end-users or uses of those servers. The particular servers that are used to store or process an end-user's data can also change dynamically (including by shifting to servers in another DC entirely) without the knowledge or involvement of the DC operators concerned.

Further, unlike C/CSPs, which control a network, a DC operator may not own or operate the servers located inside its DC, but instead provide its operating environment (i.e. power, climate and physical security). The servers remain under the exclusive control of the DC operator's customer and each such customer will have its own monitoring technical solution in place to detect and respond to any electronic or physical tampering with its equipment. The DC operator has no ability to circumvent those measures, which means surreptitious access to the customer equipment inside a DC is impossible.

The DC's customers are responsible for managing their own data on their IT equipment and the security of their data both in storage and in transit.

4.34. Consequently, in the absence of any compelling reasons to include additional providers, we do not believe that an expansion of the surveillance regime ought to be progressed.

If Government believes such an expansion would be beneficial, then it ought to clearly identify the gaps of information in current investigatory practice and to subject the

[20] p. 29, Department of Home Affairs, *Reform of Australia's electronic surveillance framework* Discussion Paper, Dec 2021

[21] ibid

[22] p.38, Department of Home Affairs, *Reform of Australia's electronic surveillance framework* Discussion Paper, Dec 2021

retention and accessibility of such information to a rigorous cost-benefit analysis, including any potential effects on the privacy of citizens.

5. How can information be accessed?

5.1. Part 3 of the Discussion Paper is devoted to the question as to how LEAs and ASIO can access relevant information as and when required.

To resolve complexities with the current framework and to address difficulties that arise from changes in technology, the Discussion Paper proposes to introduce a technology-neutral, outcomes-based framework where warrants are being sought for particular types of information, irrespective of the means through which that information has been gained. The Discussion Paper proposes that requesting agencies would likely need to justify that the method of access proposed is necessary and proportionate and/or the least intrusive with respect to the privacy of the individuals involved.

5.2. While the proposal is not without merit, it is significantly flawed in that it neglects to consider that it proposes, as far as we understand from the detail provided, to apply this regime only to the warrants that currently exist and to warrants that will be required for new categories of communications that are proposed to fall under the (new) definition of 'content'.

However, we have already noted our concern with the principle that all metadata would always be considered non-content information and, therefore, be available under authorisation and, consequently, also not be subject to the justifications mentioned above with regards to necessity, proportionality and intrusiveness with respect to privacy.

We have commented that we do not believe that the current distinction between 'content' and 'non-content' (metadata) can be maintained with a warrantless regime for all metadata.

5.3. We have serious reservations about the proposed outcomes-based regime for warrants that would focus on only some categories of content information, and leave large areas of metadata subject to authorisation. This approach would likely lead to a substantial increase in the use of large-scale surveillance by means of metadata and subsequent analysis, given the lack of, or at least substantially lower threshold for, justification that needs to be provided. At the same time, the data, especially when used in aggregation, would prove very powerful and, so we believe, often not inferior to other data sources.

5.4. Therefore, we recommend the proposed approach be reconsidered and a common set of principles apply across all types of information and agencies. If this is not possible the approach ought to at least be augmented and additional categories of information included to ensure that the most intrusive forms of information will be appropriately protected in a future surveillance framework.

5.5. Further, the regime should require LEAs and ASIO to obtain a warrant in circumstances in which there is a dispute as to whether data is appropriately classified as content, as opposed to non-content.

5.6. The regime should also include a mechanism to ensure and enforce rules against unlawful use of data for political or public communication, to obtain privileged information, identify a journalist source or a whistle-blower and provide a mechanism that applies across the system to protect privileged information and the source of information provided to journalists and protect whistle-blowers.

5.7. Moreover, the regime should have a common reporting regime which ensures that warrants and authorisations targeted across communication service providers are reported annually by Home Affairs, both in terms of numbers, the offences for which

they were sought, whether or not information was relevant to the prosecution of those offenses and how many prosecutions resulted. Further consideration should be given to all the relevant facts regarding the operation of the proposed new system that would allow it to be properly understood, reviewed and approved overtime. In addition, service providers should be allowed to report basic information regarding the information they have provided to Government agencies, the threshold met before that information was made available and its uses. It is important to industry providers that they can be transparent with their customers regarding the services they are providing how, generally, data is being used. (Also refer to our section on transparency further below.)

6. When will information be accessed?

Harmonising thresholds

6.1. The Discussion Paper proposes that the new framework aim to harmonise the existing thresholds to access information for functionally equivalent powers.[23]

6.2. It proposes that the thresholds for ASIO to use its powers to intercept, access stored communications, access computers or use optical and listening devices be contingent on whether ASIO suspects that the person is engaged in, or is likely to engage in, activities relevant to security.

6.3. It also proposes to reduce the thresholds for LEAs to engage in interception or access the above information to, by and large, crimes punishable by a maximum penalty of at least 5 years (from currently 7 years), or for some crimes related to cyber offences, by a maximum penalty of at least 3 or 2 years.

6.4. The Discussion Paper does not make a concrete proposal with respect to new thresholds for access to metadata but states:

> *"The new framework will implement the Government's response to the PJCIS review of the mandatory data retention regime. In implementing this response, the Government will consider whether the existing thresholds and authorisation requirements for law enforcement agencies and ASIO to access telecommunications data remain appropriate. The government will also consider requiring these agencies to satisfy a proportionality test before access to telecommunications data is authorised."*[24]

One current threshold of section 5D of the *Telecommunications (Interception and Access) Act 1979* is based on the threshold of 'serious offence' which, as defined in that Act, attract a maximum penalty of at least 7 years imprisonment.

6.5. As previously noted, Government has, lamentably, still not provided a response to the October 2020 PJCIS report. As such it is unclear which, if any, response to the review Government will give and, therefore, what thresholds for access to metadata it considers. We would welcome further detail and discussion.

We believe a harmonisation of legislative thresholds would be appropriate. However, thresholds should be determined having regard to proper consideration of the intrusion into the privacy of individuals rather than an assessment of 'functional equivalence' (which may already be flawed).

6.6. If a threshold using the proposed approach must be set, we point to the PJCIS recommendation that Commonwealth legislation be reviewed with view to harmonising the use of the term 'serious offence' and to making it an indictable

[23] p.39, Department of Home Affairs, *Reform of Australia's electronic surveillance framework* Discussion Paper, Dec 2021

[24] p.43, Department of Home Affairs, *Reform of Australia's electronic surveillance framework* Discussion Paper, Dec 2021

offence punishable by a maximum penalty of seven years' imprisonment or more, with a limited number of exceptions.[25] We recommend this threshold be used as a starting point for the considerations of a 'functional equivalence' approach.

Location information

6.7. The Discussion Paper suggests that "tracking information may have less impact on privacy than other surveillance information, particularly where that information is devoid of the greater substance and context derived from access to a person's communications."[26]

6.8. In line with our previous argument at sections 4.10-4.16 (that a clear distinction between intrusive 'content' information vs non-intrusive (or at least significantly less intrusive) non-content (metadata) cannot be made) we note that while this may be the case, in many instances the opposite can be the case. Location data can be very precise or very coarse depending on the service and the circumstances surrounding collection.

Consequently, we recommend that location information not be subject to any lesser access requirements than already the case. Instead, we recommend that higher thresholds be considered.

7. Safeguards and oversight

Oversight

7.1. The Discussion Paper asks the question whether additional safeguards (i.e. in addition to those that already exist under current legislation) will be required once existing safeguards have been harmonised.[27]

7.2. The current framework does not appear to place many limitations on LEAs to request prospective communications data at large scale, for a large geographic area and range of devices/communications. The disclosure of the requested information only needs to be

> *"[…] reasonably necessary for the investigation of*
>
> *(a) a serious offence; or*
>
> *(b) an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years."*[28]

An authorisation for such a disclosure comes into effect immediately and can last for 45 days from the day the authorisation is made.

7.3. Given the capabilities of modern data analytics and artificial intelligence and given the potential intrusiveness of the disclosure of metadata and other communication information into the privacy of individuals, this potential for data collection at scale through an authorisation (i.e. by a senior offer of the agency requesting the data) instead of a warrant, and without further oversight is, in our view, an unacceptable risk to the privacy of individuals. This risk ought to be remedied through the reforms.

[25] p. 135, para 6.71, Recommendation 12, Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*, Aug 2021
[26] p.45, Department of Home Affairs, *Reform of Australia's electronic surveillance framework* Discussion Paper, Dec 2021
[27] pp. 62/63 and Q 28, Department of Home Affairs, *Reform of Australia's electronic surveillance framework* Discussion Paper, Dec 2021
[28] Part 4-1, section 180(4), Telecommunications (Interception and Access) Act 1979

7.4. We recommend considering a warrant regime for disclosure of metadata on an ongoing basis (as opposed to a 'one-off' point in time disclosure) and/or disclosure at scale.

7.5. We are pleased to see that the Discussion Paper acknowledges the "critical role" that the INSLM plays in "conducting reviews of electronic surveillance-related legislation to ensure it contains appropriate protections for individual rights, remains proportionate to national security threats and is necessary."

We are, therefore, disappointed that Government has, more than one and half years after its release in June 2020, not shown any sign of responding to or implementing any of the measures that the Independent National Security Legislation Monitor (INSLM) recommended in its important report *TRUST BUT VERIFY A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters*.

7.6. Consequently, we believe that the new framework now ought to give consideration to an oversight framework with an Investigatory Powers Commission as recommended by the INSLM in its report. While the warrant-based approach for some communications data and interceptions may not be oversighted by such a Commission, consideration should be given as to where the electronic surveillance framework and the use of the far-reaching powers granted under it, sit in relation to such a Commission (or whether it ought to be oversighted by it?) which ought to be established for various other pieces of the overall security framework (e.g. *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*).

7.7. It may also be useful to consider the powers and role of the Commonwealth Ombudsman, given his current (and foreshadowed ongoing) role in the oversight of the framework.

With the increasing importance of electronic surveillance in our society, it appears appropriate to ensure that the institution that oversights such framework is adequately protected, truly independent and well-resourced, in order to properly discharge of its functions.

The New Zealand approach of dividing parliamentary oversight between distinct parliamentary committees (budget, strategy, oversight) may be an interesting model for consideration.[29]

Protection of information obtained by officers

7.8. In order to foster greatest possible trust that any information disclosed to LEAs and security agencies will not be misused and is safe from interference etc., the new Act ought to place a statutory obligation on officers handling the information to protect the information and to only use it within the (narrow) remit for which the information was sought.

Statutory protections for legally privileged information

7.9. The Discussion Paper raises the question whether there a need for statutory protections for legally privileged information (and possibly other sensitive information, such as health information)?[30]

[29] Anita Stuhmcke, The Commonwealth Ombudsman: still fit for purpose? as accessed at https://auspublaw.org/2021/09/the-commonwealth-ombudsman-still-fit-for-purpose/ on 9 Feb 2022
[30] p. 63, Q 29, Department of Home Affairs, *Reform of Australia's electronic surveillance framework* Discussion Paper, Dec 2021
p. 63, ibid

7.10. The regime should prohibit the use of surveillance and information gathering powers for the purpose of obtaining legally privileged information. It is not clear in what circumstances it would be appropriate for a national security or LEA to have access to information subject to legal professional privilege.

On the other hand, we do not believe the regime needs to make specific protections for sensitive information as defined by the *Privacy Act 1988* or health information. The protections that apply to all information obtained by use of lawful process should be sufficiently robust that they protect sensitive information and health information along with any data of individuals or other private information obtained using the process.

Minimisation of information provided about individuals not subject to an investigation

7.11. Internet service providers (ISPs) continue to receive requests for communications data (typically IP address, date and time) pursuant to s178(2) or occasionally s180[31] without specification of a subscriber TCP/UDP port number on the subscriber end associated with the request.

7.12. If the ISP is using CG NAT[32] for the IP address under consideration (which is increasingly likely due to IPv4 exhaustion), then the ISP will not be able to narrow down the information it provides to a single customer but instead will be forced to disclose information for up to 100 customers (sometimes even more) who may not be the subject of the lawful request for communications data.

7.13. Where available, LEAs always ought to provide the following information to ensure no valuable time is lost identifying the target of the request from the pool of information supplied by the Carrier/ISP and to ensure that the amount of data that does not related to the target of the investigation is minimised:

1. Subscriber IP address;
2. Subscriber TCP/UDP Port;
3. Date; and
4. Time- HH.MM.SS (UTC - Universal Time Coordinated).

7.14. We recommend that a common template for data requests be developed that includes these data fields for mandatory completion (or, as applicable, to be marked as 'not available' so as to assure the ISP that the agency has considered all of these items.)

Transparency

7.15. Question 30 of the Discussion Paper considers the expectations of the public, including industry, in relation to oversight, and how those expectations could be met. In addition to the above considerations we offer the following thoughts in relation to transparency.

7.16. We expect that most Australians, and customers of our members' services, share our members' desire to assist LEAs and security agencies to prevent crime and enforce the law and, consequently, accept that, to a certain extent, and when necessary and

[31] *Telecommunications (Interception and Access) Act 1979*

[32] Carrier Grade NAT (CG NAT), also known as large-scale NAT is an approach to IPv4 network design in which end-sites are configured with private network addresses that are translated to public IPv4 addresses by middlebox network address translator devices embedded in the Carrier's network, permitting the sharing of small pools of public addresses among many customer end-sites. This shifts the NAT function and configuration thereof from the customer premises to the Internet service provider network.32 CG NAT is also used in residential and mobile networks. (Source, Wikipedia) CG NAT is being used by Australian Internet Service Providers (ISPs).

subject to the respective laws and appropriate procedures, their privacy may at times be impacted by electronic surveillance legislation.

In return, they expect, to the greatest extent possible (ex-post) transparency from authorities as to when or in what manner such infringements may have occurred and whether the infringement of their privacy was proportionate to the crime under investigation.

7.17. Generally speaking, we believe that, at this juncture, simplicity and transparency are paramount to creating a framework that is easily understood and, importantly, trusted by the broader public.

7.18. Therefore, we recommend the new framework adopt a robust and comprehensive reporting regime.

The recommendations made by the PJCIS in its report on the review of the mandatory data retention regime in relation to improved reporting would provide a useful starting point. In particular, Recommendation 7 of the report, which the Committee recommended for implementation within 18 months of its October 2020 report, is as follows:

> *"5.41 The Committee recommends that, in consultation with other stakeholders (agencies with access to the Mandatory Data Retention Regime, the Inspector General of Intelligence and Security, the Commonwealth Ombudsman and the Commonwealth Privacy Commissioner), the Department of Home Affairs should within 18 months of this report develop guidelines for data collection to be applied across the Mandatory Data Retention Regime and the most cost effective way to achieve the intended outcome of facilitating better oversight, including an ability for enforcement agencies and Home Affairs to produce reports to oversight agencies or Parliament when requested.*
>
> *As a minimum, any such report should include the following information (in respect of each occasion on which the powers in Chapter 4 of the Telecommunication (Interception and Access) Act 1979 were used):*
>
> - *the section of the Telecommunication (Interception and Access) Act 1979 used to access the data;*
> - *the case number associated with the authorisation;*
> - *the specific offence – or offences – that the investigation related to;*
> - *if the authorisation related to a missing person case, the name of the missing person*
> - *brief reasons why the authorised officer was satisfied that the disclosure was reasonably necessary;*
> - *where the data related to a person who did not have an obvious relationship to a suspect in an investigation, brief reasons why the authorised officer was satisfied that any interference with the privacy of the person that may have resulted from the disclosure or use of the telecommunications data was justifiable and proportionate;*
> - *the name(s) of the officers involved in the case;*
> - *the name and appointment of the authorising officer;*
> - *if the agency became aware that the carrier disclosed any of the information referred to in section 187A(4) and action taken.*
>
> *Where practicable, the report should also include:*
>
> - *whether or not the data was used to rule someone out from an investigation;*

- *whether or not the person whose data was accessed was eventually charged, prosecuted and/or convicted of a crime;*
- *whether or not the data accessed eventually led to the charge, prosecution and/or conviction of another person for a crime; and*
- *the cost of the disclosure.*

For the Australian Security Intelligence Organisation, the additional record-keeping requirements should include:

- *the nature of the national security risk that led to the authorisation being given; and*
- *brief reasons why the authorised officer is satisfied that any interference with the privacy of the person that may result from the disclosure or use of the telecommunications data is justifiable and proportionate."*

7.19. We also note that meaningful transparency and oversight through a reporting regime is only possible if the information to be reported on is being provided in a timely manner.

In this context, we urge the Department of Home Affairs to deliver the report on the operation of the TIA Act within the required timeframes (within 3 months after each 30th June plus time to table in Parliament[33]). The report is often delayed by several months, thereby not allowing industry, Parliament and the Australian public to transparently scrutinise the use of these intrusive powers. (Note: at the time of writing, the report for the year ending June 2021 was not yet available: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/telecommunications-interception-and-surveillance)

8. Working together: Industry and Government

8.1. As noted above, the Discussion Paper states:

> *"The framework will have some impact on industry. The need to protect the integrity and security of communications and networks will be front of mind. Industry assistance will continue to be required – for example, in intercepting communications and accessing telecommunications data. However, it is intended that streamlining the existing framework will ultimately lead to a reduced regulatory burden."*[34]

8.2. Given that the Discussion Paper suggests changes to key concepts such as communications and that more data be retained, it is very difficult at this point to see how the new framework will lead to a reduced regulatory burden for industry. To the contrary, the proposals appear likely to add to the regulatory burden.

Attribution-based interception

8.3. Part 6 of the Discussion Paper notes the option of Government compelling individual providers to develop and maintain attribute-based interception capabilities.[35]

8.4. We raise grave concern about such a potential power, if it were to be enshrined in the new Act. It is indeed concerning to find this section of the proposed power in the part of the Paper titled "Working together: Industry and Government", when the contemplated

[33] Part 4-2, Section 186(1) and (1E)(3): "The Minister must cause a copy of a report under subsection (2) to be laid before each House of the Parliament within 15 sitting days of that House after the day on which the report was completed."
[34] p. 6, Department of Home Affairs, *Reform of Australia's electronic surveillance framework* Discussion Paper, Dec 2021
[35] p.71, ibid

power is a clear directions power, not dissimilar to a Technical Assistance Notice under the Assistance and Access Act.

8.5. While the Comprehensive Review notes the substantial costs that would accompany the development of any new attribute-based interception capability, there is also substantial complexity in how this proposal would be implemented as it requires the development of new capabilities for many of our members caught in scope.

We are extremely concerned with the implications that the implementation of such capabilities would have in relation to content scanning (for example where applied to some OTT services) and its consequences for the privacy and other human rights of the customers of the providers of services where these capabilities are being applied.

We would have equally as grave concerns about a regime that targets a single company or small number of companies alone, given the potential ramifications for competition and potential arbitrary nature of such a scheme.

Therefore, we strongly oppose the inclusion of any powers concerning attribution-based interception.

Interception Capability Plans

8.6. We recommend reducing the regulatory burden associated with submitting Interception Capability Plans on an annual basis. We welcome a less burdensome approach and the streamlining of material that needs to be included in any Plan to the most critical items needed for the agencies to be able to execute warrants effectively. For example, the current requirement to include relevant developments within a 5-year period that are likely to affect interception capabilities should be removed.

Exemptions

8.7. Establishing, maintaining and changing interception capability requires significant time and resources for carriers. The current uncertainty that the Communications Access Co-ordinator (CAC) could make a decision to refuse an application for an exemption under Part 5-3, section 192(6) of the TIA Act more than 60 days after an application was lodged presents unnecessary commercial risk. There should be no equivalent to section 192(6) in the new framework. Exemptions are also frequently subject to time limitations and providers need to re-apply before the expiry of the existing exemption to see if the exemption will be allowed to continue. This creates unnecessary commercial risk.

Furthermore, guidelines should be developed by the CAC to provide more certainty on when a carrier may or may not expect to be granted an exemption and whether such an exemption will be provided for the life of the exempted product/service.

Form of requests & hierarchy of requests

8.8. From a practical perspective, some of our members have found that requesting agencies do not always understand or aware of the requirements and processes concerning authorised officers making requests for data.

For example, at times initial contact is made with call centres or retails outlets, or through informal emails or letters, rather than through established contacts and processes.

As previously indicated, the new framework ought to require formal requests, in a uniform format, to specify a finding of materiality or relevance of the requested information to the investigation, and be issued by a duly authorised official.

When such formality/authorisation is absent in initial contacts with providers, this may have the potential to slow down the response time and to cause extra work for providers to request the appropriate authorisation.

Consequently, we recommend a uniform process and template for making requests with clear guidelines around form and contacts to assist with a more streamlined process.

8.9. With the increasing importance of electronic surveillance, it is likely that the number of requests for information will rise. As it stands, providers are already faced with a very high number of requests for data, which is steadily increasing.

Often providers are facing multiple requests at the same time from different LEAs. Where providers are not in a position to fulfil all requests simultaneously, providers ought not be left with the task of establishing a hierarchy of fulfilling the requests for information.

8.10. Therefore, we recommend the new framework, or an associated rule framework, establish standardised criteria of urgency for requests (i.e. so as to avoid a situation of requests discretionarily being characterised as being urgent) potentially coupled with a hierarchy of agencies making the requests.

Timely and clear guidelines

8.11. The new framework will need to be accompanied by timely guidelines to ensure that providers are clear as to the scope of their obligations. These guidelines need to cover both any new obligations as well as how the new framework impacts on existing obligations such as data retention and lawful intercept.

9. Conclusion

Communications Alliance looks forward to continued engagement with the Department and other relevant stakeholders on this important reform of Australia's electronic surveillance framework.

We support the review of the surveillance framework and recognise opportunities it offers for harmonisation, clarification, consolidation and updating of various pieces of legislation that currently form Australia's electronic surveillance framework.

However, we are concerned that the proposals put forward in the Discussion Paper do not, as suggested, bring less regulatory burden for our industry but rather would result in substantially more regulatory impost due to a substantially increased scope of data to be retained, both in terms of the data sets as well as of the providers in scope of the framework. We are also concerned with what appears to be a lack of recognition of the potency of so-called non-content (metadata), especially at scale and when collected over time and analysed with algorithmic means, in the context of a future oversight regime.

We continue to lend our support to the overarching objectives of a new Act and stand ready to work with all stakeholders to develop a practical, technology-neutral framework that allows LEAs and security agencies to fulfil their critical roles while adequately protecting individuals' privacy.

For any questions relating to this submission please contact Christiane Gillespie-Jones on 02 9959 9118 or at c.gillespiejones@commsalliance.com.au.

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E
info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507