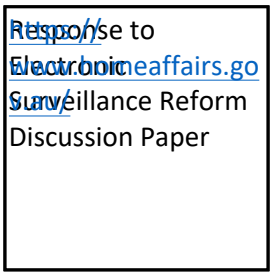
TELSTRA CORPORATION LIMITED

REFORM OF AUSTRALIA'S ELECTRONIC SURVEILLANCE FRAMEWORK

Public submission

18 February 2022



CONTENTS

EXECUTIVE SUMMARY

Telstra welcomes the opportunity to make a submission to Department of Home Affairs *Reform of Australia's electronic surveillance framework Discussion Paper* (**Discussion Paper**). We are a major builder and supplier of telecommunications networks and services, with a large customer base and a long history of providing lawful assistance to national security and law enforcement agencies.

Lawful interception of communications and access to telecommunications data is an important tool for Australia's law enforcement and national security agencies (**agencies**) that helps protect lives and solve serious crimes in this country. At the same time, an appropriate balance needs to be struck between delivering safety and law enforcement to protect the public and meeting Australian consumers' expectations of privacy and minimising the regulatory burden imposed on industry.

Simplification and clarity for all requirements

From our perspective, as a party that needs to comply with the new regime, the review should result in a simpler framework that removes any existing ambiguities and allows the electronic surveillance powers to be used consistently by agencies to investigate serious offences, subject to uniform tests of reasonableness and proportionality. To achieve this outcome, it will also be necessary to consider how the new framework interacts with existing obligations under the *Telecommunications Act 1997*, particularly those in Parts 13, 14 and 15.

Consistency of access

We recommend that all agencies requesting access to telecommunications data are required to follow the process set out for enforcement agencies in Division 4 of Chapter 4 of the TIA Act. All agencies obtaining data should meet the same threshold and be satisfied that access to information and data is reasonable and proportionate in the circumstances. This approach reduces the burden on carriers and carriage service providers and ensures consistency across the obligations for all agencies when requesting data.

Close collaboration with industry will required in developing the new framework

The existing interception, stored communications, mandatory data retention and surveillance devices frameworks are well understood by agencies and industry. In developing the new framework, particular care should be taken to ensure it retains that level of understanding and that any newly worded obligations to provide information and data are clear and easily understood by all parties that will be required to comply with the new framework. Achieving this outcome, while minimising the risk of unintended consequences and without imposing unnecessary burden on industry, will require close collaboration between government, the agencies and industry during the development of the new framework.

01 Who can access information under the new framework?

The new framework will need to balance the protection of privacy against law enforcement and security objectives. Much of the *information and data*[1] considered by the Discussion Paper is personal information. Access should be limited to the investigation of serious offences and should only be granted when reasonable and proportionate in the circumstances.

The new framework should set a clear threshold for the type (or seriousness) of offence for which information and data can be obtained.[2] Access to information and data by any agency should not be allowed unless that threshold is met.

1. **Do the existing prohibitions and offences against unlawful access to information and data adequately protect privacy in the modern day?**

   a. If so, which aspects are working well?

   b. If not, which aspects are not working well and how could the new prohibition and/or offences be crafted to ensure that information and data is adequately protected?

The existing interception, stored communications, mandatory data retention and surveillance devices frameworks are well understood by agencies and industry. In developing the new framework, particular care should be taken to ensure it retains that level of understanding and that any newly worded obligations to provide information and data are clear and easily understood by all parties that will be required to comply with the new framework.

We are of the view the following aspects of framework could be improved to provide adequate and consistent privacy protection:

- Rather than having differently worded privacy considerations for the exercise of different powers or the issuing of different warrants, the new framework should include a single set of privacy considerations which should apply to all government agencies seeking access to information and data. The relevant officer of an agency making an authorisation or applying for a warrant should be required to be satisfied on reasonable grounds (as should any issuing authority) that any interference with the privacy of any persons is reasonable and proportionate when taking into account those privacy considerations (such as, the seriousness of the offence and whether there are alternative, less intrusive, means to obtain the information sought).

- Under the current mandatory data retention framework, as noted in the Discussion Paper,[3] a number of Government agencies who are not enforcement agencies under the *Telecommunications (Interception and Access) Act 1979* (**TIA Act**) are able to access telecommunications data using other Commonwealth or State legislation. Most of these laws have no requirement for the requesting agency or officer to consider privacy when exercising these powers and contain no specific cost recovery provisions. Any agency able to access telecommunications data or content should (1) be specifically

---

1 The Discussion Paper uses the phrase 'access to information and data' to refer to the use of electronic or technologically-assisted means to covertly listen to or read a person's conversations or messages, access a person's electronic information or observe a person's activities and movements – collectively, electronic surveillance powers. This includes activities such as intercepting phone calls, remotely accessing a person's computers or using a listening or tracking device. The terms 'information and data' are used to refer to any kinds of information that could be obtained through these methods.

2 Recommendation 12, Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*, Aug 2021 and 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 Discussion paper, p16.

required to consider whether the interference of privacy is reasonable and proportionate when exercising these powers; and (2) be required to reimburse service providers on a cost recovery basis. We strongly believe the consistent application of privacy considerations to, and cost implications for, any government agency with powers to access telecommunications data will result in additional privacy protection as this will reduce the scope of requests and therefore, the amount of data being disclosed. As a service provider, consistency in approach across all agencies in accessing telecommunications data will also reduce our need to interpret multiple different access powers across numerous pieces of Commonwealth, State and Territory legislation.

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

The existing prohibitions and offences against unlawful access to information are outdated and do not account for recent developments in technology. The current drafting creates uncertainty and therefore, hinders the ability of service providers to undertake a range of activities which may not only be necessary for the protection of telecommunication networks and services but would likely be activities the public would be expecting their telecommunication providers to undertake. These could include activities such as utilising technology to scan communication content to identify and block malicious content to protect users from scams.[4]

To ensure that the prohibitions and offences which protect against the unlawful access to information and data do not inadvertently prevent service providers from undertaking important network security and fraud prevention activities, there needs to be sufficiently clear exceptions to the offences. Exceptions should be principle-based so that a telecommunications provider can undertake activities in good faith for the purpose of protecting its network from cyber-attacks and its customers from scams.

Although we understand the *Telecommunications Act 1997* (**Telecommunications Act**) is not under review in this Discussion Paper, we believe it is important that the restrictions and exceptions in Part 13 of the Telecommunications Act also be considered in the development of the new framework. This is to ensure consistency and to remove any duplication with the provisions of the TIA Act. The review needs to ensure that all parties have clarity as to when and how exceptions to the general prohibition on the use and disclosure of telecommunications data applies.

We also believe the ability of telecommunication providers to respond to a court subpoena and a coroner's authority requiring access to stored communications should be clarified. The current wording of the stored communications offence under section 108 of the TIA Act means notice needs to be provided to either the sender or the recipient of a stored communication before it can be released to the court or coroner. We query if this is the intention of the legislation? If it is, clarity should be provided as to how notice can be given if the relevant individual is deceased. Is consent from the next of kin and/or the executor of the deceased's estate sufficient?

3. Are there any additional agencies that should have powers to access particular information and data to perform their functions? If so, which agencies and why?

We have no view on which specific agencies should (or should not) have access to information and data under the new framework other than that, as access to information and data represents a significant intrusion of privacy, access should be limited to the investigation of a 'serious offence'. As noted above,

[4] The interception and stored communications offence provisions in the TIA Act have prevented some C/CSPs from taking some measures in relation to identifying and blocking malicious SMS messages due to lack of clarity. This specific issue has been addressed through the Telecommunications (Interception and Access) Amendment (2021 Measures No. 1) Regulations 2021.

and subject to our comments in response to question 10, we believe the threshold for access should be standardised along with the reasonableness and proportionality tests. All agencies obtaining data should have to meet the same threshold and be satisfied that access to information and data is reasonable and proportionate in the circumstances.

4. **Do you agree with the proposed considerations for determining whether additional agencies should be permitted to access peoples' information and data? Are there any additional considerations that have not been outlined above?**

We agree with the proposed considerations. However, there should be a clearly articulated 'serious offence' threshold for obtaining access and all agencies gaining access should be required to meet the same reasonableness and proportionality tests. It is imperative that an agencies' access to electronic surveillance powers align with a clear and compelling function, with a threshold that considers the probability or likelihood that the information is needed to investigate an offence.

The proposed considerations for determining whether additional agencies should be permitted to access information and data should also consider the specific circumstances of each agency.

02 Part 2: What information can be accessed?

We agree the definition of communication should be updated in the new framework to reflect the modern way people communicate. However, we have some reservations about defining 'communication' to include things that would not meet the ordinary meaning of the word. For example, including electronic documents, files, images and other content that is not transmitted to another person and is not intended to be transmitted to another person. While it is likely such information (or content) would be available to agencies under the existing surveillance devices warrants, they do not meet the ordinary meaning of communications. Also accessing such material is unlikely to be interception.

We suggest the new framework may need to distinguish between access to 'communications' (whether they are accessed when in the process of being transmitted or when they have already been transmitted) and 'access' to 'information' (that is stored electronically). In developing definitions for the new framework, we strongly recommend the Department and agencies work closely with industry to ensure the concepts and definitions are clear and workable.

The new framework should also clearly distinguish between content and non-content information. For instance, as noted in the Discussion Paper,[5] there is a lack of clarity on whether a URL or web browsing information is content.

From our perspective, as a service provider, clarity for all of these concepts and definitions will be critical to understanding and complying with the scope of the new obligations.

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

The proposed inclusions seem comprehensive. As noted above, we believe there should be further consideration of whether all types of information identified by the Discussion Paper should be included in the definition of communications or whether other concepts and definitions should also be adopted.

Regardless of the approach taken by the Government, it is important to ensure that by expanding existing or developing new definitions that the flow on impact will not inadvertently impact the ability of

[5] Discussion Paper, p 24.

service providers from undertaking normal business activities such as cyber security and network operation and maintenance activities.

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

In developing the new framework, consideration should be given to whether some 'communications', should be exempted from the framework. There are already a vast number of Internet of Things devices deployed and operating and the number of connected 'things' is forecast to exponentially increase over the next few years as new technologies are rolled out. However, there appears to have been little consideration about the costs and benefits of requiring carriers and carriage service providers to store the mandatory telecommunications data for these devices. For example, it seems unlikely that the timing and length of data sessions from a smart meter which provides throughput or output measures at regular intervals would provide useful information to the listed law-enforcement agencies.

Such an exemption would be consistent with the recommendation of the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) that the Mandatory Data Retention Regime (**MDR Regime**) be amended to clarify that service providers are not required to store information generated by Internet of Things devices.[6]

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

In developing the new framework, consideration should be given to whether and how access to additional data and/or additional analysis by service providers could assist the agencies. For example, we recommend, as part of this review, that consideration be given to the scope of telecommunications data that should be accessible by agencies in relation to missing persons. Under the Assistance and Access framework in Part 15 of the Telecommunications Act, certain agencies have the ability to request or require additional assistance which could provide further information which would prove useful in the investigations to locate a missing person or in determining the circumstances of their disappearance. However, under the current framework, the Australian Federal Police (**AFP**) or State police forces can only request or require this assistance if they are *"enforcing criminal law in so far as it relates to a serious Australian offences" or* "*assisting the enforcement of the criminal laws in force in a foreign country, so far as those laws relate to serious foreign offences*". In the majority of missing persons cases, this is unlikely to be the case and therefore the AFP and State police forces will not be able to get the benefit of additional assistance.

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

The new framework should clearly articulate the difference between 'content' and 'non-content' information. There are ambiguities in the existing MDR Regime which have previously been considered by the PJCIS.[7] One example of an existing ambiguity (as mentioned above) is whether a URL is considered content or non-content information. This lack of clarity creates operational risks, where a customer's personal information may be incorrectly disclosed without the appropriate warrant. Clearly

6 Parliamentary Joint Committee on Security and Intelligence, *Review of the mandatory data retention regime*, October 2020, Recommendation 5, p. 99.

7 Parliamentary Joint Committee on Security and Intelligence, *Review of the mandatory data retention regime*, October 2020, pp.95-97.

defining the terms 'content' and 'non-content' information will also provide clarity for agencies in the handling and disclosing of personal information.

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

We agree there is some merit in the approach to the definition of content in the United Kingdom. In particular, that content is anything "which reveals anything of what might reasonably be considered to be the *meaning (if any)* of the communication".

We support the recommendation of the PJCIS that such a definition should be developed in close consultation with industry, the Commonwealth Ombudsman, the Inspector-General of Intelligence and Security, the Law Council of Australia and the Privacy Commissioner.[8]

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

There may be benefit in distinguishing entity data (information identifying the subscriber of a phone number or the holder of an email account, billing information etc.) from other more privacy intrusive 'event' data (such as call records and location data) and having different authorisation requirements for the different 'types' of data. It might, for example, be appropriate to allow a wider range of government entities access to 'entity' data while restricting access to 'event' data to a specific list of law enforcement and security agencies. The usefulness of such an approach should be considered in further targeted consultation.

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

We agree there is no need for continuation of the distinction between live and stored communications. We would support an approach, similar to that taken in the United Kingdom, where interception is defined as including accessing content whether during transmission or when it is held/stored before or after in a telecommunications system.

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

Yes, both involve the same level of intrusion into privacy.

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

The new framework should clearly articulate which providers of 'communication services' will have obligations. Carriers and carriage service providers have a long history of providing legal interception, reasonable assistance and, more recently, access to data under the MDR Regime. However, the proliferation of 'over the top' messaging providers, social media applications and an expanding communications supply chain means carriers and carriage service providers may not always have the information sought by agencies or be able to intercept communications in a meaningful way. As a general rule, and to avoid unnecessary burden on carriers and carriage service providers, we believe

8 Parliamentary Joint Committee on Security and Intelligence, *Review of the mandatory data retention regime*, October 2020, Recommendation 2, p. 97.

requests for assistance and interception should be directed to the party that has the information or is able to undertake the interception.

The definition of 'designated communications providers' in Part 15 of the Telecommunications Act would appear to be a good starting point for identifying the kinds of entities that should have obligations under the new framework, depending on the definition of 'communication' that is adopted.[9] Where the definition of 'communication' is expanded along with the relevant types of communications providers, care should be taken to avoid entities being inadvertently captured by the obligations. For example, providers of smart meters or organisations with internal messaging services.

Further, the new framework should enable agencies to seek communications from international 'over the top' providers (similar to Schedule 1 of the TIA Act) to address the impact of jurisdictional limitations.

14. What are your thoughts on the above proposed approach? In particular, how do you think the information captured by surveillance and tracking devices could be explained or defined?

We suggest that the framework should regulate the type of information that can be obtained using surveillance devices and should also work towards an outcomes-based warrant framework. We support the Government's intention in seeking clarity for the types of information agencies can obtain under each warrant and authorisation in the new framework. Following an outcomes-based approach for the framework will reduce complexity and allow for flexibility to endure, despite rapid technological advancements. Relying on subordinate legislation or rules to supplement the outcomes-based framework allows for detailed matters such as the methods of obtaining access to be accounted for. We agree that further consultation with the States and Territories should be undertaken to ensure a clear and consistent approach.

03 Part 3: How can information be accessed?

Reform of the key concepts underpinning the electronic surveillance framework (discussed in our responses to the Part 2 questions above) will be an important prerequisite for the successful streamlining of the warrant framework.

15. How could the current warrant framework be simplified to reflect the functional equivalency of many of the existing warrants while ensuring appropriate privacy protections are maintained?

We support a reduction in the number of warrant and authorisation types available to agencies, with the new warrants and authorisations being distinguished from one another by the type of information being accessed (shifting the emphasis from a method-based framework to a more outcome-based framework, as the discussion paper describes it) and by the level of intrusiveness of that access (following the categorisation applied in the Comprehensive Review's recommendations).

Such a reform would enable a common set of principles to apply across different agencies using a common set of data types, authorisations and warrants.

[9] The Explanatory Memorandum for Part 15 states: '*Designated Communications Providers are defined in the table in section 317C to include the full range of participants in the global communications supply chain, from carriers to over-the-top messaging providers. This reflects the multi-layered nature of the communications environment and the types of entities that could meaningfully assist law enforcement and national security agencies. It is crafted in technologically neutral language to allow for new types of entities and technologies to fall within its scope as the communications industry evolves.*'

16. What other options could be pursued to simplify the warrant framework for agencies and oversight bodies, while also enabling the framework to withstand rapid technological change?

Rather than having differently worded considerations/thresholds for the exercise of different powers or the issuing of different warrants, the same considerations could be compiled and listed in one section.

04 Part 4: When will information be accessed?

17. Is it appropriate to harmonise legislative thresholds (as outlined above) for covert access to private communications, content data and surveillance information where existing warrants are functionally equivalent?

We agree that where powers are functionally equivalent, they should be subject to the same limits, controls and safeguards. The new framework should harmonise the existing thresholds for functionally equivalent powers relating to intercepting communications, accessing stored communications, accessing computers, or using surveillance devices to access information.

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

We support reconsideration of the appropriateness of existing thresholds and authorisation requirements for Agencies in accessing data captured under the mandatory data retention regime as well as other telecommunications data held by service providers. We also agree with the proposed option that agencies must satisfy a proportionality test before access to telecommunications data is authorised. The same proportionality tests should be applied to any agency that is able to gain access to information and data.

There is potential to improve the controls that were implemented with the introduction of the MDR Regime. Although access to telecommunications data under the MDR Regime was restricted to certain agencies, it is questionable whether these controls are operating as effectively as intended. Various agencies and bodies have relied on section 280 of the Telecommunications Act to access telecommunications data, thereby circumventing the intended restriction and avoiding assessment of whether disclosure is reasonable and proportionate. There is an inherent risk that such access could erode the trust customers have with us in relation to the protection of their privacy.

We recommend that all organisations requesting access to telecommunications data are required to follow the process set out for enforcement agencies in Division 4 of Chapter 4 of the TIA Act. This reduces the burden on carriers and carriage service providers from verifying the coercive powers of every agency or department requesting the data. It clarifies that all entities seeking telecommunications data are also captured under the standard cost recovery system, to ensure consistency across the obligations for all agencies when requesting data and encourages agencies to make more targeted and limited data requests.

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

We do not agree that information about a person's location or movements is not as privacy intrusive as surveillance information, especially if considered over time. Location data to be collected under the new framework (or retained under existing legislation) can be used to develop an extensive view of a person's movements. As location data improves, agencies need to use 'human-source' or 'tracking device' surveillance may decrease and their reliance on location data increase. Accordingly, we consider a 'serious offence' threshold must be met in order to seek access to location information and that a

reasonable and proportionate in the circumstances test (such as that currently applying to authorisations under the MDR Regime) be satisfied by any agency seeking access to location information.

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

We support the proposed approach of warrants and authorisations to be targeted at a person in the first instance.

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

We support the proposal to standardise the thresholds and purposes for which third party powers can be used by law enforcement agencies and ASIO. Adding another requirement whereby the issuing authority needs to be satisfied that obtaining the information directly under a warrant would be impractical or ineffective, ensures that all reasonable avenues have been exhausted prior to getting a third-party warrant. Applying the higher threshold consistently across all third-party warrants appropriately balances privacy concerns, whilst providing agencies with the necessary powers to investigate serious criminal or security related conduct.

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

We recognise the difficulties with policing online activities and connecting them with specific individuals. Accordingly, we support introducing group warrant regimes for law enforcement agencies and ASIO to be applied consistently across all warrant types, corresponding with higher thresholds to ensure necessity and proportionality when applying for and issuing these warrants.

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

We support incorporation of a clear, express requirement to ensure electronic surveillance powers are only used where reasonable and proportionate. We also agree with the matters to be considered by an issuing authority when considering necessity and proportionality. However, we believe that agencies *should* also be required to establish this to the reasonable satisfaction of the issuing authority in any application for the ability to use a power.

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

We do not have any comment on who should have the power to issue warrants to agencies seeking to access information. However, we note that in relation to stored communications, agencies do not always need to go to an issuing authority for a stored communications warrant to access stored communications.

We understood that the stored communications regime under the TIA Act was to afford greater protection to content. However, due to the wording of section 108 of the TIA Act (which sets out the offence of accessing stored communications), some agencies have been able to utilise search warrants to access stored communications by giving prior notice to the relevant individual. We understand that generally, there is a lower threshold to be met for search warrants in some States, as they can be signed by a Justice of the Peace. If the intention is that content should only be accessed by agencies using a stored communications warrant, then the new framework dealing with access to communication content will need to be carefully drafted to prevent access via other means.

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

Maintaining strict controls on the ability to use and share electronically accessed information should continue to be a paramount concern. A consistent approach should be taken for limiting the use and disclosure of information across state and federal jurisdictions, including the timing of the destruction of information. A tiered approach for sharing information between agencies, guided by permitted purposes ensures clarity and direction to the way sensitive information will be handled. Destruction provisions should allow agencies to undertake operational needs and continue to perform their functions, whilst maintaining the privacy of individuals as a priority.

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

We agree with the proposed approach of considering destruction provisions in light of agencies' operational needs, performance of their functions, appropriate oversight and consideration of the privacy of individuals.

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

While we support the availability of emergency processes to the agencies for time critical and emergency situations, it is important that service providers are not put in a position or are required to take the risk on assessing the veracity of a verbal request. All requests to service providers should be in writing and be made to the provider via their normal channels for receiving agency requests. The use of existing processes (for instance, being sent from a known email address used regularly by the agency to make requests to a provider) will give the service provider confidence that the request is genuine. This will also give the service providers documentary evidence that can be retained for audit purposes. Service providers should also receive civil immunity if it actions such a request in good faith.

05 Part 5: Safeguards and oversight

Achieving clarity in the revised framework (for issues such as harmonising warrant thresholds and simplifying the provisions that govern how agencies use and disclose information) will assist oversight bodies to do their jobs effectively and will promote transparency and greater understanding of the framework by public and industry. We agree that the Independent National Security Legislation Monitor (**INSLM**) plays a critical role 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.[10] The INSLM's report into the assistance and access regime,[11] contains a number of recommendations related to safeguards and oversight of the Assistance and Access regime contained in Part 15 of the Telecommunications Act. We believe a number of these recommendations are also relevant to the proposed new framework.

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

The new framework 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.

[10] Discussion Paper reference p. 63.
[11] Independent National Security Legislation Monitor, *TRUST BUT VERIFY: A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters*, June 2020.

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

The new framework 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 law enforcement agency 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*. The protections that apply to all information obtained by lawful process should be sufficiently robust that they protect sensitive information along with any data of individuals or other private information obtained using the process.

30. What are the expectations of the public and industry in relation to oversight of these powers, and how can a new oversight framework be designed to meet those expectations?

While we expect that most Australians will view electronic surveillance as being necessary to assist the agencies to maintain Australia's security and enforce the law, they would expect these powers are used only in very limited circumstances. Where use of electronic surveillance is required, they would expect that the agency involved carefully consider whether the crime or security matter is of sufficient seriousness as to warrant use of the powers. Requiring all agencies with access to the new framework to report annually on their use of the powers (and the offences for which use of the powers was required) would provide the public, as well as the associated oversight bodies, transparency about the use of the powers.

31. What, if any, changes are required to the scope, role and powers of the Commonwealth Ombudsman to ensure effective oversight of law enforcement agencies' use of powers in the new framework?

In developing the new framework, previous recommendations of the PJCIS on the MDR Regime should be considered.

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

In developing the new framework, previous recommendations of the PJCIS on the MDR Regime should be considered.

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

In developing the new framework, previous recommendations of the PJCIS on the MDR Regime should be considered.

06 Part 6: Working together: Industry and Government

The existing interception framework has been in place for a long time and is well understood by industry and the agencies. Development of the MDR Regime benefited from close collaboration between government and industry during development and the early stages of implementation particularly with respect to establishing the Regime.

In developing the new framework, there also needs to be close collaboration and consultation with industry and the agencies to minimise the risk of unintended consequence or of imposing unnecessary additional

impact on industry. For example, new or expanded obligations may require further capital investment in systems, or changes to processes that are now familiar and well-tuned within an organisation.

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

We consider the existing interception and MDR framework to be generally workable (noting our comments above about the range of non-enforcement agencies under the TIA Act that have been able to access telecommunications data using other Commonwealth or State legislation). As a service provider, we support a consistent approach across all agencies in accessing telecommunications data.

35. How could the new framework reduce the burden on industry while also ensuring agencies are able to effectively execute warrants to obtain electronic surveillance information?

The new framework could be simplified by removing current ambiguities and ensuring any new obligations are clear and easily understood by all parties. From our perspective, this includes:

- Having the same thresholds for functionally equivalent powers relating to intercepting communications, accessing stored communications, accessing computers, or using surveillance devices to access information.
- Requiring all agencies requesting access to telecommunications data to follow the process set out for enforcement agencies in Division 4 of Chapter 4 of the TIA Act rather than relying on section 280 of the Telecommunications Act.
- Standardising interception and stored communications warrants if the new framework no longer distinguishes between live and stored communications.

We also agree with replacing the current Interception Capability Plan requirements with a standing obligation for carriers and carriage service providers to maintain a plan, updated as required.

The current interception and data retention exemption processes do not provide sufficient certainty for carriers and CSPs. Establishing, maintaining and changing interception and data retention capability requires significant time and resources. The current uncertainty that the CAC could make a decision to refuse an application for an exemption under sections 187K (6) and 192(6) more than 60 days after an application is lodged presents unnecessary commercial risk. This is especially as the service provider might have already acted on the basis the exemption has been granted under section 187K(5) or 192(5). There should be no equivalent to sections 187K(6) or 192(6) in the new framework. 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. Interception and data retention exemptions also tend to be time limited so carriers and CSPs have to re-apply for exemptions at the end of this time period with no certainty they will be granted. Apart from making it difficult to plan, it is almost impossible to retro-fit interception or data retention capability into an established product. Our view is that unless there is a material change in the way a service is provided or used by customers, exemptions should last in perpetuity.

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

We understand that the review in this Discussion Paper does not extend to the Telecommunications Act. However, we believe a holistic approach must be taken for this reform to be truly effective. To ensure clarity and consistency on when and how telecommunications data can be accessed, used and

disclosed, and to remove duplication of agency powers and areas of uncertainty, consideration must be given to Parts 13, 14 and 15 of the Telecommunications Act which cover:

- A general prohibition on the use of telecommunications data with exceptions.
- Obligations for carriers and CSPs to provide assistance to government authorities.
- Agency powers to issue technical assistance requests, technical assistance notices and technical capability notices.

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

We believe the development of the new framework should include formal government responses to all of the PJCIS recommendations on the MDR Regime.

37. Do you have views on how the framework could best implement the recommendations of these reviews? In particular:

a. What data generated by 'Internet of Things' and other devices should or should not be retained by providers?

There are already a vast number of IoT devices deployed and operating and the number of connected 'things' is forecast to exponentially increase over the next few years as new technologies are rolled out. However, there appears to have been little consideration about the costs and benefits of requiring carriers and carriage service providers to store the mandatory telecommunications data for these devices. We believe consideration should be given to providing industry wide exemptions to certain IoT technologies or use-cases. For example, it seems unlikely that the timing and length of data sessions from a smart meter which provides throughput or output measures at regular intervals would provide useful information to the listed law-enforcement agencies. Importantly, if exemptions are identified, they should be applied uniformly across industry, such that any service provider who provides that service is exempt from the Regime.

b. Are there additional records that agencies should be required to keep or matters that agencies should be required to report on in relation to data retention and to warrants obtained in relation to journalists or media organisations? How can any new reporting requirements be balanced against the need to ensure sensitive law enforcement or security investigations and capabilities are not compromised or revealed?

No comment.

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

No comment.

d. What would be the impact on reducing the number of officers who may be designated as 'authorised officers' for the purposes of authorising the disclosure of telecommunications data?

No comment.