Active Cyber Defence Alliance

Active Cyber Defence Alliance (ACDA)- Surveillance Law Reform Response to DoHA Discussion Paper

A document developed by the Active Cyber Defence Alliance (https://acda.group)

Lead author & discussion curator Helaine Leggat.

Contributors: Helaine Leggat, Ben Whitham, Francis Cox, Bruce Gordon, Mitchell Redshaw, Andrew Cox,

Current version release 11 February 2022

Surveillance Law Reform Response /Submssion

Disclaimer

The statements in this document are the opinions of the authors as members of the Active Cyber Defence Alliance and do not necessarily reflect the views of their individual employers.

Who is the Active Cyber Defence Alliance?

The Active Cyber Defence Alliance is special interest group comprised of industry, academic and government stakeholders whose aim is to foster awareness, adoption and capability in active cyber defence practices across Australia with the goal of lifting Australia's cyber resilience.

Active Cyber Defence Alliance - Cyber Strategy Group

Andrew Cox
CEO
Avantgard Pty Ltd

Ben Whitham
CEO
Penten Pty Ltd

Debbie Lutter
CEO
AUSCSEC Pty Ltd

Duncan Unwin
Managing Director
Tobruk Security

Francis Cox
Compliance Consultant

Helaine Leggat
Attorney at Law
ICT Legal Consulting

John Powell
Principal Security Consultant
Telstra Purple

Rob Deakin
Director Cyber Security
ACCC

Phillip Moore
Technical Manager
Avantgard Pty Ltd

What is Active Cyber Defence?

Active cyber defence:

- employs cyber intelligence, deception, active threat hunting and lawful countermeasures to detect and respond to malicious activity (Passive cyber defence relies on conventional cyber security practices such as network hygiene, firewalls, identity and access management, virus filters, good user behaviour etc.)
- leverages the foundation provided by passive cyber defence to provide greater visibility of the contextualised threat landscape
- seeks to grasp the initiative with attendant negotiating power and assurance by leveraging intelligence and indicators of compromise to identify an attack, respond to, or against the capability to give the defender the ability to adapt quickly in a proactive way

excludes offensive cyber actions which are the sole domain of authorised government agencies, although it could include mechanisms to coordinate potential responses by such agencies

Introduction

In making this submission the Active Cyber Defence Alliance (ACDA) seeks to contribute to proposed Surveillance Law Reforms in areas where these affect Australians' ability to defence themselves in the cyber domain.

The legality of active cyber defence hinges upon authorised or unauthorised (i.e. unlawful access) to computers and computer systems. The proposed amendments to Australia's surveillance laws (30 years old) offer an opportunity for us to suggest amendments authorising access to information for purposes of active defence.

We seek the ability to lawfully access information and networks to obtain Cyber Threat Intelligence (CTI) in an appropriate and lawful manner in aid of cyber defence. A more detailed explanation of our objective may be found in our response to Question 3.

Note: Not all questions have been addressed. The enclosed document is a consolidation of input from the named contributors in their private capacity.

Questions

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

No. New definitions of data, data value, intent and derivative use are required.

1a. If so, which aspects are working well?

The awareness of data and its value, plus its vulnerability to theft and misuse has grown markedly. This has set the scene for better controls and better public and organisational acceptance of those controls.

1b. 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 problem of the end value of data not being apparent to the legitimate collector means that intent becomes key. For example, power metre-reading data is legitimate for a power authority to collect for billing purposes and aggregate demand modelling. Further use of that data to detect patterns of people being at home, how many there are, the hours they keep and whether the house is empty to rob, clearly are not.

We acknowledge that the *Privacy Act 1988* does cater for protections with respect to 'secondary purpose' of use and disclosure of Personal information, but it does not go far enough.

Definition of legitimate intent and collection of data for that intent should and can be subject to simple guidelines and controls. Further use of that data, individually and in aggregation must be classed as a completely different scenario with different controls and criteria applied.

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?

No. There will always be legitimate uses for data and the need to use it beyond the initial intent (purpose). This opens the way to disclosure, abuse and loss of control. As a result there is very little data or threat intelligence sharing at present, particularly in the private sector. However, categorisations in the methodology of further use could avoid some of these issues. For example, if under controls, data is further evaluated for security intelligence value, that intelligence could be shared under simpler guidelines than the raw underlying data could. While this might not the be the preference for the intelligence community, it might offer a mediated middle step. If the use of the shared intelligence provided a compelling finding, requests for full data access could then be considered under a controlled process.

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?

Increasingly, all agencies will have need to access information and data to discharge their public and legal duty to the owners of the data, and to meet their obligations under law more broadly.

Rather than that making the problem bigger, layering the levels of sharing may provide a safer and simpler way to facilitate this. Sharing of high-level intelligence data might be fairly ubiquitous. Access to more specific threat data may be the next step with additional visibility and controls. Under some circumstances Least often, access to source data may be justified in some cases with additional scrutiny, disclosure and controls.

This issue applies to the private sector equally. It must be recognised that the government sector cannot win this battle alone and must equip and enable the private sector in parallel under an appropriate regime.

From an ACDA perspective, the question should be reframed as:

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

From an ACDA perspective, the answer is that certain private sector entities, and/or individuals within such entities, should be empowered to access particular information for purposes of intelligence discovery in relation to information and information systems (Cyber Threat Intelligence (CTI). The current exception provided under telecommunications and criminal law for 'network protection duties' is too narrow and not fit for purpose.

Private sector entities, for example Tier 1 financial institutions, should be empowered to lawfully access information and information systems for cyber security intelligence – CTI purposes.

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?

Firstly, intent should be defined. Data to satisfy legitimate intent should be supported (and audited). Any further access or usage of that should not be permitted and active controls applied. If further access were requested, intent should again be defined and managed accordingly.

The epidemic of cyber-crime is forcing us to move from individual defence with delegated powers to specific agencies since it is no longer adequate. As a result, individuals and industries are moving to a Collective defence model and this requires exchanging of information and clarification of the principals under which information can be lawfully obtained and shared.

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

Since it has been shown that any attribute or datum at all becomes usable when aggregated with other data under in the hands of creative, commercially driven, or maliciously driven entities, a much broader definition of data is required.

Anything that a communication 'carries' in any sense is by definition information.

See also our answers below on "content' information and "non-content" information.

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

Some new concepts are needed here. Definitions for: raw data, identified data, meta data, intelligence and threat intelligence all need tightening and clarity as the basis for separate classifications of sensitivity and limitations of access.

The concept of data value goes along with this. There is the primary value of data in line with the intent of collecting it. There are further attributions of value with additional uses of the data including aggregation and intelligence outcomes. It is not sufficient to say to the originator or owner of data – I will reward you for the primary value of your data only. What else I do with it and value I generate is mine alone (basically, the Google model). So long as the emerging technologies base their outcomes on source data, the same rules should apply. The acid test might be:

1. If you did not have original source data, could you have created your product?

2. If source data was taken away now could you maintain the value of your product? If 'no' is the response for either or both of these questions the same rules should apply.

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

By adopting the technology neutral approach propounded in the 1990s in Model Laws and Electronic Communications Convention which involved international co-operation, specifically through the executive arm of government, in this case, including the Department of Foreign Affairs and Trade (DFAT).

Notably, this approach has been too often neglected in Australia and the United States of America with the result that both countries have issue, system and technology-specific legislation, and regulators. In addition to the complexities of federal legislative regimes this approach brings unnecessary confusion and an inability to keep up with (i) changes in technology, and (ii) changes in human behaviour. A technology neutral approach would cater for AI, quantum computing and emerging technologies, including the uses of new technologies into the future.

In this regard, we strongly urge the Department of Home Affairs and DFAT to re-visit the:

1. UNCITRAL Model law on Electronic Commerce adopted in June 1996;
2. UNCITRAL Model Law on Electronic Signatures adopted in July 2001; and
3. Convention on the Use of Electronic Communications adopted in November 2005.

These Model Laws and the Convention were intended to strengthen the harmonisation of the rules regarding electronic commerce and foster uniformity in the national enactment of the Model Laws. The same rationale should apply to surveillance (including Mutual Legal Assistance Treaties, the Clarifying Lawful Overseas Use of Data (CLOUD) Act and Agreement etc.

4. And – the Council of Europe's Convention on Cybercrime (Budapest Convention) adopted in November 2001 - the first international treaty seeking to address internet and computer crime by harmonising national laws, improving investigative techniques, and increasing cooperation among nations.

While we recognise that the 1990s approach has led to a lack of certainly in interpretation and application of the law in some respects, the answer is not in providing system, issue and technology- specific legislation. The answer is in court made law and the judicial process.

We need judges and administrative personnel trained and empowered to apply and interpret existing law to new technologies and use cases. This is not difficult – Australia has seen the interpretation of postal services under sec 51 of the legislative powers of Parliament in the Australian Constitution interpreted to include electronic communications. There are many other examples.

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

In the information age, surveillance involves access to information/data, whether it is static or in transit; whether in electronic form or not. If duly authorised authorities (agencies) have a legal right to access information/data, the distinction between 'content' information and non-content' information is semantic.

The issue in relation to the distinction, however, goes to privacy and human rights etc., (prohibitions against 'Big Brother' surveillance), so it is vital to make the distinction between 'content' information and 'non-content' information for lawful surveillance purposes.

In reference to this question, and the question below, we have examined the *UK Investigatory Powers Act 2016* (IPA), and support the UK definitions for:

> "Content ('content' information), which in relation to a communication and a telecommunications operator, telecommunications service or telecommunication system, as any element of the communication, or any data attached to or logically associated with the communication, which reveals anything of what might reasonably be considered to be the meaning (if any) of the communication, but—
>
> > (a) any meaning arising from the fact of the communication or from any data relating to the transmission of the communication is to be disregarded, and
> >
> > (b) anything which is systems data is not content."
>
> In other words, content concerns 'meaning', and the definition of 'content' in IPA, specifically excludes 'communication-related' information (sometimes referred to as 'meta data' and which is 'non-content' information).

We note further that UK IPA defines "Communications data" to include "entity data" or "events data", providing a clearer definition and a hierarchy with respect to access authorisation. The clarity provided here and the distinction above are useful to address the practicalities of issues such as the retention of records and evidence currently in the TIA.

We think it important to remember that communication happens between (i) machines (as in the client – server model, IoT etc.) as well as between (ii) human beings and machines, and between (iii) human beings and human beings. Consideration should be given to the 'content' information and 'non-content' information in all these 3 scenarios. For example, does it matter what content information is transmitted between machines, when machines have no rights to privacy, and legal relationships are not recognised between machines? What about an extension of rights to the owners and operators of machines – something relevant to IOT, software, firmware etc.

From the perspective ACDA, Cyber Threat Intelligence (CTI), 'content' information and 'non-content' information are both critical to a strong and vigilant cyber defence posture.

We believe it is necessary to make an exemption/exception for access to 'content' information and 'non-content' information for Active Cyber Defence and Cyber Threat Intelligence purposes. This can be achieved by recognising the legitimate purpose for access and by

removing the fault elements from the crimes of unauthorised access, interference etc. in the *Criminal Code Act 1995* to this end. Stipulations can be made regarding secrecy, disclosure etc. Limitations, checks and balances, and provision for proper oversight can be provided.

In addition, consideration might be given to a definition. Maybe: Anything that contains 'atomised' or source data is certainly content. Perhaps the atomised status might be related to the uniqueness of a set of data it is derived from to identify an individual or entity. Information that mixes atomised data with derived data is also content. Only information that contains no data that is traceable back to the lower levels of the source data should be deemed meta data and therefore not content.

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 support the proposition that Australia uses/leverages the UK IPA definition of 'content, and the IPA definition of 'communication' i.e:

> *"Communication", in relation to a telecommunications operator, telecommunications service or telecommunication system, includes—*
>
> *(a) anything comprising speech, music, sounds, visual images or data of any description, and*
>
> *(b) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus.*

We note also that switched circuit telecommunications and broadcasting ((a) and (b) above) are not the be-all and end-all of surveillance. Provision must be made *mutatis mutandis* for Internet Protocol (IP) packet switching – i.e. this is why data surveillance laws also need amended.

In our view, it would be constructive to recognise the convergence of telecommunications and broadcasting technologies in law, and handle broadcasting and telecommunications technologies in the same way with respect to surveillance, privacy etc. In other words, there should no longer be any need for a separate data surveillance statute. Furthermore, there should no longer be separate state and territory data surveillance statutes. Surveillance demands uniform law at the federal level.

We also support co-operation and alignment between the Five-Eye nations, and standardisation that will assist international law enforcement.

Regarding the approach in other jurisdictions, we suggest that it might be useful to examine South African law – the *Regulation of Interception of Communications and Provision of Communication- Related Information Act* (RICA), a law that regulates the interception of communications and associated processes such as applications for and authorisation of interception of communications. There is much to be learned in relation to live and stored communications, operational implementation, oversight and legislative over-reach.

The South African Constitution provides for a right to privacy and the limitation to the right of Privacy. The right to privacy is provided for in the *Protection of Personal Information Act 2013* (POPI). RICA provides for the limitation to the right to privacy through surveillance.

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?

- Are there benefits in distinguishing between different kinds of non-content information?
  - Yes. This provides hierarchies in relation to access and oversight. (This is covered above). It also informs legal record-keeping and evidential retention requirements – currently provided for under the TIA, which need to be provided for in any legislative reform.
- Are there particular kinds of non-content information that are more or less sensitive than others?
  - Yes. For example, geo-location data and tracking data. Information and data, be it 'content' information and 'non-content' information, and it is part of a whole connected global communications eco-system. For example, connected vehicles in the proximity of a hospital tell a story beyond 'non-content' information. There are many other examples; and
  - No. In the final analysis, the aggregation of data means that everything is commixed at its most sensitive classification (APRA's CPG 234 recognises this).

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

Arguably, the internet is fundamentally stateless by design. Live has no meaning. In any case, surveillance is inherently a one-way collection of data. It can be argued that data collected 'live' stops being surveillance once the observer interacts with the surveillance subject and is covered under other communication legislative and regulatory frameworks. So, the distinction between 'live' and 'stored' communications is now much less meaningful as effectively all 'live' electronically communicated data is stored, for varying periods of time, in systems during transit from collection point to observation point. In the face of this fact, any legal or regulatory framework that was dependent on the live / stored distinction could reduce enforceability of that framework. It is not a useful distinction.

The ability to narrowcast data, to effect 'live' electronic surveillance, is now ubiquitous (Periscope, body worn cameras, dash cams) as is the ability to record, replay and re-broadcast 'stored' surveillance recordings as if they were live (Zoom, Teams etc). This argues any live / stored distinction is in reality meaningless. The question could better be addressed around whether the observer of the surveillance would make a different decision based on the live / stored status of the communications. It could be argued that an observer acting on "live" and NOT stored communications puts the observer at risk of repudiation from the subject.

Use Case: Active Cyber Defence

> An individual or a corporate entity using active cyber defence is in effect conducting surveillance on their electronic traffic with the outside world in a similar way to the use of CCTV security cameras for security of their physical property. It can be argued that similar evidentiary quality standards of collection, handling, communication and storage would apply to support action taken on the basis of that surveillance. Frameworks should identify acceptable quality standards / criteria for using that surveillance to protect all parties.

Use Case: Citizen calls to a government call centre.

During a call the audio/video/data streams may be routed through IVR, voice biometrics, call recording ("for training purposes only") and the call centre agent may additionally capture part or all of the information stream. Such call centre systems store – translate / transcribe – backup – create and collect metadata about the call, in real time. This argues that all communications must be considered "Stored" hence the live / stored distinction may no longer be a useful distinction within any regulatory framework.

So what might be more appropriate?

A more valuable distinction may come from the records management discipline – ephemeral or persistent. This distinction may be usefully applied and may generate additional elements of a useful taxonomy for surveillance and other communications.

A deeper enquiry into the matter may expose a key quality of surveillance data (content or metadata) used as part of lawful surveillance for example being the detection of trigger words (bomb), repeating behaviours (location), proximity (met with) and relationship (owns a gun).

What would the distinction ephemeral or persistent achieve?

Data streams identified as ephemeral – whether stored or not – would be inadmissible as a basis for accusation or action providing a measure of comfort to people concerned about "the surveillance society" and creating an environment where ephemeral data could be destroyed without liability. This is reflected in the GDPR principle that people have a right to be "forgotten".

More importantly – an enforceable regulatory framework may be possible if creating persistent surveillance records was only permitted after one of the trigger events authorised in the relevant framework was detected. Data streams or parts of data streams prior to trigger events could be classified / identified as ephemeral.

This also aligns with the practice of the largest information gathering organisations globally as observed by the persistence of data collected by internet search engines, and "algorithms" used by Apple, Google, Social Media platforms and Microsoft etc.

Ephemeral / persistent

The ephemeral / persistent distinction reflects the "purpose of collection" [intent – link to privacy]. It minimises "collateral privacy breach".

Questions for further investigation:

Should citizens be able to nominate data streams as ephemeral or persistent?

In effect there are already multiple partial implementations of this with "private browsing" and commercial VPNs that obscure source IPs. Any framework that did not clarify the status of this clandestine capability will be at best mis-understood and at worst defeat lawful surveillance as shown by organised criminal operator's use of AN0M.

Should agencies be able to nominate data they collect as ephemeral or persistent?

This may better support current legislative record retention disciplines and transitional legislative arrangements.

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

Lawful surveillance:

Lawful surveillance by its very definition represents an intrusion into the privacy at least of the individual or situation for that lawful purpose. It seems difficult to find a convincing rationale to treat the privacy intrusion from live or stored surveillance communications differently.

This excludes action taken as a result of the surveillance. For example identifying the current location of the person to effect an arrest may use live surveillance feeds. It can be argued that once a decision is made to act, the information gathered, while it may have come from surveillance system is no longer surveillance but lawful gathering of intelligence.

Intrusion:

There are many common / commercial intrusions into privacy.

One is evidenced on Facebook and similar platforms where a group picture allows every individual to be tagged creating in effect a “collateral privacy breach” as the tagged subject has no control over the identification (correct or incorrect) and distribution of this evidence of their private behaviours.

Banks and credit platforms effectively conduct surveillance – intruding on their customer’s privacy using transaction data to detect potential fraud, they might argue to benefit their customer. A useful framework would clarify the conditions and limitations under which this data is used and shared.

Use Case: Active Cyber Defence

In using Active Cyber Defence, an entity identifies a cyber-attack, collects data about the Cyber Threat Intelligence tactics, techniques and procedures (TTPs). A useful framework will identify the conditions under which TTPs and their supporting evidence can be shared – and how Personally identifiable information (PII) captured with such evidence is limited, desensitised, obfuscated or removed.

A clearer definition of intrusion may also be warranted. Perhaps, the now accepted definition of “repeated” is useful. Bullying, abuse and other behaviours that our society finds unacceptable are now in place across enterprises (policy) as well as in law. In each case, the distinction involves repetition of the intrusive behaviour.

Questions for further investigation:

Authorities in Chinese Cities are proud of recognising and tracking all citizens in public and government spaces. Their espoused approach uses the synopticon principle to frame this intrusion as for the public good. We also see the synopticon principle adopted by “digital natives” in mainly younger generations in Australia. Citizens expect to be provided with data relevant to their private preferences, activities and behaviours. What part of the framework will reflect this principle and how does this balance or support the “panopticon” principle that surveillance changes behaviours towards increased [civic] compliance.

In any discussion of privacy, one question that can provide clarity is "Who owns the surveillance or communications material?" Establishing principles of data ownership (accountability) and data custodianship (responsibility) be identified. Legal and regulatory controls would apply to the data custodian as far as handling the surveillance and communications material, access management etc.

As mentioned in Q's 1-6 it is possible to build a sensitivity model to some extent. Another dimension to the definition is the breadth of the data set that an individual datum is held in. The wider the data, the more impossible it is to de-identify the data and preserve privacy, as more unique data characteristics will appear with each addition datum.

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?

Not answered

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?

Not answered

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?

Not answered

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?

Not answered

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?

Not answered

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

Not answered

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

Thresholds need to be defined based on current working definitions in more mature societies and cultures with feedback loops so they remain current and are not invalidated by societal adoption of new technologies.

Appropriate thresholds can positively impact our society.

Use Case: GDP impact of digital identity:

> Estonia has implemented digital identity as a result of "losing" the first cyber war. After 10 years they measured a 2% benefit to GDP. [Quote from Estonia's former CIO to Vic Government in 2017]

Use Case: Active Cyber Defence (ACD)

> Using ACD gives an entity the capability to detect – both by design and inadvertently. Thresholds must not invalidate inadvertent collection as this risks invalidating the significant benefit to the entity and society as a whole of early and accurate detection of cyber attacks.

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

Not answered

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

Not answered

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

Not answered

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

Not answered

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

Not answered

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

Not answered

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

Not answered

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

Not answered

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

Not answered

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

Not answered

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

Not answered

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?

Not answered

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

Not answered

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

Not answered

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

Not answered

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?

Not answered

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

Not answered

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?

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?

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

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?

End of Document