18 February, 2022

Electronic Surveillance Reform Branch
Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

By email lodgement: Submissions and discussion papers (homeaffairs.gov.au)

To whom it may concern:

Subject: IoTAA submission to Reform of Australia's electronic surveillance framework discussion paper

IoT Alliance Australia (IoTAA), https://iot.org.au/ welcomes this opportunity to address issues raised in the Reform of Australia's electronic surveillance framework discussion paper.

IoTAA is the peak Australian IoT industry body, with over 500 participating organisations and 1000 individual participants. We grow the Australian IoT eco-system, help build capability and good practice, advocate for policies that help accelerate adoption and "IoT for good" that is safe and secure IoT deployment and uses of Internet of Things (IoT) devices and services in Australia. Our mission is to accelerate the adoption of IoT to improve competitive advantage of Australia and benefit Australian society.

We consent to publication of this submission.

The IoT industry is in the early stages of its growth and development in Australia. Accordingly, regulatory compliance can be a barrier to the establishment, operation and growth of IoT services. With this issue in mind, the IoTAA notes that the existing electronics surveillance framework can be viewed as comprising:

(a) standing powers which may be applied by law enforcement or national security when required; and
(b) operating conditions imposed as a cost of doing business for particular types of service.

Examples of existing standing powers include:

- The various warrants in Part 2 of the *Surveillance Devices Act 2004* (**SDA**) including surveillance device warrants, retrieval warrants, computer access warrants, data disruption warrants, and network activity warrants.
- The broad set of powers in part seven of the SDA to compel an individual with knowledge of a computer system to assist law enforcement to obtain access.
- The very broad power to issue technical assistance requests, technical access notices and technical capability notices under part 15 of the Telecommunications Act 1997 (**Telco Act**).

- The ability for a magistrate to issue an account takeover warrant under Part IAAC of the *Crimes Act 1914*.
- The wide range of powers granted to ASIO in the *Australian Security Intelligence Organisation Act 1979*.

Examples of operating conditions include:

- The conditional obligation not to intercept messages expressed in section 7 of the Telecommunications (Interception and Access) Act 1979 (**TIAA**).
- The conditional duty not to discloser or use any "information or document" associated with a communication or communication service, expressed in section 276 of the Telco Act.
- The obligation to maintain an interception capability in s189 of the TIAA and the Interception Capability Plan Determination 2018 (No.1) made under that Act.
- The mandatory data retention obligation in s187AA of the TIAA.
- The broad obligation to assist in 313 (3) of the Telco Act.
- The national security obligations in 313 (1A), (2A) and associated provision of the Telco Act.

The IoTAA acknowledges the important role that law enforcement and national security agencies play in protecting safety and security of all Australians. The IoTAA supports the consolidation and refinement of the powers agencies use to obtain the information they need subject to proper judicial supervision, oversight and public reporting.

However, the IoTAA notes that regulatory obligations listed above apply generally to carriers and carriage service providers no matter what the service they provide, or its potential relevance to law enforcement or nation security. This issue was considered in part by the PJCIS in its Review of the Mandatory Data Retention Regime (2020) and it recommended that **IoT services be excluded from mandatory data retention obligations** (see paragraph 5.28)

The IoTAA supports the existing operating conditions to the extent that network operators are required to ensure the security of information in transit but, otherwise, would like to see the review produce a regulatory framework that imposes ongoing regulatory obligations only for organisations likely to have information relevant to law enforcement or national security purposes and where the imposition is absolutely necessary. To this end, we consider **IoT should by default be excluded from obligations in relation to lawful surveillance**, with existing standing powers used on an as-needs basis to effect lawful surveillance as and when required.

Although most IoT services use a component of public telecommunications facilities (potentially carried over a carrier or carriage service provider) only a small proportion carry messages between individuals and/or other data that could be relevant to an offence or to national security matters. It should also be noted that many IoT services are delivered to only one customer and, therefore, operate outside the telecommunications regulatory regime. For example, a power supply company might engage an IoT service provider to support the control and management of gas and or electricity using dedicated IoT infrastructure. Such an implementation does not involve the supply of carriage services to the public (there being no third party) and, therefore, is not subject to network security or data protection obligations under the Telco Act.

Accordingly, we ask that the review to limit expansion only to the extent necessary to make information available in a serious case that involves a third party member of the public.

We consider there to be no need to extend standing powers to cover IoT devices and systems as the standing powers are already adequate as is, and that by default, data from IoT devices should be excluded.

The new framework should remove the obligation on IoT providers to undertake mandatory data retention and/or to maintain an interception capability unless subject to a specific needs-based request.

Where compliance with standing powers is considered an adequate substitute for ongoing regulatory obligations, the mechanism in section 314 of the Telco Act for compensation on the basis of cost but not profit should be maintained.

Finally, we consider that the prohibitions and offences against the unlawful surveillance of an individual or individuals through the collection, processing and/or analysing of IoT information could be strengthened to deter data processors and controllers from unlawful surveillance, and that action to strengthen the prohibitions and offences should be done in conjunction with the review of the Privacy Act.

We thank you for the opportunity to make this submission.

We are available to discuss our comments and to provide any clarifications that you may require.

Yours Sincerely,

Frank Zeichner

CEO, IoT Alliance Australia

www.iot.org.au

Level 6, 91 York Street

Sydney 2000

+61 408 233 762

IoT Alliance Australia

Attachment C: List of questions

Part 1: Who can access information under the new framework?

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

IoTAA strongly supports the current process for consultative review of Australia's electronic surveillance framework which requires a substantial overhaul in the light the exponential rise in methods and types of data being collected, including through IoT, which may be used to identify persons and their behaviours.

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?**

We consider there is scope to strengthen the prohibitions and offences against the unlawful surveillance of an individual or individuals through the collection, processing and/or analysis of IoT data.

Australia's present electronic surveillance framework focuses on the telecommunications carriers and carriage service providers as the entities responsible for gaining access via interception requirements and other mechanisms. In this regard, there are considerable obligations.

With the advent and rapid growth in data collection and use, including through IoT, access to this data is possible for a wide array of entities in an IoT ecosystem including data collectors, data hosting providers, distributers, processors, and ultimately the data user/s. Hence, the challenge of prohibiting unlawful surveillance has become considerably more complex. In addition, the ability to combine disparate data sets through big data and Artificial Intelligence (AI) along with technology such as facial recognition, movement detection, traffic measurements, etc, makes the challenge of preventing unlawful surveillance more difficult. As a consequence, it is increasingly complex to prohibit actors in the ecosystem from curating and analysing data sets to deduce information about individuals.

In this regard, broader matters need to be considered such as behaviour and controls on data collectors/providers/processors to prevent unlawful surveillance and to protect consumer's privacy. This is already under consideration with the Privacy Act Reform, and we consider the prohibitions and offences against unlawful surveillance need to be strengthened. We also ask that any changes introduced to strengthen the prohibitions and offences are aligned with changes arising from the review of the Privacy Act.

The IoTAA has produced an IoT reference architecture that assists in identifying the relationships between providers, technologies, data etc in a 10-layer model. This model will be helpful to the Department of Home Affairs in understanding where various actors may be able to access content and/or user data, which in turn will help identify classes of entities where prohibitions may need to be introduced or strengthened to better prohibit unlawful access to content. The framework is available at https://www.iot.org.au/wp/wp-content/uploads/2016/12/IoT-Reference-Framework-v1.0.pdf

Data and metadata can be collected and used at up to 10 layers (and possibly more sublayers) in complex IoT systems, such as those used for surveillance. Each layer may also

have (or should have) security mechanisms, access controls and may not be directly to layers below or above.

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

No comment.

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

No comment

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?

No comment

Part 2: What information can be accessed?

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

The attempt to redefine the definition of "communications" in terms of data capture seems inherently flawed from an architectural point of view, see our answer to question 1(b). Communication is predominantly a layer 2/3/4 capability within the IoTAA reference architecture framework. Data and metadata at other layers, especially related to actual end users and providers, data content etc are not normally categorised as "communication". We caution against redefining terms that have international meaning. Moreover, bending definitions of "communication" will have wider implications for non-carrier, local network, private and other communications networks should be deeply considered.

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

IoT is often a one-to-many relationship. Many IoT enabled services are deployed in environments where there is no direct relationship between a person active in that environment and the provider of the service. For example, a home IoT device may be installed and used in a domestic environment where the person that installs the device, enables the IoT service and/or sees reports is not a person whose activities are monitored or reported upon. For example, an internet connected kitchen appliance (fridge, toaster, kettle) being used indicates someone is in the house, but not whom.

An IoT device such as a smart water-meter or electricity meter may be installed in a rental property, or a shared household, or outside a property to enable observation of activity within a property. A person may suffer a harm through excessive and unreasonable surveillance, or as a result of a device actuating an outcome that is adverse to a person. We

consider the one-to-many nature of IoT devices (one device, many possible users) should be considered in the framework.

Identification through merging of data sets. Any data stream in itself may not be sufficient to personally identify a person, but may in combination with other data sets reveal such information.

We support amendments to the framework to the extent that those amendments are necessary and proportionate to address lawful surveillance requirements. Any amendments must ensure data collection does not cause harm to other individuals that may arise in circumstances where personal information is not being used: that is, where the relevant data being collected, used or shared is not personally identifying information about or in relation to individuals.

We also support targeted and proportionate changes to the electronic surveillance framework that have the effect of improving accountability of regulated entities and providing regulatory incentives for exercise of responsibility and restraint of regulated entities.

Given the wide scope of the current national security definition and the intrusive nature of the powers (and attendant penalties for non-compliance), we recommend Government adopts a narrower 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.

The definition of communication needs to be made more specific to purpose, the distinction between metadata and content [if that is to be maintained] needs to be more properly considered and expressed. The proposed new definition of communications service provider needs to be very carefully considered so that it is clear whether private networks supporting private businesses which only use third-party Infrastructure are covered and if so how are the rules apply or not to third-party infrastructure providers necessary for such systems and the communication systems themselves.

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

The framework will need to take into account the merging of data sets from disparate sources, via disparate entities, some of which have the capability to merge and apply AI or machine learning to identify individuals and other sensitive information. In this context, the framework will need to accommodate understanding and visibility of data processing and aggregation points as places of vulnerability and clearly articulate when the application of advanced data processing techniques is unlawful.

8. What kinds of information should be defined as 'content' information? What kinds of information should be defined as 'non-content' information? Is there a quantity at which non-content information becomes content information and what kinds of information would this apply to?

From a communications layer perspective, any data, whether content or metadata, above layer 4, could be considered "content".

However, the distinction between content and non-content is highly contextual, in the abstract. For example, an internet connected kettle may have data about what

temperature the water was boiled to (content of the communication), but the information of when, how many times the kettle was boiled (metadata) can provide valuable information about house occupation. From this example, it can be seen that metadata (i.e., information about how many times and at what time a communication is made) can be either non-content or content depending on context. It is worth noting that the communications in this example are machine-to-machine, not a communication from a person to another person.

To make this question more meaningful, it will be necessary to better define contexts for data collection.

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

No comment

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

We consider there are likely to be benefits arising from classifying some form(s) of non-content information as more sensitive than other form(s) of non-content information. However, this is not as simple as just defining some types of non-content information as sensitive. Sensitivity will depend on context, use case and use. For example, as noted in our answer to Question 8, non-content information about the use of a home appliance (kettle, fridge, car, etc) can be used for ascertaining when a periodic should be scheduled, or for surveillance of an individual (to the extent it's clear *which* individual is using the appliance). As such, sensitivity depends on who is using the information, and the context in which they're using the information.

Sensitivity can also depend on contextual factors such as critical infrastructure or national security.

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

The concepts 'live' (meaning 'in real time') and 'stored' are important concepts to include in the framework to ensure agencies, service providers and the community clearly understand how, where and when the interception of a communication is prohibited (and hence, unlawful) without appropriate authorisation. However, in terms of the treatment of the two types of communication, we see no need to distinguish between the concepts. By default, interception of, or access to either type of communication should be prohibited (deemed unlawful), and regarding IoT information specifically, we consider it should be exempted from obligations placed on carriers and carriage service providers.

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

As noted in our answer to Question 11, we consider the terms 'live' and 'stored' need to be retained to agencies, service providers and the community clearly understand how, where

and when the interception of a communication is prohibited. However, we consider the treatment of each of the types of communication should be identical, and this is at least in part due to the fact that surveillance of either type of communication would likely have the same 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?

To protect and retain meaningful sensitive information, consideration needs to be given to the type(s) of information agencies are lacking from the current framework and to identify where they would most usefully obtain it from and how this would be best facilitated. This may require access to data providers/processors and aggregators – rather than or in addition to communications providers.

Note, data centre operators, aggregators and data providers may also not have access to content, but will to different sets of meta-data which may or may not be useful – depending on context, use case etc.

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?

The internet of things opens up a cornucopia of additional devices beyond "Surveillance devices" which could be used to provide data that personally identifies people. Data from such devices such as movement detectors merged with other data sets could well (and indeed are) able to track and monitor individuals.

An approach that also looks at data sets that have a high personal identification factor (PIF) should be considered in the approach. https://www.csiro.au/en/news/news-releases/2021/new-data-privacy-tool-ensures-anonymous-covid-19-data-remains-secure-and-private

Part 3: How can information be accessed?

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?

No comment

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?

No comment

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 support amendments to the framework to the extent that those amendments are necessary and proportionate to address lawful surveillance requirements. Any amendments must ensure data collection does not cause harm to other individuals that may arise in circumstances where personal information is not being used: that is, where the relevant data being collected, used or shared is not personally identifying information about or in relation to individuals.

We also support targeted and proportionate changes to the electronic surveillance framework that have the effect of improving accountability of regulated entities and providing regulatory incentives for exercise of responsibility and restraint of regulated entities.

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

In the event that other entities have additional obligations placed on them, consultation and consideration of capacity to implement, cost recovery, and timeframes will need to be undertaken.

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

The Privacy Act (under reform review) and other legislative tools address privacy implications into person's location and movements. It is imperative that the surveillance framework aligns and accommodates these.

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)?

Where objects are IoT devices, where required for serious security matters, they would better be focussed on those that have a high personal identification factor (see answer to question 14) such as facial recognition devices.

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

No comment.

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

No comment

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 developments to the extent that those developments are necessary and proportionate to address surveillance and other harms to individuals that may arise in circumstances where personal information is not being used: that is, where the relevant data being collected, used or shared is not personally identifying information about or in relation to individuals.

We also support targeted and proportionate changes that have the effect of improving accountability of regulated entities and agencies and providing regulatory incentives for exercise of responsibility and restraint of regulated entities.

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

Information obtained by lawful order for law-enforcement purposes should be used only for the purpose which is obtained. There should be clear penalties associated with obtaining information for a purpose other than a stated purpose, for using or communicating the obtained information where not necessary to the enforcement of a relevant law. Supervisory agencies should be required to audit and verify the integrity of evidence gathering activities in compliance with the proposed framework.

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

Please see our answer to Question 25.

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

The case for emergency powers which circumvent standard procedures is not well made. Circumstances and the need should be clearly articulated.

Part 5: Safeguards and oversight

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

The new framework ought to consider the oversight framework proposed by the INSLM.

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

The safeguards should prohibit the use of surveillance and information gathering powers for the purpose of obtaining legally privileged information.

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?

Please see our answer to question 28.

The oversight framework should ensure greater transparency and simpler to understand process for to members of the public and industry. A relevant supervisory agency should be set up to be independent, properly funded and operating under a minister or department separate from the relevant regulated law-enforcement or national security agency.

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?

No comment

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

No comment

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

No comment

Part 6: Working together: Industry and Government

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

The burden of complying with lawful requests to intercept / access information can fall disproportionally against smaller IoT operators who are less likely to have the staff and other resources to introduce mechanisms to capture content for law enforcement agencies.

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?

Where the scope of industry is extended beyond those currently required, an education, awareness transition period may be necessary, and consideration given to funding to support material additional costs, additional staff and tools to be able to respond.

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

By ensuring clear guidelines and time for industry consultation on material changes to the framework. This is particularly important for obligations that are extended beyond carriers and carrier service providers.

Part 7: Interaction with existing and recent legislation and reviews

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

Internet of Things devices and especially their derived data sets that may personally identify individuals extend well beyond traditional "surveillance devices". Those with potentially greater interest would be those associated with higher personal identification factors (PIF).

This question needs a greater focus on the circumstances/use cases and proportionate needs of this broader range of devices (and data sets) before a meaningful list can be identified. Why? Because, in theory nearly all data sets have some value of PIF and could conceivably be valuable in identifying individuals – retention of these is a practical impossibility.

Moreover, the retention of many of these data sets are likely to only be practicably possible by non-carriers/carrier service providers – that is data providers/processors etc.

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

We would expect this to generate positive results for industry in engaging with agencies, provided the authorised officers are appropriately senior, trained and operate within a culture of compliance subject to independent oversight.