BCA

Business Council of Australia

Reform of Australia's electronic surveillance framework

Discussion paper

February 2022

Contents

1. About this submission 2

2. Key recommendations 2

3. Key points 2

 3.1 Proportionality 3

 3.2 Keeping pace with technological change 3

 3.3 Clarifying which agencies can access information 3

 3.4 Types of data and privacy implications 3

1. About this submission

This is the Business Council's submission in response to the Discussion Paper on the Australia's electronic surveillance framework. Our submission does not respond to every question raised in the Discussion Paper.

The Business Council represents businesses across a range of sectors, including manufacturing, infrastructure, information technology, mining, retail, financial services and banking, energy, professional services, transport, and telecommunications.

2. Key recommendations

The Business Council recommends:

1. Any new electronic surveillance framework be proportional, with close consideration of the regulatory costs that will be borne by industry and privacy implications for Australians in any revised framework
2. Avoiding the introduction of conditions on individual businesses, and instead focus on industry wide requirements.
3. Any new legislative framework should include consistent, clear, and principles-based criteria for what information gathering techniques are within scope, to manage the emergence of new technologies.
4. Developing a single, definitive list of entities that can access data under any new framework, and considering the benefits of prescribing this within primary legislation
5. Avoiding requiring businesses to build entirely new systems to store surveillance data without appropriate support and consideration of the privacy outcomes.

3. Key points

The Government is seeking views on wholesale reforms of the legislative framework governing electronic surveillance in Australia. This will involve repealing a number of acts (including the *Telecommunications (Interception and Access) Act 1979* (TIA Act), the *Surveillance Devices Act* 2004 (SD Act), and parts of the *Australian Security Intelligence Organisation Act 1979*. The intention is to replace the current laws with a single, streamlined and technology-neutral Act. We support reform of the various acts to simplify and modernise the legislative framework.

These reforms follow the findings of the Comprehensive Review of the Legal Framework of the National Intelligence Community, undertaken by Dennis Richardson AC. The review noted the TIA Act rested 'on outdated technological assumptions, and has become complex to the point of being opaque … the process of reforming the TIA Act presents a unique opportunity to also introduce consistent controls'. Development of the new framework must occur in close consultation with industry to minimise the risk of unintended consequences and to ensure the new framework does not pose any unnecessary additional burden on industry.

This submission does not address every section of the discussion paper, and instead focuses on several sections which have a substantial effect on Australian businesses. The fact that there are currently 35 different warrants and authorisations that agencies may use to undertake a range of surveillance activities does not make sense, particularly in light of the differing thresholds and requirements that each must meet. This is a chance to modernise what has become an outdated set of laws to ensure Australia is appropriately able to meet new challenges while protecting Australian citizens and businesses from unnecessary intrusions into their private communications.

3.1 Proportionality

We support reforms to the Act that ensure an appropriate balance between law enforcement and intelligence agencies and the legitimate interests of businesses and citizens. As a guiding principle, any reform efforts should be open, inclusive, and transparent. This should also be reflected in any final framework, along with ensuring it remains proportional to the challenges being addressed. A proportional framework will ensure that protections against unjustified intrusions into privacy continue to meet Australians' expectations.

It will also ensure businesses are not burdened with requirements that might prove anti-competitive or impose onerous and unnecessarily costly requirements. Requirements targeted at specific entities will create unnecessary market distortions, as individual businesses must meet costs their competitors do not.

We recommend the government carefully consider the financial costs that will be borne by industry and privacy implications for Australians in any revised framework. We do not support introducing requirements that only individual businesses will have to meet, or involving arbitrarily targeting a single company or small group of companies.

3.2 Keeping pace with technological change

The findings of the Comprehensive Review highlight that the existing framework has not kept pace with new and emerging technologies. We support reforms that will deliver a technologically neutral framework. However, this should be done in a way that can not only oversee new forms of surveillance as technology evolves, but also appropriately prevent 'scope creep'.

The Discussion Paper asks how the framework can best account for new technologies, explicitly identifying artificial intelligence and quantum computing. To account for new technologies and ensure a framework is truly technologically neutral, any new framework should have consistent, clear, and principles-based criteria for what information gathering techniques are within scope.

3.3 Clarifying which agencies can access information

As has been noted in previous consultations on Australia's data retention laws, the number and range of bodies requesting information under existing laws has grown substantially.

We support arguments made by others that the number and type of bodies should be clearly defined. There are substantial privacy implications from allowing many government organisations to request information under existing laws, given these allow for intrusion on the privacy of individual Australians.

Beyond the privacy implications, we also wish to highlight that these also come with a substantial regulatory cost to business. Allowing a broad swathe of organisations to request surveillance information is not an effective use of the limited resources available to businesses to respond. It draws effort away from issues of national significance.

We recommend government develop a single, definitive list of entities that can access data under any new framework. It would be appropriate to give due consideration to previous recommendations made by bodies such as the Law Council for this to be prescribed within primary legislation. This will ensure that – while it can be updated – it is only done so after due consideration.

3.4 Types of data and privacy implications

The Discussion Paper raises questions that effectively go to the use and definition of communications, data, and metadata. It also contemplates whether there are differing levels of sensitivity associated with each of these.

We recommend the government carefully consider the wider privacy and regulatory costs associated within a revised framework. It would not be appropriate to create a regime that sees businesses required to make

substantial new investments (unless government is willing to provide financial support) or over-collect information about their users to satisfy potential new warrants.

As noted above, we support modernisation of the legislative framework governing electronic surveillance. As part of this, we look forward to government considering any proposed new requirements to a thorough cost-benefit analysis. It will be critical that there is close consideration of whether the costs (both financial and otherwise) of creating these new requirements would be outweighed by the actual benefits, and whether it represents the least-cost means of achieving government's goals.

For example, any new regimes should avoid creating unnecessary costs for businesses, who may have to build new systems and data storage capabilities. Businesses will have to make substantial investments if they are required to store information such as a person's browsing history. If government considers the costs worthwhile, it should appropriately support businesses to establish these new systems, as was done for the data retention regime.

It should also avoid having the net effect of eroding the privacy of all Australians, regardless of whether they are of legitimate interest to law enforcement or intelligence agencies (as businesses would need to collect more information about all their users to be able to satisfy potential warrants). This would particularly run counter to the argument underpinning the ongoing review of the Privacy Act: that there is a concern about the amount of data being collected and held by businesses.

We also recommend government give due consideration to the sensitivity of all types of data. It would not be appropriate, for example, to suggest that there are lower consequences or privacy implications for 'metadata', any data that is 'at rest' (i.e. not actively being communicated), or other technical data. This would mean, for example, ensuring that metadata should not be made available to agencies on the basis of written notice only.

The ongoing review of the Privacy Act is contemplating whether these types of information (such as technical information) deserve additional protections, or potentially to be treated equally to personal information. We do not agree with some of the suggestions that have been made as part of the review of the Privacy Act on this topic (given the disproportionate regulatory costs their inclusion as 'personal information' would create). However, the concerns that have been raised through the review of the Privacy Act highlights that these types of information are considered to have substantial privacy value by and are deserving of appropriate consideration.

BUSINESS COUNCIL OF AUSTRALIA

42/120 Collins Street Melbourne 3000 T 03 8664 2664 F 03 8664 2666 www.bca.com.au

© Copyright February 2022 Business Council of Australia ABN 75 008 483 216

All rights reserved. No part of this publication may be reproduced or used in any way without acknowledgement to the Business Council of Australia.

The Business Council of Australia has taken reasonable care in publishing the information contained in this publication but does not guarantee that the information is complete, accurate or current. In particular, the BCA is not responsible for the accuracy of information that has been provided by other parties. The information in this publication is not intended to be used as the basis for making any investment decision and must not be relied upon as investment advice. To the maximum extent permitted by law, the BCA disclaims all liability (including liability in negligence) to any person arising out of use or reliance on the information contained in this publication including for loss or damage which you or anyone else might suffer as a result of that use or reliance.