Electronic Surveillance Reform Branch

Department of Home Affairs

PO Box 25

BELCONNEN ACT 2616

electronicsurveillancereforms@homeaffairs.gov.au

Dear Electronic Surveillance Reforms Branch,

Reform of Australia's electronic surveillance framework – Synergy response to Discussion Paper

Thank you for the opportunity to provide feedback on the 'Reform of Australia's electronic surveillance framework discussion paper' (Discussion Paper).

Our response to seven of the eight parts is attached below. We have chosen not to respond to the 37 questions individually, instead we have grouped our responses to related questions within each part.

We note that our feedback will be used to inform the drafting of the proposed electronic surveillance legislation and welcome the opportunity to discuss our submission now and during future consultations.

Synergy Law is a Synergy Group legal offering, specialising in Government law and legal advisory services. Synergy Law also looks to opportunities Government can 'lean into' future legal issues such as cyber security, infrastructure security, emerging energy resources, climate law, ICT and technology, data sharing and information law, to support Government operations becoming 'future ready.'

Thank you for considering our submission. We look forward to hearing from you.

Regards,

Melanie Hutchinson,
SPECIAL COUNSEL, SYNERGY GROUP AUSTRALIA

mhutchinson@synergygroup.net.au
[redacted]

Bobbi Campbell,
PARTNER, SYNERGY GROUP AUSTRALIA

bcampbell@synergygroup.net.au
[redacted]

Australia's electronic surveillance framework reforms

Response to the Department of Home Affairs Reform of Australia's electronic surveillance framework Discussion Paper

Introduction and general remarks

Technology, in particular the internet and digital modes of communication, knits together the very fabric of our lives, our lifestyles, how we work and do business. It is fair to say that for the foreseeable future, we will continue to embrace the lifestyle and cultural conveniences that have developed with the evolution of these modern technologies. Digital modes of communication afforded by an array of smart devices have indelibly become part of our everyday existence. Indeed, the rapid evolution of technology and uptake within society has outpaced the existing legislative framework by a significant margin.

Against this backdrop, we note the growing realisation of Government that retrofitting law to suit culture is no longer a sustainable solution. It is therefore timely and appropriate for the Government to pursue action to replace the existing patchwork of laws with a unified, technology-neutral, legislative framework, as announced by the Department of Home Affairs in the discussion paper titled 'Reform of Australia's electronic surveillance framework', published on 6 December 2021 (the Discussion Paper).

We note that this is the most significant reform to Australia's national security laws in more than four decades, the discussion paper follows a review of the legal framework of the National Intelligence Community, undertaken by Dennis Richardson AC (the Richardson Review), which found that the existing electronic surveillance legislative framework is no longer fit for purpose.

Consequently, the Richardson Review recommended the repeal of the *Telecommunications (Interception and Access) Act 1979*, *Surveillance Devices Act 2004,* and parts of the *Australian Security Intelligence Organisation Act 1979* and replace them with a single, consolidated, technology-neutral, Act (see recommendation 75). These findings are not unexpected when considering the point in time when the original legislation was first conceived. Specifically, that it was designed around Government ownership of telecommunications networks and was designed to protect the privacy of fixed line phone calls and telegrams. Circuit-switched carrier networks were typical, and Voice over Internet Protocol (VOIP) and Over-the-Top (OTT) message applications, including social media, were not yet sprouting in our consciousness.

Interestingly, the Discussion Paper identifies that the new laws could apply to a much broader range of information beyond that which falls within the current scope of the *Telecommunications (Interception and Access) Act 1979*. This could result in OTT and Unified Communications providers being subject to similar requirements for interception and data retention as traditional carriers. Further, the Discussion Paper suggests that the new laws could apply to a much broader range of information beyond the conventional "communications" that fall within the current scope of the *Telecommunications (Interception and Access) Act 1979*. For example, cloud-hosted data including electronic documents stored using Google Drive or Dropbox, data generated by IoT devices like smart vehicles or home appliances, draft or unsent emails and instant messages and information from the use of non-messaging smart phone applications.

Another significant issue to highlight is that the Discussion Paper considers extending additional surveillance powers to agencies including the Australian Transaction Reports and Analysis Centre, the Australian Taxation Office, Australian Border Force and Australian Criminal Intelligence Commission and State and territory corrective service agencies if their respective governments request it. This is an interesting consideration, noting all the changes to these Agencies that would be needed, including charter, people, technology, security, safeguards, assurance and oversight to allow for this. There is nothing in place to capture and control who/where/when/why Electronic Surveillance is being carried out. The working relationship between ASIO and AFP is decades in the making, even so, discussion on creating such a capability is ongoing. How does the Government propose to achieve and operationalise the proposed extension of additional surveillance powers to these Agencies? The devil will be in the drafting, and it remains to be seen just how far these powers will extend and which agencies will be permitted to wield them.

Consideration should also be given to the proliferation of encrypted apps such as Signal, Telegram among others (not to mention blockchain and related technology) that are designed to be difficult (if not impossible) to access, resulting in communications on these platforms by default requiring more intrusive means to intercept. These apps are commonly used as collective social concern increases with respect to how personal data is accessed and used by government, big tech, social media and e-commerce platforms. An ever-increasing percentage of the population are concerned about protecting their data and identities and accordingly are turning to encrypted apps for their communications. In other words, it must not be assumed that use of encrypted apps is limited only to bad actors.

Further, potential threats to national security are often transnational with affiliate groups communicating on encrypted apps across multiple jurisdictions. This creates cross-border complexities with respect to sovereignty and when and under what circumstances searches under warrant can take place, if at all.

It is essential that an appropriate balance is struck between technological advancement, use of these technologies and robust and effective law enforcement to avoid unintended consequences. There is a direct corollary between enhanced state surveillance and democratic and social cost. It is all too easy for civil liberties to be eroded in the name of national security, leading to loss of social cohesion and trust in Government. Therefore, it is extremely important that these reforms are considered in conjunction with a robust federal human rights framework. These reforms present an opportunity to get the balance right.

Synergy Law welcomes the proposed reform of Australia's electronic surveillance framework, and the opportunity to provide a submission in response to the Discussion Paper. We note however that the detail will be in the drafting, and accordingly, welcome the opportunity to make future submissions as the reform process progresses.

Response to questions

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

The reforms outlined in the Discussion Paper offer a unique opportunity to reposition Australia's surveillance legal framework, with human rights at the centre. Such an approach is consistent with the fundamental, guiding principle that the national security framework exists to protect freedoms for all Australians. It has been decades since the current provisions were first enacted and there is substantial merit to claims that existing prohibitions and offences against unlawful access to information and data no longer protect privacy as robustly today as these laws might have done

when first established. The reforms process proposed in the Discussion Paper represent a timely opportunity for the Government to review the existing powers, prohibitions and offences against unlawful access to information and data, to ensure that they are relevant, proportionate, necessary, and subject to appropriate governance and oversight. In particular it is an excellent opportunity to examine whether these provisions are consistent with the rationale supporting their introduction and if not, to take appropriate measures.

The Discussion Paper asserts the Government will work closely with State and Territories to 'ensure the new framework is harmonised with state and territory legislation to provide appropriate protections against observing activities, listening to conversations and tracking a person's movements through unauthorised use of surveillance devices.' (p15). However, the Discussion Paper doesn't provide any details concerning how this harmonisation of laws will be achieved. We also question what harmonisation means in this context. For example, does it mean establishing a Commonwealth system to replace the disparate state framework, or additional reforms to the state and territory laws to align them with the proposed federal reforms, or a system where some powers are state based, and others federally based?

The covid pandemic has highlighted the disparate boundaries of power between the states and territories and the federal government, at times resulting in a tennis match of power play as the Federal Government batted the ball of responsibility over the net to the states and territories who promptly batted it back asserting inadequate funding, and resources among other things. With this in mind, how does the Government propose to achieve harmonisation of state, territory and federal laws while also ensuring accountability and shared responsibility under the new framework?

The proposed reforms indicate that the Government is considering adding other agencies to the framework. However, it is not clear how these powers would be granted to additional agencies, under what conditions and what oversight rules would govern these agencies. For example, would the role of the Inspector General of Intelligence and Security (IGIS) be expanded? Specifically, will the reforms result in extending IGIS oversight if additional Agencies are granted powers? If so, has the impact on IGIS capability and resources been assessed? Further, how will command and control of surveillance activities be transparent, accountable and include meaningful oversight between agencies? Who will be responsible for overseeing intelligence and security agencies under the new framework? A robust threshold would be needed before an agency is added, particularly if the core business of that agency is not law enforcement. The key question remains, do these proposed new agencies need these additional surveillance powers in order to effectively perform their everyday functions?

Part 2: What information can be accessed?

We agree that the current definition of communications is unclear and its application to modern technologies is complex and artificial[1] . Any proposed definition of communications should keep the focus on human rights front of mind. One such definition could read: 'Communication includes any exchange or record of information or data in any form between two or more people, devices or locations.' However, any proposed replacement definition should be technology agnostic and capable of enduring beyond current technologies and those yet to be invented.

[1] Reform of Australia's electronic surveillance framework – Discussion Paper, p21.

The Discussion Paper talks at length about communications covering both information and data. Is it intended to distinguish a point of difference between data and information? If yes, does data in the context of the proposed reforms, mean raw data or cleansed data, transformed data or some other form of data set. Does information mean data plus the context behind or underpinning the data? The lack of clarity around what these words mean in the context of the proposed reforms suggest definitions should be given to data and information as part of the overall reframing of the definition of communications.

Part 3: How can information be accessed?

No comment at this stage.

Part 4: When will information be accessed?

The proposed harmonisation of legislative thresholds for covert access to private communications, content data and surveillance information where existing warrants are functionally equivalent has the potential to oversimplify governance and oversight. There is danger in a one size fits all approach. It may make operational sense to establish a common legislative threshold with respect to situations where a person *has committed* or *is engaged in* an activity relevant to security. However, it is far less straight forward with respect to obtaining warrants where a person is only suspected or is likely to (but actually hasn't) engaged in activities relevant to security. More detail is needed to fully explore the unintended consequences of these proposed provisions.

Likewise, the proposal to streamline thresholds that apply to law enforcement agencies' use of these powers to allow an issuing authority to authorise access to private communications and surveillance information if satisfied that a person has committed or is reasonably suspected of committing or is likely to commit an offence punishable by a maximum penalty of at least five years imprisonment. It is unclear what privacy protections would be established to complement the streamlined framework proposed in the Discussion Paper.

With respect to the proposed thresholds in relation to access to information about a person's location or movements, it is common knowledge that Big Tech routinely do this; think Google and Googlemaps. We question whether the proposed framework will have unintended consequences with respect to amplifying the reach of technology companies like Google, Meta, among others, and their ability to legitimately track a person's location or movement based on their online activities.

Necessity and proportionality are key, as is robust judicial oversight. We note that the Richardson Report recommended a reduction in judicial oversight on the basis that Ministerial authorisations and oversight by IGIS is sufficient; expressly stating that 'Ministers should continue to authorise ASIO and Intelligence Services Act agency activities. These authorisations should not also be subject to judicial or other independent authorisation.'[2] However, similar frameworks in other Five Eyes nations currently require judicial authorisation for their equivalent surveillance and electronic intelligence collecting powers. It is our firm view that Judges, Magistrates and / or AAT members should issue warrants for law enforcement agencies seeking access to information which they would otherwise be unable to access. This is critically important for several reasons including maintaining a clear

[2] Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community | Attorney-General's Department (ag.gov.au) at p63.

separation of powers. If judicial oversight is not present, what would be considered a reasonable and proportionate alternative to ensure legitimate use and execution of powers?

If the Government is serious about garnering public trust and confidence in the proposed surveillance framework, maximum rigour in the form of clear separation of powers and robust judicial oversight is vital in our view.

Part 5: Safeguards and oversight

As mentioned above, these reforms offer a unique opportunity for the Government to reposition surveillance powers, with human rights at the centre of the new framework, which is consistent with the fundamental, guiding principle that the national security framework exists to protect freedoms for all Australians.

Currently, limited statutory protection exists under the Uniform Evidence Acts under which privilege may be availed to resist disclosure of certain information in a court of law. These reforms offer a timely opportunity to enshrine the common law immunity allowing an individual or individuals to resist demands to disclose information or produce documents relating to lawyer client communications, into comprehensive statutory protections for legally privileged information.

Public expectations in relation to oversight of these powers, put human rights and freedoms[3], at the top of the list of priorities. Accordingly, the new oversight framework must be designed to meet those expectations, whilst balancing them against national security concerns. A key measure in safeguarding these fundamental human rights is for robust judicial oversight. Further, a federal human rights framework should be established prior to the implementation of the proposed surveillance reforms – it makes sense that national security and surveillance powers follow or should be woven into a federally legislated human rights framework. The protection of human rights and related freedoms underpins the rationale for national security legislation, it therefore follows that human rights should be at the centre of these reforms. It would be prudent to consider Australia's human rights obligations established under international law and international treaties to which Australia is a signatory in any reform.

We note the proposal to remove information regarding electronic surveillance and warrant registers from reporting requirements if it does not assist meaningful transparency. It would be useful to understand if the draft legislation proposes a definition of 'meaningful transparency' for reporting purposes. Is a definition being contemplated by Government?

Additionally, the Richardson Review recommended (at Recommendation 145), for IGIS to be subject to a legislative requirement to report annually on public interest disclosures received by, and complaints about similar conduct made. However, this does not appear to be addressed directly in the Discussion Paper. We note the intention that the Government will consider how reporting and record keeping can be revised and streamlined to effect meaningful transparency, however it is not clear if this revision extends to adding reporting obligations to IGIS. With respect to streamlining

[3] Including but not limited to the right to privacy and the expectation that their personal data will be protected and not disclosed without legitimate, reasonable and proportionate legal cause.

existing record-keeping and reporting obligations to ensure effective and meaningful oversight, we question the overall impact to IGIS. Specifically, will the reforms result in extending IGIS oversight if additional Agencies are granted powers? If so, has the impact on IGIS capability and resources been assessed? Further, how will command and control of surveillance activities be transparent, accountable and include meaningful oversight between agencies? Who will be responsible for overseeing intelligence and security agencies under the new framework?

We also note the reference again to 'meaningful transparency' and suggest that this concept be explicitly defined.

Part 6: Working together: Industry and Government

It is highly unlikely that Agencies will have the capacity to store all the data and information gathered or operate at speed and scale. Trusted Industry partnerships will be critical in enabling and ensuring that Agencies take full advantage of emerging and disruptive technologies.
Synergy welcomes the opportunity to discuss this aspect further.

Part 7: Interaction with existing and recent legislation and reviews

Data generated by the 'Internet of Things' and other devices, including OTT applications, software programs etc is produced in unfathomable quantities. Not all this data and information should or needs to be retained by providers. Questions of storage capacity, and as mentioned above in response to Part 6, It is highly unlikely that Agencies will have the capacity to store all the data and information gathered or operate at speed and scale. This may raise environmental questions for the Government to answer, including regarding the amount of power needed to sustain data centres and how that power is sourced, for example whether coal powered or via a more sustainable form of power generation.

At this juncture, with the information provided, it is unclear what the full scope of unintended consequences might be with respect to limiting the expansion of the Public Interest Advocate (PIA) framework only in relation to journalists and media organisations. An examination of the role, scope and purpose is needed. Equally important is the need to establish clear criteria for the skill set required for a PIA. For example, if the PIA has no training or background in media and journalism, they will likely be an ineffective advocate for journalists. There needs to be clear legislative provisions around the skills and qualifications of a PIA.

Conclusion

In line with the Richardson Review's recommendations, the Government's discussion paper promises to ensure that Australia's surveillance laws are technology-neutral and relevant to both current and future technologies. However, the devil will be in the detail, and it remains to be seen how the drafting of the new legislative framework will capture and balance the appropriate and measured surveillance of bad actors whilst ensuring the broader remit of reform; that the legislative framework is rendered fit for purpose now and in the future.

The Government has indicated that it is looking to countries who have successfully undertaken a reform of this nature, specifically the Five Eyes nations. However, there is no 'one size fits all' method to reforms of this nature and the Government will need to ensure that the draft legislation is appropriately customised to suit Australia's unique circumstances.

The extent of the impact of these reforms on Government agencies, Industry and citizens is yet to be assessed. However, the scope of the reforms, in particular how robust the oversight provisions are, will ultimately determine the level of public confidence and trust in the new framework. Indeed, rigorous and independent judicial oversight will be essential to achieving this public trust and confidence. Whilst reform is required to provide for necessary safety and security, there is also a need to balance any such reforms with necessary democratic accountability and basic freedoms that citizens deserve.

We note that this is just the beginning of the consultation process and welcome the opportunity to continue the discussion. If you have any questions or require clarification of any view expressed above, please do not hesitate to reach out to us.

~

About Synergy Law

Synergy Law is a Synergy Group legal offering, specialising in Government law and legal advisory services. Synergy Law also looks to opportunities Government can 'lean into' future legal issues such as cyber security, infrastructure security, emerging energy resources, climate law, ICT and technology, data sharing and information law, to support Government operations becoming 'future ready.' If you would like to know more, reach out to Melanie Hutchinson (mhutchinson@synergygroup.net.au) and Bobbi Campbell (bcampbell@synergygroup.net.au)