Tech Council of Australia
www.techcouncil.com.au

11 Feb 2022

[redacted]
Assistant Secretary (A/g)
Electronic Surveillance Reform Branch
Department of Home Affairs

Thank you for the opportunity to respond to the discussion paper on reform of Australia's electronic surveillance framework. The Tech Council of Australia (TCA) supports the development of a strong and safe digital economy that respects Australians' private information. As such, we welcome engagement to ensure electronic surveillance is as practical, respectful and transparent as possible.

About the Tech Council of Australia (TCA)

The TCA is Australia's peak industry body for the tech sector. The Australian tech sector is a pillar of the Australian economy, contributing $167 billion per annum, and employing 861,000 people. This makes the tech sector equivalent to Australia's third largest industry, behind mining and banking, and Australia's seventh largest employing sector.

Representing a diverse cross-section of Australia's technology sector, including hosts of large online platforms, telecommunications companies, firms developing and rolling out Internet of Things applications and equipment, and small and medium enterprises (SMEs). This means the TCA has unique insight into the diverse implications electronic surveillance laws have on the full spectrum of Australian technology companies, users, and the broader ecosystem.

Reform of Australia's electronic surveillance framework

The TCA supports efforts to create a single, streamlined and technology-neutral surveillance framework. Australia's current system is piecemeal, decentralised and difficult even for larger technology firms to parse. Decades of incremental changes have made it difficult for technology firms to contribute to the overall design of Australia's legislative framework.

This reform is an important opportunity to embed principles, practices and protections that balance privacy and law enforcement priorities clearly and consistently. It has the potential to create a surveillance framework that can adapt with technology, deliver significant regulatory reform that will reduce burden on the private sector and enable the Government to continue to conduct legitimate law enforcement activities. We are supportive of efforts to modernise Australia's surveillance framework that do not seek to expand powers or modify established norms around content.

Given the importance of this reform, the TCA and our members strongly support thorough, frank and ongoing consultation. We hope this submission will serve as the starting point for trusted and continuous engagement as this reform progresses. Through the technical expertise our members have to offer, we would welcome the opportunity to co-design details of legislation to ensure it meets its objectives as practically and effectively as possible.

At this early stage and as details are refined, the TCA recommends adopting the following design principles to help fulfil the overarching objectives of the reform:

1. **Open, inclusive and transparent oversight**: oversight of warrants must be transparent and involve the judicial system to the greatest extent possible. Oversight and safeguards should also be informed by technical expertise, both during the policy design phase and upon implementation. Strong accountability mechanisms are vital for public confidence in any reform efforts.

2. **Respecting Australians' privacy through precise and proportionate access**: even data and metadata that might appear benign can be highly sensitive, especially when combined. Reforms should ensure information is accessed as close to a person of interest as possible and prevent unintentional collection of third-party information. Using intrusive powers must also be proportionate to the offence being investigated, even when said powers are the best or only method of investigation.

3. **Clear, practical, and technically-informed design**: defining which data and collection methods are in-scope in a clear and technology-neutral manner will provide certainty and protect against scope creep. These definitions and warrant processes should be centralised and informed by technical expertise to avoid costly, burdensome, and conflicting obligations. Early and ongoing industry engagement will help to ensure reforms are practical, achievable and minimise unnecessary costs.

With these principles in mind, the TCA has the following comments on specific aspects of the discussion paper. We hope for these views to be the start of an ongoing collaboration that helps the Government to deliver practical, effective, and proportionate reforms.

Open, inclusive and transparent oversight

TCA members consider strong oversight and safeguards as essential to public confidence in any reforms and Australia's digital communications ecosystem. We welcome acknowledgment that the powers within this reform effort are intrusive and require robust independent oversight. At this juncture, simplicity and transparency are equally paramount to ensure the Australia public can easily understand the intent and impact of any reforms.

Reform efforts must also make accountability a priority. To enshrine strong accountability mechanisms, we recommend that warrant regimes involve independent judicial oversight and meaningful reporting to the greatest extent possible. We note that some discussions proposing harmonising legislative thresholds (q. 17) risk transferring authority for certain warrants from the judiciary to the Attorney-General. To avoid watering down oversight of such intrusive powers, we recommend erring in favour of the judiciary wherever Government looks to harmonise processes that currently have differing authorising channels.

As governments in free societies face an increasing diversity of threats, particularly in the cyber realm, compliance and oversight mechanisms governing intelligence and law enforcement collection of data must keep pace. International terrorist groups have not historically engaged in election interference, for example, but nation-state actors do so, which requires oversight to protect against possible (perceived) politicisation of intelligence and collection authorities, as well as other, more traditional forms of abuse.

In the context of criminal investigations, we recommend that the framework also include safeguards to provide notice to impacted users unless doing so will compromise the

investigation. Such notice to the impacted user is a fundamental mechanism to ensure individuals' rights are respected and accountability is ensured.

Relatedly, enterprise customers of providers expect that governments will come to them directly should law enforcement authorities seek enterprise data, just as governments around the world did prior to the enterprise moving to the cloud. Bypassing an enterprise customer by going through the cloud service provider is not necessary or proportionate unless the enterprise is wholly corrupted with criminal conduct or its most senior leadership is under investigation and the company otherwise lacks a robust compliance structure.

It is also important that oversight and review mechanisms are informed by technical expertise, and able to consider different modes of collection on their individual merits. We would welcome an opportunity to discuss how this expertise might best be delivered.

Further, while supportive of efforts to create a technology neutral framework, strong and thorough safeguards remain essential. We advocate caution in any shift to 'outcome-based' approaches to warrants that bundle different collection methods together without regard to the methods used (q. 16).

Failing to consider methods risks unintentional scope creep, significant regulatory burden and unnecessarily intruding on the privacy of third parties. For example, intercepting live communications is less invasive and burdensome than combining this interception with information stored by a carrier (see section below titled 'Aggregating warrants' for further discussion). Similarly, using a tracking device is less invasive and burdensome than combining with access to wider location data (see section titled 'Access to information about people's movements' for further discussion).

We instead recommend a technology neutral framework that embeds case by case technical advice on the most precise communication method to access necessary information and targets any warrant at this specific pathway. This approach would draw on technical expertise to specify which collection method(s) are sufficient to access necessary information, while minimising unnecessary burden and invasions of privacy.

There must also be a clear and direct mechanism by which providers can challenge overbroad, unreasonable, or otherwise illegal orders. Surveillance authorities should include a statutory right to appeal for providers and, where appropriate, for impacted individuals. The right to appeal should recognise a comity challenge based on any conflicts of law present should the provider be compelled to comply with the order. With regards to reporting requirements, we believe that governments, without compromising ongoing investigations, should provide extensive reporting on their use of criminal and national security surveillance authorities and should allow providers to do the same.

In response to the question of oversight (q. 30), we would recommend a consolidated framework that learns from other jurisdictional regimes that currently (or will in the future) allow access to data from 'communication services' and how they work.

Respecting privacy of Australians through precise and proportionate access

We believe that the rules that govern the search and seizure of data in the virtual world should be no less privacy protective than rules in the physical world, and in some instances the virtual world merits additional protections. Reform efforts must ensure strong data protection safeguards. For example, allowing interception of personal information, even if done in the name of public safety, implicates user expectations of private communications.

In order to achieve both public safety goals and data protection safeguards, regulation must take into account those legitimate security and privacy concerns (e.g. concerns that the new framework will require providers to build new decryption/interception capabilities).

In response to the question of whether there are any additional safeguards that should be considered in the new framework (q. 28), we recommend that the Department of Home Affairs explicitly state the responsibility of law enforcement and national security officers to protect information obtained using statutory powers.

Advancing technology challenges existing rules and approaches to privacy. Just as physical trespass is no longer the sole hallmark of an invasion of privacy in American jurisprudence, so too in the digital era new rules must be adopted to keep up with a changing world. We always favour targeted collection over bulk collection, and believe the latter is tolerable, if at all, only in very narrowly and carefully drawn circumstances. We strongly recommend that safeguards establish clear aims to minimise impacts on third party interests, and actions that may undermine the security of a communications product, service, network, or platform.

Getting the balance right is a complex and technical issue that warrants a close and ongoing conversation. Below are some examples of topics we would welcome the opportunity to discuss further.

Aggregating warrants (q. 15, section commencing p. 33)

The TCA supports a warrant framework that recognises impacts on privacy, and a framework that reflects current ways people communicate and interact. However, we do not support 'bundling' different communication types together under a single warrant. We have concerns such an approach would undermine the precise and proportionate use of surveillance powers in a way that respects the privacy of Australians. As flagged above, different types of communication vary in the depth, breadth and time horizon of information captured.

We note the discussion paper's reference to functionally equivalent powers in the Comprehensive Review, and we support moves to more consistent controls. That said, we strongly support the Comprehensive Review's acknowledgement that "…it does not follow that all agencies should have access to all electronic surveillance powers. Each request for new powers should be considered individually on its merits." (Volume 2, paragraph 27.31 refers.)

This is because aggregated access to all forms of Australians' private information has a much greater minimum impact on privacy than warrants targeted at specific communication channels. As a result, 'bundled warrants' inevitably shift the current policy balance away from Australians' privacy in favour of law enforcement. While some communication channels may tend toward having overlapping information generally, each circumstance is unique and should be assessed on a case-by-case basis. More intrusive surveillance

methods should only be used where proportionate to the law enforcement objective, and where less invasive alternatives do not provide access to necessary information.

As mentioned earlier in this submission (regarding q. 16), a bundled approach would impede privacy considerations when relevant authorities consider a warrant. Where currently an issuing authority might find less intrusive forms of surveillance sufficient and proportionate, bundled 'outcomes-based' warrants risk forcing an authority into a binary choice between all forms of surveillance, or none at all. We instead recommend a technology neutral approach that retains a focus on using the fewest and least invasive means of surveillance necessary.

Warrants for objects, third parties and groups (q. 17, section commencing p. 38)

As noted above, we welcome efforts to harmonise limits, controls and safeguards where powers are functionally equivalent. However, efforts to streamline should not water down protections and safeguards to the lowest common denominator. As noted above, the TCA particularly supports erring toward the involvement of the judicial system, informed by technical advice, wherever inconsistencies arise.

This holds especially true for any circumstance where agencies seek to use powers against objects, third parties and groups. We recognise that the current electronic surveillance framework is complex and inefficient to navigate. In rethinking this framework and considering what, how and when information may be accessed, clear guardrails and guiding principles are critical to ensure that the new framework is proportionate and able to properly protect individuals' security, privacy and control over their data.

We believe a careful, targeted and consistent view of the subject of the surveillance in each case will help to meet these aims. In considering which surveillance methods are least invasive, we recommend enshrining that access should always be related to the person that is the subject of the surveillance, and that access should be sought at a level as close to this subject as possible.

Given the potentially significant collateral impact on other Australians' privacy, circumstances for these powers should be truly exceptional. As noted above, when third-party interests are implicated those should be recognised and wider collection should be tolerable, if at all, only in very narrowly and carefully drawn circumstances. We recommend that these circumstances, at minimum, include a higher offence threshold than more precise methods, and evidence there is no other practical way of collecting necessary information.

Warrants for minor offences (q. 17, section commencing p. 38)

The TCA strongly opposes exceptions that would bypass sentence-based thresholds in any circumstances (p. 41 of the discussion paper refers). Our view is consistent with the Comprehensive Review, which explicitly disagreed with granting two-year offences exceptions to a three-year threshold. As the review noted, "it would be disproportionate to enable warrants to be available for all crimes merely because they involve a cyber element".

Three years is already a very low bar for the use of intrusive powers, which risks capturing many offences that Australians may not expect or agree with. Surveillance powers must only be used for offences with maximum sentences between three and five years in truly exceptional circumstances where less intrusive forms of evidence gathering have been genuinely attempted and exhausted, and there is compelling reason to believe surveillance powers would provide necessary information.

Any breaches of such a low threshold would be a disproportionate sacrifice of Australians' privacy and inconsistent with the recommendations of the Comprehensive Review. The Review is clear: "offences should only be included as exceptions to the five year threshold for surveillance if they are punishable by at least three years' imprisonment and the use of electronic surveillance powers is necessary in order to effectively investigate the offences".

Respect for Australians' privacy and the invasiveness of these powers means restricting their use to serious offences, which means consistent sentence-based limits. We recognise there may be circumstances where surveillance powers might be the only means of investigation. However, it is difficult to argue Australians' privacy is respected if, in practice, privacy can be systematically breached when investigating relatively minor offences.

The review also noted "to the extent that the offences are more serious than the applicable penalties might suggest, the appropriate way forward would be to adjust the penalties". Such an approach would deliver far greater consistency, accountability and transparency than case-by-case exceptions, with far less risk of ever-expanding scope creep.

We strongly recommend ruling out any exceptions that would allow surveillance warrants to bypass all sentence-based thresholds, noting that any such use would be a disproportionate invasion of Australians' privacy.

Where offences under a three-year threshold rely on intrusive surveillance powers to investigate, we recommend instead assessing whether these offences are sufficiently severe to warrant longer sentences and the powers of investigation these sentences entail.

For offences with maximum sentences of three to five years, we recommend requiring clear evidence less intrusive evidence gathering has been genuinely attempted and exhausted, and compelling reason to believe surveillance would provide necessary information.

We note the Comprehensive Review's recommendation to reduce general maximum sentence requirements from seven to five years. To assess the practicality and privacy impact of such a change, we recommend setting out clearly the range of offences likely to fall under this reduced threshold as soon as possible.

Access to information about peoples' movements (q. 19, section commencing p. 44)

While we note the Comprehensive Review's finding that tracking devices may not be as invasive as other forms of surveillance, we do not recommend extrapolating this finding to all forms of information on a person's location and movements. As the Review notes, monitoring someone's movements or 'pattern of life' over an extended period is "highly intrusive" (volume 2, paragraph 19.3 refers).

Tracking devices and other pre-existing types of information about peoples' movements are not functionally equivalent – and is a case example of why clear definitions that recognise methods of collection will continue to matter in a future framework. While information on location or movements might appear benign, it is uniquely prone to accumulation over time and retrospective access.

For instance, with user consent, online platforms can securely record and host years' worth of historical information on a user's location and movements. While a person's movements might be typically observable to others in passing, a reasonable person will feel differently about information capturing months or years' worth of prior movements. The invasiveness

of this is clearly greater than surveillance devices that only begin to collect information once a warrant has been issued.

For this reason, wider information on movements warrants stricter limitations compared with conventional tracking devices. Such devices are inherently less invasive as, unlike privately held tracking information, their reach cannot extend back in time.

For this reason, the TCA recommends that any further investigation of reforms targeting peoples' movements focus explicitly and exclusively on tracking devices – consistent with Recommendation 92 of the Comprehensive Review. We also recommend clarifying that 'tracking devices' refers to devices that exclusively conduct 'live' tracking, and excludes privately-held multipurpose devices (e.g. mobile phones) with location tracking capabilities and access to location data prior to a warrant being issued.

Privacy impacts of metadata, stored data and retention (q. 8-13, section commencing p. 23)

We strongly support the discussion paper and Comprehensive Review's acknowledgment that current settings make outdated assumptions about the intrusiveness of particular types of information and collection methods. As the Government contemplates updates to address these assumptions, they must take into account the potential sensitivity of metadata.

Contrary to even relatively recent assumptions, metadata can be just as sensitive as other forms of information. This should be considered seriously when assessing which bodies should have access to this information (p. 17 refers). Metadata should not be available to agencies based on a written notice only. Further, access to metadata by agencies, including by means of technical assistance, warrants a higher bar than merely being of general assistance. In line with other forms of private information, metadata should only be made available when specifically required in relation to a known offence. To this end, we recommend bolstering the thresholds and processes for accessing metadata to better reflect its sensitivity.

Similarly, we support the discussion paper's suggestion that stored data has become more sensitive than it might have been in decades past. Aggregated stored data is now as intrusive as live communications, and in some cases is arguably more so. Recognising this would demonstrate privacy is a serious consideration of Government, and help to build vital social licence for other actions. We recommend bringing the thresholds for accessing stored data up to the same standard as live communications.

We would also support the Government exploring the wider implications of stored data becoming more sensitive. For instance, under the Customs Act 1901, border officials can force Australians to provide access to stored data on the mere suspicion a person may be of interest for a wide variety of reasons, and make copies if data "could" contain information related to an offence or a security matter. These reasons do not need to be substantiated nor provided. It is difficult to reconcile this burden of proof with other domestic settings, including surveillance laws, which better balance privacy and law enforcement priorities. We recommend that Government consider wider policy updates to reflect the sensitivity of stored data in the digital era, including in the Customs Act 1901.

Particularly in the digital era, we believe that limitations on post-acquisition conduct – such as retention, querying and other use, and dissemination of data – are an important part of any legal regime. We recommend requiring clear justifications for ongoing retention and

collection of data. We also recommend ensuring emergency access authorisations are carefully limited, and subject to full-dress review as soon as practicable after the fact.

To remove any doubt, the TCA would not support attempts to expand mandatory data retention to other platforms or types of data. Consistent with our view that information should be accessed as close to a person of interest as possible, Governments should prioritise obtaining necessary information, including stored information, by targeting individuals and data owners over platforms and providers. Access through both channels would be needlessly redundant and, consequently, disproportionate.

Unnecessary retention of data also creates both cybersecurity and privacy risks, and imposes these risks on every Australian that uses digital communications. Any such attempts would almost certainly also attract widespread public attention and risk impacting Government's social licence for more practical and necessary reforms. For these reasons we recommend ruling out any expansions of mandatory data retention as soon as possible.

Clear, practical, and technically robust design

As the discussion paper acknowledges, the current legislative framework is overly burdensome and complex. It imposes a significant regulatory burden on industry, especially small to medium companies. This burden is not solely derived from the complexity of the current system, but also the varied levels of technical experience and expertise across enforcement and regulatory agencies. This results in disconnects between policy intent and impact, and gaps between agency expectations and what is feasible or sustainable for technology firms. The TCA and its members welcome Government efforts to reduce regulatory burden to address unnecessary complexities and inconsistencies.

Surveillance reform must be both future proof and enshrine protections against scope creep. The discussion paper rightly notes that as technologies, and data collection tools, evolve, surveillance often takes entirely new forms. A technology neutral framework will avoid these reform efforts becoming either obsolete or overly broad. Furthermore, in response to the question about who the framework could best account for emerging technologies (q. 7), we recommend undertaking a dedicated expert review, consultation and report outlining clearly which criteria are used to determine what information gathering techniques are in-scope would ensure criteria do not shift over time. A similar effort is ongoing for "ancillary services" under ePrivacy Regulation.

We welcome strong policy agency leadership with a whole-of-government perspective in this review, as well as industry representation to help identify practical realities and appropriate criteria. Submissions to the Comprehensive Review demonstrate frontline agencies will apply pressure to loosen definitions, thresholds, and oversight. Given the intrusive nature of these powers, frontline pressure for flexibility must be balanced against the bigger picture: a need for proportionality, accountability and certainty for citizens and industry alike.

We also welcome central leadership and early consultation as such fundamental reform will be highly technical and complex. Establishing clear definitions and principles behind processes are just the start. Ongoing collaboration will be essential to ensure details are as clear, practical and technically robust as possible.

Clear and consistent definitions

Clear and consistent definitions are vital for TCA members, and for the next steps of this reform process. We welcome efforts to better clarity key terms and concepts such as

'communication', 'content' and 'stored communication'. Definitions such as these have serious implications for members both in terms of which businesses are impacted, and what the obligations imposed on impacted businesses would be.

Loosely or improperly defined terms will unnecessarily impact broad swathes of Australia's technology sector, imposing preventable and significant regulatory burden. This reform is a vital opportunity to embed clear and universal definitions for the terms and concepts that underpin surveillance and collection actions across agencies.

We are aware that the definition of "communication," as well as traditional distinctions between content and metadata, are under pressure as technology advances, and we are also aware of views that this makes things too complicated. We continue to believe, however, that there is a meaningful distinction between content and non-content, at least in many cases, and remain generally comfortable with the distinction in UK law and US law, between the "substance, purport, or meaning" of a communication (see 18 U.S.C. § 2510(8)), and "dialling, routing, addressing, and signalling information" (see 18 U.S.C. § 3127(3)-(4)).

We generally support the three-tier categorisation of data as reflected in U.S. law and in the European Union's eEvidence proposal, differentiating between content, traffic data, and basic subscriber records.

That said, and as acknowledged above, the implications of non-content information for core privacy rights have increased and warrant significant protections. Certain non-content traffic data can be extraordinarily revealing and privacy intrusive. Compelled access to such data should require prior judicial approval and independent oversight. Geolocation information deserves treatment as highly sensitive data, similar to content data. And any real-time monitoring should be subject to the most robust safeguards and oversight in law. A future-proofed system should be capable of distinguishing these types of data to consider their merits and privacy impacts independently.

We recommend establishing clear and consistent definitions very early in the policy development process, in consultation with the technology sector, given how integral these definitions will be to the design and impact of future reforms. The TCA would welcome the opportunity to be a part of this policy design and review process.

Centralised and practical processes and obligations

We also welcome efforts to clarify which agencies have the power to request telecommunications data or metadata, and simplify warrant and data request frameworks. This reform is a vital opportunity to establish a centralised process for requests and approvals. Central oversight and authority for approvals is fundamental for transparency, accountability, and to manage the privacy and security risks that come from uncoordinated requests for information. Even without intent, aggregated data from piecemeal requests can ultimately turn into information that is more sensitive and invasive than the sum of its parts.

Reform efforts must also focus on the achievable. In response to the question of workability (q. 34), this means avoiding costly, burdensome, and conflicting obligations. To this end, efforts should look into the practical implications of extending the framework to cover 'communication services', with regard to mandatory data retention, interception capabilities and cooperation with enforcement authorities.

We believe centralising access requests through one or more 'clearing house' agencies would ensure that access requests benefit from increased consistency, clarity and technical

know-how. This would then result in requesting agencies being able to more efficiently and effectively obtain the information and data that they need, and recipient organisations being able to more easily understand and respond to these requests.

Further, the aggregation of these access requests through a centralised mechanism will provide stakeholders with a clearer and more comprehensive view of the access being requested, contributing to more accurate assessments of the necessity and proportionality of these requests. As such, we recommend establishing centralised processes for obtaining access where possible.

Related to clear and consistent definitions, the TCA would welcome early discussions on any industry obligations that might arise from access to stored data (q. 5-7). It is currently not clear how Government might intend to capture additional kinds of information, such as activities on the internet. We again emphasise that any such information should be collected as closely to the target individual as possible. Further to the security and privacy-based reasons outlined earlier in this submission, relying on upstream providers is not practical.

For example, the broad scope of Australians' internet activities would create enormous data storage requirements, imposing significant cost burdens on local industry. Further, warrants targeting individuals are likely to be functionally equivalent. It is unclear how any additional benefit is likely to outweigh significant regulatory costs, impacts on innocent Australians' privacy and impacts on Government's social licence for other security measures. We recommend ruling out measures that would impose significant additional data storage costs on Australian businesses.

The TCA also recommends clarity for industry through a Government commitment to develop a single, definitive list of entities that can access telecommunications data. TCA members currently respond to a wide range of public entities that likely fall outside the original intent of current legislation, including local councils and fair trading bodies.

In addition, the TCA recommends better checks and balances for non-law enforcement agencies that use sections 280(1)(b) and 313(3) of the Telecommunications Act to request information. Members have engaged with a number of entities that have failed to cover the costs of responding to a request. Not only is this contrary to legislation, but it also undermines industry's ability to support legitimate surveillance. Catering to wider requests diverts vital resources away from requests by law enforcement and security agencies, to entities that may not fall under the scope or the intent of the Act.

Further, the TCA recommends granting the Department of Home Affairs authority to provide ongoing interception exemptions where it is not possible to intercept data on certain products. Given these circumstances are highly unlikely to change, the requirement to apply for an exemption every year is unnecessarily burdensome for Government and providers.

Technically robust and future proofed reform through industry consultation

We acknowledge that the views above on definitions, processes and obligations are high level and that many details require refinement. As flagged throughout this submission, we hope this engagement marks the beginning of frank, trusted and ongoing collaboration as details are developed further. We recommend that Government engage closely and consistently with industry throughout the policy development process, including on how technical expertise can be integrated into implementation of future reforms.

We are grateful for current efforts to convene a roundtable between Home Affairs and TCA members. Looking to the future, the TCA and its members would welcome early, ongoing, and formal engagement on technical requirements, engineering requirements and specific legislation between now and when reforms are considered by the Parliamentary Joint Committee on Intelligence and Security.

We would also welcome discussions on how technical expertise might be built into the operation of any reforms once they are implemented. As noted above, it is important that oversight and review mechanisms are informed by technical expertise. In practice, this may take the form of an independent advisory function that provides confidential technical advice on how individual warrants might best be targeted. The specific complexities of each situation merit a means of providing tailored technical advice on a case-by-case basis.

Further to case-by-case consultations, it may be appropriate to establish more durable groups, with representatives from industry and government, to discuss longer-term issues outside the pressured environment of a particular investigation. We have also found that having a single point of contact within a governmental entity helps to ensure consistent communication and can avoid misunderstandings and work through logistical, technical, and legal restrictions that impact providers' ability to respond to governments' legal process.

We would encourage the Government to supply meaningful use cases or examples to support reforms. With broad changes that can potentially impact a wide variety of services it is significantly easier to reach a concrete legal and engineering view of reforms when they are supported by examples. We would also encourage the Department to use case studies that cover the broad nature of offences and activities that could be enabled rather than focusing on niche severe cases.

We appreciate the opportunity to contribute feedback to the ideas proposed and look forward to ongoing dialogue.

Yours sincerely,

Kate Pounder
CEO, Tech Council of Australia
e: kate@techcouncil.com.au
m: +61 402 110 498

Summary of TCA Recommendations

Open, inclusive and transparent oversight

1. To enshrine strong accountability mechanisms, we recommend that warrant regimes involve judicial oversight and meaningful reporting to the greatest extent possible.
2. In the context of criminal investigations, we recommend that the framework also include safeguards to provide notice to impacted users unless doing so will compromise the investigation.
3. We instead recommend a technology neutral framework that embeds case-by-case technical advice on the most precise communication method to access necessary information and targets any warrant at this specific pathway.
4. We would recommend a consolidated framework that learns from other jurisdictional regimes that currently (or will in the future) allow access to data from 'communication services' and how they work.

Respecting privacy of Australians through precise and proportionate access

5. We recommend that the Department of Home Affairs explicitly state the responsibility of law enforcement and national security officers to protect information obtained using statutory powers.

Aggregating warrants

6. We strongly recommend that safeguards establish clear aims to minimise impacts on third party interests, and actions that may undermine the security of a communications product, service, network, or platform.
7. We instead recommend a technology neutral approach that retains a focus on using the fewest and least invasive means of surveillance necessary.

Warrants for objects, third parties and groups

8. We recommend enshrining that access should always be related to the person that is the subject of the surveillance, and that access should be sought at a level as close to this subject as possible.
9. We recommend that these circumstances at minimum include a higher offence threshold than more precise methods, and evidence there is no other practical way of collecting necessary information.

Warrants for minor offences

10. We strongly recommend ruling out any exceptions that would allow surveillance warrants to bypass all sentence-based thresholds, noting that any such use would be a disproportionate invasion of Australians' privacy.
11. Where offences under a three-year threshold rely on intrusive surveillance powers to investigate, we recommend instead assessing whether these offences are sufficiently severe to warrant longer sentences and the powers of investigation these sentences entail.
12. For offences with maximum sentences of three to five years, we recommend requiring clear evidence less intrusive evidence gathering has been genuinely attempted and exhausted, and compelling reason to believe surveillance would provide necessary information.

13. We note the Comprehensive Review's recommendation to reduce general maximum sentence requirements from seven to five years. To assess the practicality and privacy impact of such a change, we recommend setting out clearly the range of offences likely to fall under this reduced threshold as soon as possible.

Access to information about peoples' movements

14. We recommend that any further investigation of reforms targeting peoples' movements focus explicitly and exclusively on tracking devices – consistent with Recommendation 92 of the Comprehensive Review.
15. We also recommend reaffirming that in this context, 'tracking devices' refers to specialised devices, not privately-held multipurpose devices with location tracking capabilities.

Privacy impacts of metadata, stored data and retention

16. We recommend bolstering the thresholds and processes for accessing metadata to better reflect its sensitivity.
17. We recommend bringing the thresholds for accessing stored data for surveillance purposes up to the same standard as live communications.
18. We recommend that the Government consider wider policy updates to reflect the sensitivity of stored data in the digital era, including in the Customs Act 1901.
19. We recommend requiring clear justifications for ongoing retention and collection of data. We also recommend ensuring emergency access authorizations are carefully limited, and subject to full-dress review as soon as practicable after the fact.
20. We recommend ruling out any expansions of mandatory data retention as soon as possible.

Clear, practical, and technically robust design

21. We recommend establishing clear and consistent definitions very early in the policy development process, in consultation with the technology sector, given how integral these definitions will be to the design and impact of future reforms.
22. We recommend establishing centralised processes for obtaining access where possible.
23. We recommend ruling out measures that would impose significant additional data storage costs on Australian businesses.
24. The TCA also recommends clarity for industry through a Government commitment to develop a single, definitive list of entities that can access telecommunications data.
25. In addition, the TCA recommends better checks and balances for non-law enforcement agencies that use sections 280(1)(b) and 313(3) of the Telecommunications Act to request information.
26. Further, the TCA recommends granting the Department of Home Affairs authority to provide ongoing interception exemptions where it is not possible to intercept data on certain products.
27. We recommend that the Government engage closely and consistently with industry throughout the policy development process, including on how technical expertise can be integrated into implementation of future reforms.