We welcome the opportunity to respond to the Department of Home Affair's consultations for the reform of Australia's electronic surveillance framework. The initiative is a unique opportunity to establish a modern enduring framework. Microsoft has been present in Australia for over 30 years, today we have over 10,000 partners in Australia working with us – 69 per cent of them are small businesses and combined they employ 300,000 Australians. Our company mission is to empower every person and organisation on the planet to achieve more, and we measure our success by the success of our customers and partners. Microsoft recognises the importance of public-private partnerships in developing and implementing these critical reforms and remains committed to working with the Government to improve Australia's surveillance framework.

GENERAL COMMENTS

As Microsoft has shared with the Department of Home Affairs previously, we have long called for governments to modernize law enforcement access to digital evidence and to reconcile conflicts of law that result when governments seek cross-border data. We have centered our call for international agreements to govern law enforcement access to data around six principles. This was in keeping with our obligation, as a global company with millions of users, to help policymakers "confront critical questions about how to protect privacy and give law enforcement the tools they need to keep us safe." In short, our ongoing approach to addressing these challenges is very much consistent with your current undertaking, and we are once again pleased to participate and assist you where we can.

The six principles we announced in 2018, all of which we think apply in the present moment, are as follows:

1. **The universal right to notice** – Absent narrow circumstances, users have a right to know when the government accesses their data, and cloud providers must have a right to tell them.
2. **Prior independent judicial authorization and required minimum showing** – Law enforcement demands for content and other sensitive user data must be reviewed and approved by an independent judicial authority prior to enforcement of the order, and only after a meaningful minimum legal and factual showing.
3. **Specific and complete legal process and clear grounds to challenge** – Cloud providers must receive detailed legal process from law enforcement to allow for thorough review of the demand for user data, and must also have clear mechanisms to challenge unlawful and inappropriate demands for user data.
4. **Mechanisms to resolve and raise conflicts with third-country laws** – International agreements must avoid conflicts of law with third countries and include mechanisms to resolve conflicts in case they do arise.
5. **Modernizing rules for seeking enterprise data** – Enterprises have a right to control their data and should receive law enforcement requests directly.
6. **Transparency** – The public has a right to know how and when governments seek access to digital evidence, and about the protections that apply to their data.

We developed and explained these principles further in a three-page, public document that is available here.

We also ground our comments below in an additional, and we believe shared, objective: the need for clarity and simplicity in surveillance law. With the rapid development of technology and an abundance of often outdated, Byzantine legal regimes governing lawful access to data, a lack of clarity and simplicity inevitably generates confusion, resource-intensive disputes, delays, and errors, and ultimately threatens both security and privacy. Lastly, given the difficult and unique challenges raised by cross-border data requests, we believe it's important that this effort and the questions presented consider particular circumstances if the Australian government were to seek data pertaining to an individual located outside of Australia.

SPECIFIC COMMENTS

Consistent with the principles described above, we offer the following additional comments on the Discussion Paper, including responding to certain questions set out in the Paper:

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?
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?
2. Do the existing prohibitions and offences against unlawful access to information and data adequately allow the pursuit of other objectives, e.g. cyber security of networks, online safety or scam protection/reduction?
3. Are there agencies you consider should have powers to access particular information and data to perform their functions? If so, which agencies, and why?
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?

Comments on Part 1:

Existing prohibitions against unlawful access to data as applicable to government requests for data vary considerably depending on the specific legal authority—which often relies on outdated assumptions and terms, as referenced in the Discussion Paper—as well as the information sought and authority requesting access. Such differences are only compounded when considering cross-border data requests, which may result in technology providers being stuck between a valid request for data from one jurisdiction and a valid blocking statute or other restriction in another jurisdiction. While attempts to harmonize prohibitions on unlawful access to data are critical, and necessary to protect user privacy,

such efforts must also be viewed through the lens of international requests when technology providers and data itself transcend national borders.

At a high level, one could make the argument that laws which have as their primary focus the criminalisation of unlawful access to data could also contribute to maintaining cybersecurity of networks and maintaining the internet as a safe and fraud free space. However, they could not be seen to adequately allow the pursuit of these separate and distinct policy objectives. To illustrate this, it is important to recognise that:

- Cyberattacks happen despite unlawful access to data being a criminal offence.
- Breaches of online safety codes happen in instances where there may be no unlawful access to data.
- Online fraud primarily happens by taking advantage of a victim's trust and unauthorised access to their data could be seen as a technique to achieve that. Online safety awareness and education is key to dealing with online fraud.

Statutory prohibitions on intercept, and providing criminal penalties for the same, tend not to have serious impact in achieving improved online safety or reduction in online fraud. These two latter behaviours are generally not carried out by people intercepting networks - they are carried out by bad actors accessing a network legitimately but manipulating it for their own purposes. The most likely cross over objective with statutory prohibitions on unlawful access is to enhance or protect cybersecurity.

Additionally, Microsoft has not historically commented on which agencies of governments should be empowered to access information. However, in keeping with principles 1 and 6 described above, we believe that appropriate oversight mechanisms must include public transparency and independent oversight. As a general matter, where intelligence agencies enjoy access to information under more secretive legal standards than those applicable to law enforcement agencies (e.g., in the United States, FISA as opposed to the Stored Communications Act), secrecy should be carefully limited and other mechanisms, such as parliamentary or judicial oversight, should be enhanced.

Part 2: What information can be accessed?

4. Are there other kinds of information that should be captured by the new definition of 'communication'? If so, what are they?
5. Are there other key concepts in the existing framework that require updating to improve clarity? If so, what are they?
6. How could the framework best account for emerging technologies, such as artificial intelligence and information derived from quantum computing?
7. What kinds of information should be defined as 'content' information? What kinds of information should be defined as 'non-content' information?
8. Would adopting a definition of 'content' similar to the UK be appropriate, or have any other countries adopted definitions which achieve the desired outcome?

9. 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?
10. Should the distinction between 'live' and 'stored' communications be maintained in the new framework?
11. Do each of these kinds of information involve the same intrusion into privacy? Or should the impact of each be considered differently?
12. 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?
13. What are your thoughts on the above proposed approach? And in particular, how do you think the information captured by surveillance and tracking devices could be explained or defined?

Comments on Part 2:
We are aware that the definition of "communication," as well as traditional distinctions between contents and metadata, are under pressure as technology advances, and we are also aware of views that this makes things too complicated. We also believe that non-content information can implicate core privacy rights and deserves significant protections. This has been appropriately reflected in recent privacy regulations around the world, including the General Data Protection Regulation in the EU. We continue to believe, however, that there is a meaningful distinction between contents and non-contents, at least in many cases, and we 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 "dialing, routing, addressing, and signaling information," see 18 U.S.C. § 3127(3)-(4). Although there have been hard cases, we do not believe the distinction as applied in US law has broken down completely or that it should be jettisoned.

While the impact of disclosing stored communications can be just as privacy intrusive as disclosing real-time communications, we believe there are unique considerations specific to real-time surveillance that merit heightened and ongoing judicial review and minimization requirements.

We also believe that a compelled access framework should apply equally to providers likely to have relevant information and should not discriminate or provide a slanted regulatory playing field in favor of certain classes of providers.

Part 3: How can information be accessed?

14. How could the current warrant framework be simplified to reflect the functional equivalency of many of the existing warrants?
15. 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?

Microsoft

Comments on Part 3:

Wherever possible, we believe artificial distinctions in the law should be eliminated in favor of a functional approach focused on the privacy of the data in question. Experience teaches that market and technological developments will soon overtake legal categories focused on specific applications or technologies. This accords with the principle of clarity and simplicity described above.

Part 4: When will information be accessed?

16. 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?
17. Should the restrictions that apply to covert access to electronic information differ from those that apply to accessing similar information in the physical world?
18. Are there any other changes that should be made to the framework for accessing this type of data?
19. What are your views on the proposed thresholds in relation to access to information about a person's location or movements?
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)?
21. Is the proposed additional threshold for group warrants appropriate??
22. Is the proposed additional threshold ('impractical or ineffective') for warrants targeted at criminal networks and groups appropriate?
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?
24. Should magistrates, judges and/or AAT members continue to issue warrants for law enforcement agencies seeking access to this information?
25. What are your thoughts on the proposed principles-based, tiered approach to use and disclosure?
26. When should agencies be required to destroy information obtained under a warrant?
27. What are your thoughts on the proposed approach to emergency authorisations?

Comments on Part 4:

In general, we favor clarification and simplification of legal rules, as noted above. However, we recognize that this is a very difficult undertaking, for reasons explained here. We believe that the rules that govern the search and seizure of data in the virtual world should be no less privacy protective than those rules in the physical world, including the importance of providing the user notice of a demand for their data where it would not truly jeopardize the investigation. In some instances, the virtual world merits additional protections beyond those commonly afforded to searches in the physical world. In many respects, users can expect a higher level of security in the cloud for their most sensitive information compared to on-premises servers or physical storage options. And certain users, such as public sector

agencies and providers of critical infrastructure, would be unable to rely on the cloud and digital transformation generally without robust cybersecurity and privacy protections.

Separately, our main concern with group warrants is that governments are at a higher risk of encroaching on privacy rights of entirely innocent parties. The Discussion Paper elsewhere states that consideration will be given to incorporating the principles of necessity and proportionality to all applications for warrant, which is especially important in the group warrant context. Our initial impression is that the proposed language around the threshold test is vague and potentially confusing. The report states that "group warrants would only be available where the issuing authority is satisfied a warrant in relation to individual members of the group would be impractical or ineffective." These are concepts which are difficult to define. A statutory test setting out well defined and easy to understand criteria which must be met before a warrant was granted would be preferrable. The suggestion that a group warrant would not be available where the identities of all group members is known is open to circumvention.

The portion of the Discussion Paper that considers situations where an agency requires a service provider's assistance to execute the warrant merits further consideration. What happens if the group warrant includes a foreign national? Or an Australian who, during the currency of the warrant, travels to a jurisdiction which criminally prohibits intercepts on their territory (e.g., the U.S.). These are complications in a single target warrant which expand hugely when you consider multiple individuals in a group warrant. There is also no mention of whether it will be possible to sever a warrant if one target drops out of jurisdiction for example.

Moreover, additional consideration is likely required in relation to the interaction of the government agency with the service provider and what obligations each remain under during the currency of the warrant. For example, additional information would be helpful to evaluate what steps will the requesting agency take to notify the service provider if member(s) of the group leave the jurisdiction while the intercept is live; is the provider under an obligation to notify the agency if the target's geo location information indicates a change in jurisdiction; and what ability will there be for providers to challenge overly broad warrants.

Regarding access to information about a person's location or movements, we generally support the ideas that animate the U.S. Supreme Court's decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018). There, the Court recognized that advancing technology – particularly involving smart phones that track location over time – challenges existing rules and approaches to privacy. Just as physical trespass is no longer the sole hallmark of an invasion of privacy, so too in the digital era new rules must be adopted to keep up with a changing world.

We always favor targeted collection over bulk collection, and believe the latter is tolerable, if at all, only in very narrowly and carefully drawn circumstances. When third-party interests are implicated in data access, those should be recognized in the law as well, and we continue to oppose any collection method that would threaten the security of a

communications product, service, network, or platform. See principle 3 above. 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.

Further, when seeking information belonging to a commercial or public sector entity, including a school or nonprofit organization, we believe the principles of necessity and proportionality almost always require that law enforcement seek the information directly from the entity, and not from a cloud service provider. Simply because an entity has moved its operations to the cloud, does not mean it should lose its privacy rights and ability to protect its own privileges and prerogatives. The entity may also have access to information not within the possession, control, or custody of the provider and may otherwise be able to furnish responsive information to law enforcement more efficiently. Except in very narrow circumstances, such as when an entity is wholly dedicated to criminal activity, law enforcement should serve compulsory process on the entity and not the provider.

Regarding emergency requests, emergency authorizations for lawful access should be carefully limited, and subject to full-dress review as soon as practicable after the fact, in keeping with principle 2 above. Given that the process understandably does not involve the same oversight and safeguards as a traditional legal demand, we have found that it is important for service providers to retain discretion when evaluating an emergency so we can continue to quickly respond to documented threats to the life or safety of individuals in a way that is consistent with international laws and protects the privacy and human rights of our users.

Part 5: Safeguards and oversight

28. Is there a need for statutory protections for legally privileged information (and possible other sensitive information, such as health information)??
29. What are the expectations of the public in relation to oversight of these powers, and how can a new oversight framework be designed to meet those expectations?
30. 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?
31. How could the new framework streamline the existing record-keeping and reporting obligations to ensure effective and meaningful oversight?
32. Are there any additional reporting or record-keeping requirements should agencies have to improve transparency, accountability and oversight?

Comments on Part 5:
The existence of legal professional privilege (as well as other sensitive information, to include health information) is crucial to the proper functioning of a democracy's rule of law and the protection of fundamental rights. We support having clarity around these issues in statute and additional safeguards for surveillance that may impact these rights. We also believe, in the context of routine criminal investigations, individuals targeted by government

surveillance are in the best position to defend their rights and, absent narrow circumstances, should be provided notice prior to their data being disclosed. Such notice to the impacted user is a fundamental mechanism to ensure individuals' rights are respected and accountability is ensured.

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 ensure against possible (perceived) politicization of intelligence and collection authorities, as well as other, more traditional forms of abuse.

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. We note that increased investment in compliance and oversight bodies has substantial efficiency improvements for Government and decreased regulatory burden for technology companies.

Part 6: Working together: Industry and Government

33. 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?
34. How could the new framework be designed to ensure that agencies and industry are able to work together in a more streamlined way?

Comments on Part 6:
Apart from 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 and legal demand. We have found that consistent communication is the best way to avoid misunderstandings and work through logistical, technical, and legal restrictions that impact providers' ability to respond to governments' legal process. We believe that it is appropriate for the Government to provide specific case studies prior to Parliamentary Joint Committee for Intelligence and Security processes. These case studies will enable more detailed evidence and consideration by technology companies through this important review mechanism.

Part 7: Interaction with existing and recent legislation and reviews

35. Do you have views on how the framework could best implement the recommendations of these reviews? In particular:
a. What data generated by 'Internet of Things' and other devices should or should not be retained by providers?

b. Are there additional records that agencies should be required to keep or matters that agencies should be required to report on in relation to data retention and to warrants obtained in relation to journalists or media organisations? How can any new reporting requirements be balanced against the need to ensure sensitive law enforcement or security investigations and capabilities are not compromised or revealed?

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

Comments on Part 7:

In general, we oppose mandates to retain data, and believe market factors and the need to provide desired services should be allowed to operate and guide providers' decisions. We do believe that special oversight and scrutiny may be appropriate for certain types of investigative targets, including but not limited to legal process obtained in relation to media organizations, politicians, religious groups, or other sensitive targets.

In keeping with principle 5 above, for example, we believe that governments should obtain data about enterprises, including commercial and public sector entities, from those entities, and not from their providers. With regards to public sector data, we believe it is never appropriate for governments to request each other's data, placing providers in the middle of state-on-state surveillance.