The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
PO Box 289
North Sydney NSW 2059
Australia
ABN 76 369 958 788

25 May 2020

Mr Andrew Hastie MP
Chair
Parliamentary Joint Committee on Intelligence and Security
Email: pjcis@aph.gov.au

Dear Mr Hastie

TELECOMMUNICATIONS LEGISLATION AMENDMENT (INTERNATIONAL PRODUCTION ORDERS) BILL 2020

The Australian Industry Group (Ai Group) welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) on its review into the effectiveness of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (IPO Bill).

In principle, we support the intent behind the IPO Bill which is to ultimately tackle national security threats and serious crimes effectively that require international cooperation. We have a mutual objective with Government to protect Australians from crime such as terrorism, to enforce law and to enable the intelligence, interception and enforcement agencies to effectively do so in a rapidly evolving digital environment. Indeed, Ai Group works closely with Government and its agencies on improving Australia's cybersecurity. Protecting the security of communications and information between businesses and their customers is of fundamental importance.

It is important that Australia leverages global activities and adopts, where possible, globally consistent approaches. Australian agencies will need to work more effectively in concert with key foreign jurisdictions and ensure global consistency of technologies that are developed to address threats. This can be enabled by establishing effective cooperation arrangements between Australian and overseas agencies to obtain improved and timely threat information, cooperation and assistance to more effectively fight crime and national security threats. For instance, we were pleased to see global issues like digital trade and cyber crime, with an emphasis on partnerships, included as priorities in the Federal Government's 2017 International Cyber Engagement Strategy and the role of the Australian Ambassador for Cyber Affairs under the Department of Foreign Affairs and Trade.

As Australia engages in international cooperation that requires cross-border access to data, it is also important that proper privacy and security safeguards are put in place to ensure trust between governments, businesses and their customers. Legislation that weakens this protective framework leads to public distrust – the impact of which should not be underestimated by legislators and policymakers.

This will require proper consultation including sufficient time to ensure that relevant stakeholders are consulted with and rigorous assessment is undertaken, especially in light of the current COVID-19 pandemic. We are also mindful of the risks of unintended consequences for businesses and the community arising from rushed legislative decisions with limited consultation, as seen with the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (TOLA Act).

At this stage, we would like to provide preliminary views. As further consultation is undertaken, there may be additional matters raised. We would also welcome the opportunity to work closely with the PJCIS as the review progresses.

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

1. Proper consultation

According to the Second Reading for the IPO Bill, the scope of the Bill will capture a broad and diverse range of businesses:[1]

> *Our Commonwealth, state and territory law enforcement agencies will be able to apply for an independently authorised order for communications interception, stored communications or telecommunications data to be served on a 'designated communications provider' in the other country by a coordinating Australian Designated Authority.*
>
> ...
>
> *Designated communication providers will include carriers and carriage service providers, as well as message application providers, voice and video call application providers, storage back-up providers, and other electronic content providers such as website providers, chat forums and social media platforms.*

Industry is increasingly characterised by the universal use of networked systems and the embedding of communications, digital and ICT in all processes and products. These include not just "communications businesses" and "IT businesses", but also a wide range of manufacturers and industrial solutions providers whose products and services are increasingly networked and digital. Many sectors have the capability of being a digital platform or business. Ubiquitous smartphones and connected devices in the workplace and at home mean the effects could be extensive. The IPO Bill is therefore relevant to a wide range of businesses.

Parliament should reflect on the development of the TOLA Act, which impacted on a very large number of businesses, civil liberties organisations, academia and other national and international stakeholders who voiced their concerns about the Act and continue to do so. In the lead up to Parliament passing the TOLA Act, Ai Group urged further consultation by Government to ensure that the potentially broad impacts of the legislation were tested by exposure to a cross-section of industry and the broader community. Ai Group was especially concerned that there was limited consultation within very short timeframes before the Act was passed, given the scope of companies that could be captured under this legislation was broader than may have been originally envisaged by Government.

Substantial amendments are still needed to the TOLA Act as soon as possible to clarify it and limit its impact in the areas of greatest risk.[2] These are to ensure that the Act does not weaken existing cybersecurity structures, that it balances security and privacy considerations and minimises unintended consequences, particularly the ability of Australian businesses to compete with international competitors not subject to the same degree of potential interference. Unintended consequences of the TOLA Act as it stands include damage to Australia's image overseas and to trust in Australian products.[3] In this regard, we welcome continued engagement with the PJCIS, the Department of Home Affairs, Independent National Security Legislation Monitor (INSLM), and other relevant stakeholders to help improve the Act.

Returning to the IPO Bill, the TOLA Act experience highlights the importance of proper consultation and we support the PJCIS's role in bringing this about. This is especially critical in light of the current COVID-19 pandemic, which may impact on the extent of stakeholder engagement.

---

[1] Commonwealth, Parliamentary Debates, Chamber, 5 March 2020 (Alan Tudge MP, Minister for Population, Cities and Urban Infrastructure).

[2] For further details, see: Joint submission by Communications Alliance, Ai Group, AIIA, AMTA, DIGI and ITPA to the PJCIS on "Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018" (Submission No. 23, July 2019), Link: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018/Submissions

[3] Australian Strategic Policy Institute, "Perceptions survey: Industry views on the economic implications of the Assistance and Access Bill 2018" (December 2018), p. 3.

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

2. Independent oversight

During the INSLM's review of the TOLA Act, we took a question on notice from its public hearing regarding a proposal to create a robust and independent oversight mechanism for the TOLA Act. Our joint response with some other industry associations to the INSLM would be equally applicable for the current PJCIS review of the IPO Bill.

The TOLA Act essentially seeks to replicate in the digital realm the existing powers of law enforcement agencies in the physical realm. However, in doing so, more intrusive powers may be created beyond the physical realm to accommodate a highly sophisticated and continually changing digital environment.

Such powers should be properly balanced with proportionate oversight mechanisms that offer robust and independent approval processes, and appropriate safeguards and constraints. It is important that such a mechanism is examined for its suitability in a broader national security context, including the IPO Bill.

The basis for the IPO Bill is part of Government's process to enable a bilateral Clarifying Lawful Overseas Use of Data (CLOUD) Act agreement with the United States:[4]

> *Given our agencies are making a significant and increasing number of requests to the United States, this bilateral agreement will provide our law enforcement and national security agencies with independent authorisation for efficient access to cross-border data.*

Having significant privacy protections and a commitment to the rule of law is a requirement in the design of CLOUD Act Executive Agreements. The US Department of Justice's White Paper about the CLOUD Act states the following (emphasis added in bold):[5]

> *The CLOUD Act requires that the agreements include numerous provisions protecting privacy and civil liberties. Orders requesting data must be lawfully obtained under the domestic system of the country seeking the data; must target specific individuals or accounts; must have a reasonable justification based on articulable and credible facts, particularity, legality, and severity; and* ***must be subject to review or oversight by an independent authority, such as a judge or magistrate.*** *Bulk data collection is not permitted. Foreign orders may not target U.S. persons or persons in the United States. Agreements may be used only to obtain information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism. They may not be used to infringe upon freedom of speech. The functioning of each agreement is subject to periodic joint review by the parties to ensure that it is being properly applied. To be clear, the Act does not require foreign partners to adhere to standards that perfectly match the U.S. legal system. However,* ***to be eligible, a country must establish appropriate standards and checks and balances within its legal framework to protect privacy, civil liberties, and human rights.*** *Agreements are reviewed by the U.S. Congress at inception and for renewal every five years thereafter.*

To be consistent with the requirements of the CLOUD Act Executive Agreements, issuance of International Production Orders should be subject to proper independent oversight. To avoid potential conflict and ensure consistency with the current TOLA Act review, consideration should be given to our proposal to the INSLM on essential features for proper independent oversight.

---

[4] Commonwealth, Parliamentary Debates, Chamber, 5 March 2020 (Alan Tudge MP, Minister for Population, Cities and Urban Infrastructure).
[5] US Department of Justice, "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act" (White Paper, April 2019), p. 5.

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

Recommended essential features for proper independent oversight include:[6]

- The person responsible for making an impartial judgment to issue an order should have the breadth of experience and independence that is likely to be required for this task e.g. a senior serving judge.

- We are unsure whether the current Administrative Appeals Tribunal (AAT) model would meet the above judicial requirement. If this cannot be achieved under the current model, consideration should be given to the creation of a new dedicated unit with access to a panel of judges. The UK's Investigatory Powers Commissioner Office (IPCO) may serve as an example. Notably, the INSLM found in its conversations in the UK and US that IPCO was critical to the UK obtaining a CLOUD Act agreement from the US, an agreement which Australia also seeks.[7]

- The decision by the assigned judge ought to create a "double lock" i.e. it ought to be preceded by ministerial approval of an order.

- The decision of the assigned judge to approve or disapprove an order should be binding on the requesting agency.

- In assessing orders, the assigned judge should seek advice from an independent technical expert. Such an expert would be selected by a technical expert panel, with the panel nominated by industry.

- Decisions would need to be done efficiently and expeditiously, enabled by access to a sufficient number of suitably qualified judges and technical experts.

3. Inconsistency with CLOUD Act on compliance requirements

According to the US Department of Justice's White Paper, the CLOUD Act does the following:[8]

> *First, the Act authorizes the United States to enter into executive agreements with other countries that meet certain criteria, such as respect for the rule of law, to address the conflict-of-law problem. For investigations of serious crime, CLOUD agreements can be used to remove restrictions under each country's laws so that CSPs [communications service providers] can comply with qualifying, lawful orders for electronic data issued by the other country.*
>
> *Second, the CLOUD Act makes explicit in U.S. law the long-established U.S. and international principle that a company subject to a country's jurisdiction can be required to produce data the company controls, regardless of where it is stored at any point in time. The CLOUD Act simply clarified existing U.S. law on this issue; it did not change the existing high standards under U.S. law that must be met before law enforcement agencies can require disclosure of electronic data.*

From preliminary member feedback, there may be an inconsistency between the IPO Bill and an intention for CLOUD Act Executive Agreements relating to compliance and compulsion. Part 8 of the Bill refers to a new compliance obligation with respect to International Production Orders. As explained in the Explanatory Memorandum to the Bill, this Part includes a provision (section 124) whereby a designated communications provider must comply with an International Production Order or attract a civil penalty.[9]

---

[6] These summarised features were proposed in our joint response with the Communications Alliance and ITPA to the INSLM. A copy of this response can be provided on request.
[7] INSLM, Opening Statement at TOLA Act Public Hearing (20 February 2020), p. 8.
[8] US Department of Justice, "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act" (White Paper, April 2019), p. 3.
[9] Explanatory Memorandum, Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (Cth), para [411].

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

In contrast, it is our understanding that CLOUD Act Executive Agreements do not create a new compliance obligation on the service provider. The intent of the Executive Agreements are to only remove potential conflicts of law. As stated in the US Department of Justice White Paper (emphasis added in bold):[10]

> ***CLOUD Act agreements, however, do not impose any new obligation on U.S.-based global CSPs to comply with a foreign government order****; nor does the fact of an agreement establish, by itself, that a foreign government has jurisdiction over that CSP. By the same token,* ***CLOUD Act agreements do not impose any new obligation on foreign CSPs to comply with a U.S. government order****; and the fact of an agreement, by itself, does not establish that the U.S. government has jurisdiction over a foreign company. In addition,* ***these agreements do not impose any obligation on either government to compel companies to comply with orders issued by the other. The only legal effect of a CLOUD agreement is to eliminate the legal conflict for qualifying orders****. Because the United States currently receives many more requests for electronic data than it submits to other countries, we expect the CLOUD Act will have a more dramatic (and beneficial) impact on foreign requests to the United States than on U.S. requests to foreign partners, at least for the foreseeable future.*

In addition to the above, we are uncertain if there are other aspects of the IPO Bill that are inconsistent with the CLOUD Act. We therefore recommend that the Bill should be rigorously reviewed to address any inconsistencies.

If you would like clarification about this submission, please do not hesitate to contact me or our Digital Capability and Policy Lead [redacted]

Yours sincerely,

[redacted]

Peter Burn
Head of Influence and Policy

[10] US Department of Justice, "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act" (White Paper, April 2019), pp 4-5.