# Microsoft submission to the Parliamentary Joint Committee on Intelligence and Security inquiry on the *Telecommunications Legislation Amendment (International Production Orders) Bill 2020*

## Introduction

Microsoft appreciates the opportunity to provide comments to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) as part of its inquiry into the *Telecommunications Legislation Amendment (International Production Orders) Bill 2020* (the IPO Bill).

Microsoft has long recognised that the traditional Mutual Legal Assistance Treaty (MLAT) processes for enabling governments' access to data held in foreign jurisdictions is no longer fit for purpose and hinder the ability of law enforcement to effectively investigate crimes and ensure public safety. This is a valid frustration shared by many nations, including Australia.

It is why Microsoft has advocated strongly since 2014[1] for a new set of international arrangements that allow for the sharing of information between countries with the appropriate legal rules and due processes that respect human rights and individual privacy. Microsoft welcomed the passage of the CLOUD Act by the US Congress in 2018 as an important milestone on this journey towards modernising the law and enabling enforcement officials to do their jobs, whilst protecting privacy rights across borders.

We therefore welcome Australia's negotiations with the United States to establish an agreement under the terms of the Cloud Act. However, as we outline below, Microsoft has concerns about how this agreement may be implemented through the IPO Bill.

## Microsoft's Principles for law enforcement access arrangements

As governments begin to reform global frameworks for digital evidence, Microsoft has highlighted six principles that we believe represent global standards that should govern cross-border law enforcement requests, such as those envisioned by the IPO Bill[2] and the international agreements it is designed to facilitate. These principles are intended to ensure that governments resolve conflicts of law and streamline legitimate law enforcement access to evidence while maintaining the underlying rule of law, accountability and transparency protections necessary to maintain trust in governments and technology.

We encourage the committee to review Microsoft's White Paper discussing these principles. In brief, they are:

1. **Notice.** Absent narrow circumstances, people have a right to know when the government accesses their data, and cloud providers must have a right to tell them. Secrecy should be the exception, not the rule.

[1] https://blogs.microsoft.com/on-the-issues/2014/01/20/time-for-an-international-convention-on-government-access-to-data/

[2] https://blogs.microsoft.com/on-the-issues/2018/09/11/a-call-for-principle-based-international-agreements-to-govern-law-enforcement-access-to-data/

2. **Prior independent judicial authorisation and required minimum showing.** All demands for content or other sensitive data should be pre-approved by an independent judicial or equivalent authority based on a required minimum showing. The standards that govern authorisation should be rigorous and set forth a clear legal and factual basis sufficient to protect privacy and prevent government overreach or abuse.
3. **Specific and complete legal process and clear grounds to challenge.** Government demands for data must contain sufficient detail to enable the identification of and challenge to inappropriate demands in court.[3] A process must exist so that service providers or data owners can challenge unlawful demands
4. **Mechanisms to resolve and raise conflicts with third-country law.** International agreements must contain mechanisms to resolve or raise potential conflicts directly with third-party countries when such conflicts arise. International agreements for cross border access to evidence should resolve conflicts, not create new ones.
5. **Modernising rules for seeking enterprise data.** Absent extraordinary circumstances, enterprises should have the right to control their data and receive investigatory demands directly from law enforcement. Unless an enterprise is permeated with criminal conduct, it is rarely necessary and proportionate to seek enterprise data from a cloud service provider instead of seeking the data from the enterprise directly.
6. **Transparency.** Cloud providers should have the right to publish transparency reports documenting the number of demands they receive, the number of customer accounts affected, and the government issuing these orders.

Based on our analysis of the IPO Bill against these principles, we have identified areas that we recommend the PJCIS should focus on through its inquiry. We will explore these issues further in our submission, but in summary these are:

- **Notice:** While ongoing investigations occasionally require secrecy to be effective, secrecy should be the exception not the rule. The proposed Bill imposes a blanket prohibition on service providers notifying their customers of an international production order ("IPO") targeting their data and does not require the government to *ever* notify the target of surveillance that their data has been examined. Absent such protections, citizens will *never* know if the government has sought and reviewed their communications or sensitive data. In the digital world, we believe the right to notice of surveillance is a universal human right that should be clearly protected by this legislation. A data owner's right and control over its data should not be fundamentally altered because it has chosen to move that data to a secure cloud rather than maintain it on premises. Such transparency increases trust in government and in law enforcement authorities, and avoids disincentivising cloud adoption, to the detriment of Australian digital transformation and competitiveness. Accordingly, we believe the Bill should require investigators make their case for secrecy to an independent authority and limit reasonably the duration of any secrecy orders that are granted.
- **Judicial authorisation and required minimum showing:** We share the concerns others have raised about the independence of the AAT. Additionally, the basis for issuing an IPO should provide more robust standards for authorisation that require a specific factual basis to support a

[3] Microsoft considers in particular that demands for access to data should explain that: (i) the demand has received prior independent judicial authorisation; (ii) the investigation that gave rise to the demand relates to a specified "serious crime" as defined in the relevant international agreement; and (iii) the demand does not further an investigation that infringes internationally-recognised human rights.

finding that the targeted account, identifier or device contains evidence of a serious crime such as terrorism.

- **Grounds to Challenge:** The Bill authorises service providers to object to an IPO only on the basis that it does not comply with the designated international agreement. Although the Explanatory Memorandum states that this right to object is in addition to any other review rights or remedies available under Australian law, this provision is not set out in the Bill itself. The Bill should explicitly provide a basis to challenge IPOs that are overbroad, abusive, violate the terms of an international agreement or are otherwise unlawful.
- **Mechanisms to Resolve and Raise Conflicts with Third-Country Laws:** The Bill provides no clear legal basis for service providers to challenge IPOs that would force them to violate the laws of a third country. Without such mechanisms, the IPO could lead to more conflicts of law and defeat the spirt and intent of intentional agreements envisioned by the Cloud Act.
- **Enterprise Data**: The Bill's definition of service provider would include those providing services to business and government enterprises. The Bill should either exclude the use of IPOs directed at service providers for enterprise data or include a requirement that investigators seek evidence directly from enterprises unless there is evidence that doing so would jeopardise the investigation.

## Detailed comments on alignment to Microsoft's principles

### Principle 1: Notice & Transparency

We believe that everyone has a fundamental right to know when they have been the target of a government investigation or surveillance request. We believe strongly that these fundamental rights should not disappear just because customers store their data in the cloud rather than in file cabinets or desk drawers. While we agree there are limited circumstances in which law enforcement must be able to operate in secret to prevent crime and terrorism and keep people safe, we also believe there should be limits to the scope and duration of secrecy requirements. This is why we have challenged the U.S. Government repeatedly over the past several years in an effort to advance this principle and we continue to believe that individuals and organisations have a right to know when governments access their digital information.[4]

We understand that alerting the target of a law enforcement demand may imperil an ongoing investigation or result in further danger to public safety – secrecy orders are appropriate in those limited circumstances. That said, international agreements, and the laws written to facilitate those agreements, must make clear that secrecy should be the exception, not the rule. When secrecy is required, we believe that investigators should be required to (1) make their case for secrecy to an independent authority; and (2) present case-specific facts to justify both why the government itself should not be obligated to notify the target and why the government must limit the cloud provider's

[4] https://blogs.microsoft.com/on-the-issues/2016/04/14/keeping-secrecy-exception-not-rule-issue-consumers-businesses/#sm.00001qg545hu8ldwmw7h8092g7f67

https://blogs.microsoft.com/on-the-issues/2019/09/25/ensuring-secrecy-orders-are-the-exception-not-the-rule-when-the-government-seeks-data-owned-by-our-customers/

https://blogs.microsoft.com/on-the-issues/2013/08/30/standing-together-for-greater-transparency/

right to notify its customers of the request. Any nondisclosure or secrecy order imposed on a cloud provider must be narrowly limited in duration and scope and must not constrain the provider's right to speak any more than is necessary to serve law enforcement's demonstrated need for secrecy. At its core, we believe that law enforcement's need for secrecy cannot be indefinite. Notice and government transparency when the government has reviewed a particular person's communications and sensitive data increases trust in government, in law enforcement, and in technology.

The IPO Bill as currently drafted does not provide for such protections. We also have concerns that the exceptions to clause 152 do not seem to readily cover disclosure between related bodies corporate in the same corporate group – such as between a Microsoft Australia employee (employed by Microsoft Pty Ltd) and an employee in the US (employed by Microsoft Corporation) who may then use that information pursuant to US law. This could unintentionally prevent a global company from communicating internally with its counsel and corporate leadership in relation to compliance with legitimate demands.

We recommend the PJCIS consider stronger protections in the Bill for the disclosure of IPOs to the target of the order, even if it was only after the investigation has concluded and the risk to the investigation has passed. This should include requirements that law enforcement authorities notify targets of surveillance after any risk to the investigation is over and rules that clearly permit service providers to notify their customers unless a time-limited non-disclosure order, supported by specific facts suggesting risk to the investigation, has been issued by an independent authority.

We also recommend adding a provision that would permit the Australian Designated Authority to notify any third country whose citizens may be impacted by an IPO order prior to execution unless this would present a risk to the investigation. Under the US-UK Cloud Act agreement, there is a requirement for the Designated Authorities to notify appropriate authorities in third countries, if the target of an order is located outside of the territory nor a national of the issuing party, *"except in cases where the Issuing Party considers that notification would be detrimental to operational or national security, impede the conduct of an investigation, or imperil human rights."*[5] This is an important provision for raising and addressing potential conflicts of law in a manner consistent with the spirt of international law enforcement cooperation. We recommend that the PJCIS should encourage a similar clause in the proposed US-Australia Cloud Act Agreement requiring the notification of third counties and allow for this notice in the IPO Bill.

Finally, we support the provisions in the Bill that permit providers to disclose "the total number" of IPOs served on the provider over a period of at least six months). This is consistent with Microsoft's support for greater transparency about government demands for customer data. However, in furtherance of greater transparency in the negotiation and implementation of international agreements we recommend the Australian government disclose any draft agreement prior to it being finalised by both parties. This will allow for meaningful public input on issues of important public interest

## Principle 2: Prior independent or judicial authorisation

While Microsoft would prefer that authorisation for IPOs reside only with an independent judicial

[5] Article 5, Clause 10, Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on access to electronic data for the purpose of countering serious crime

officer, we recognise that the AAT does perform a legitimately independent function within the Australian system. To add confidence in the process, we suggest that the PJCIS seek confirmation that only members of the Security division of the AAT can authorise IPOs and that the PJCIS recommends additional requirements for the membership of the Security division that are empowered to authorise IPOs, to ensure that members have the requisite legal, technical, and privacy experience when considering the government's investigatory powers. We also recommend more rigorous standards for approval of IPOs.

## Principle 3: Grounds to Challenge

Cloud providers act as a critical check to ensure that governments' use of their investigative powers strictly adhere to the rule of law. When law enforcement seeks access to customer data, cloud providers' thorough review of law enforcement demands serve to ensure that governments are respecting the rights of internet users around the world. We recommend the grounds for challenging an IPO should explicitly include situations in which an IPO is overbroad, abusive, or otherwise unlawful in addition to potential violations of the relevant international agreement. While it may be the rare instance in which law enforcement orders generate such concerns, cloud providers may only identify concerns after a request has been made and should have a clear path to raise such concerns with a court.

## Principle 4: Mechanisms to resolve and raise conflicts with third-country law.

Government-to-government dialogue and international agreements are the only legitimate mechanisms to facilitate cross-border demands for electronic evidence in a manner that respects international borders and sovereignty. An international agreement between two countries, however, may not resolve all conflicts that might arise with a specific law enforcement demand, particularly when the demand implicates a third country's citizens or laws. Consequently, international agreements and the laws that implement the agreements must contain mechanisms to resolve or raise potential conflicts when they arise.

The Bill currently contains no express provision for a provider to raise a potential conflict of law. While the principle of international comity is well-established in Australian case law, we recommend that the IPO Bill explicitly cites comity as a consideration and a defence for non-compliance.

## Principle 5: Modernising Rules for Seeking Enterprise Data

Public and private organisations – and even governments themselves, including the Australian Government – are increasingly moving their digital information to the cloud. Transition to cloud-based infrastructure, however, should not change the basic principle that these enterprises have a right to control their data and receive investigatory demands directly from law enforcement.

Absent extraordinary circumstances, seeking data directly from enterprises will not compromise a law enforcement investigation or result in a danger to public safety. This is especially true when the legal demand implicates large organisations, which likely have an interest in cooperating with law enforcement. Microsoft's experience as reflected in our transparency reporting shows that law enforcement demands for enterprise data are relatively infrequent. This is because law enforcement in Australia and elsewhere around the globe recognise that approaching an enterprise customer and controller of the data directly is more efficient and proportionate to their investigative needs. In fact, the U.S. Department of Justice recognised these best practices in 2017 when they issued recommended practices for "Seeking Enterprise Customer Data Held by Cloud Service

Providers." We believe that Australia should formalise this approach by either excluding enterprise data from the scope of the IPO Bill or by incorporating binding limitations into the IPO Bill that codify these existing best practices as outlined below.

In Australia, this distinction between a cloud service provider and its enterprise customer was recognised in the drafting of the Explanatory Memorandum for the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 on how the term "proportionate" should be interpreted under that Act; and that it may not be "proportionate" to give a notice to a provider:

> *"who, while able to assist, did not control the relevant data and was not in a position to help as adequately as a more directly related provider. In that instance it would need to be clear that the controller of the data was unable to assist."*[6]

At this stage the IPO Bill does not have similar guidance nor does it acknowledge the commercial relationship that exists between a designated communications provider such as a cloud service provider and an enterprise or government customer, where the cloud service provider does not control their end user's data. However, Australian law has long recognised that there is a clear distinction between public networks and private networks for communicating within an enterprise, under the Telecommunications Act's definition of "immediate circle".

"Immediate circle" includes a person and their employees and a corporate group (a parent corporation and its subsidiaries or controlled entities). This definition in law was a recognition that many private networks may have the technical characteristics of a carriage service but should not be regulated as such.

Microsoft recommends that these existing statutory concepts from the Telecommunications Act could be extended to exclude an enterprise customer's internal data from the data which a designated communications provider has to provide under an IPO. The focus of the designated communications provider's obligations would then be on use of services for messaging outside the customer's closed user group.

This would involve introducing a new restriction on the making of an IPO in relation to the following:

a) a carriage service used for the carriage of communications between two end-users each of whom is outside the immediate circle of the customer to whom the designated communications provider supplies the carriage service;
b) a message application service to the extent the service is used by end-users to send or receive messages to or from other end-users, where all of those end-users are within the immediate circle of the customer to whom the designated communications provider supplies the message application service;
c) a storage/back-up service, to the extent it is used to store or back-up material by end users who are within the immediate circle of the customer to whom the designated communications provider supplies the storage/back-up service; and
d) a general electronic content service, where the relevant material can only be accessed by or delivered to persons by means of that service who are within the immediate circle of the customer to whom the designated communications provider supplies the general electronic content service

---

[6] Page 68, Revised Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

Alternatively, rather than an absolute carve-out, there could be a requirement that the judicial officer not make an IPO unless satisfied that the requesting agency could not feasibly obtain the information directly from the customer of the designated communications provider.

Clause 30(6) of the Bill includes a restriction along these lines in relation to an interception order, but there is not a similar clause restricting the making of an IPO for stored communications or telecommunications data. On this approach, Microsoft recommends a new category of 'internal customer communications' could be created and the authorising officer could be required, before making an IPO covering 'internal customer communications', to be satisfied that:

a) the criminal law enforcement agency exhausted all other practicable methods of identifying the internal customer communications used, or likely to be used, by the person involved in the offence being investigated; and
b) obtaining the internal customer communications used or likely to be used by that person would not otherwise be possible without risk of compromise to the integrity of the investigation.

We appreciate this opportunity to comment on the review of the IPO Bill and look forward to continuing engagement on these important matters of public safety.