Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/about/contacts

The Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

1 April 2020

Submission: Telecommunications Legislation Amendment (International Production Orders) Bill

The attached submission by the Australian Privacy Foundation responds to the Committee's inquiry regarding the *Telecommunications Legislation Amendment (International Production Orders) Bill 2020* (Cth)

Summary

The Bill is deeply flawed. It conflates bureaucratic convenience with what is imperative. It obfuscates accountability through inadequate transparency, including reliance on the under-resourced Commonwealth Ombudsman. It enshrines an inappropriate level of discretion and weakens parliamentary oversight regarding interaction with governments that disrespect human rights. It is a manifestation of a drip by drip erosion of privacy protection in the absence of a justiciable constitutionally-enshrined right to privacy in accord with international human rights frameworks.

The Bill is at odds with the self-interested claim by the Minister for Home Affairs that "There will be no trade-off of Australia's existing privacy and civil liberty protections to achieve this most welcome boost to our agencies' ability to keep Australians safe". The existing protections are inadequate and are weakened by the proposed legislation.

The Foundation, along with other civil society bodies, expresses concern regarding the short time frame for public consideration of a major legislative proposal, particularly during the COVID 19 pandemic.

The Bill should be reconsidered.

Dr Bruce Baer Arnold
Vice-Chair
Australian Privacy Foundation

David Vaile
Vice-Chair
Australian Privacy Foundation

Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (Cth)

This submission covers –

1. Background – The Foundation
2. Inadequate Community Consultation
3. Absence of demonstrated need
4. A framework for future abuse
5. Disregarding proportionality
6. Public Interest Monitors
7. Reliance on AAT
8. Destruction
9. Concerns re 'Likeminded Governments'
10. Objections by providers
11. Inadequate Accountability
12. Inadequate Supervision

1: Background - The Foundation

The Australian Privacy Foundation is the nation's premier civil society body concerned with privacy.

The Foundation is politically independent. It is not beholden to any funder or partner. Its membership encompasses legal practitioners, engineers, health specialists, academics, business analysts and others. It has been active over several decades in substantive contributions to public policy development at the Commonwealth, state and territory levels.

Information about the Foundation is attached and is available on its website – www.privacy.org.au – along with copies of its submissions to a range of law reform bodies.

2: Concerns regarding community consultation

The Inquiry is the latest instance of consultation that resembles a potemkin village. Civil society has a short opportunity to comment on a detailed and technically challenging proposal in the absence of a clear justification for changes that progressively erode privacy protection.

As noted in the covering letter for this submission it is **not** the case that "There will be no trade-off of Australia's existing privacy and civil liberty protections to achieve this most welcome boost to our agencies' ability to keep Australians safe". The Foundation rejects that self-serving claim by the Minister for Home Affairs. Existing privacy legislation and practice (for example supervision by the under-resourced and inward-looking Office of the Australian Information Commissioner) is inadequate. A benchmark for that inadequacy is provided by Europe.

Contrary to the Minister's claim – and his reference to "robust privacy and civil liberty protections" – the proposed legislation will erode privacy and civil liberty protections. The Government has not provided a compelling case for adoption of the Bill. The Government also has not provided a persuasive reason for why passage of the Bill is imperative.

Notional consultation about a succession of enactments that reshape Australian civil liberties fosters distrust and deprives policymakers of the guidance that averts the need to spend public money fixing ill-conceived and poorly-administered projects such as MyHealth Record. Genuine consultation is

especially important at a time where people are rightly sceptical after observing the SportsRorts scandal, CensusFail and RoboDebt.

The short period for consultation is particularly egregious given 'hibernation' of Parliament House during the COVID 19 pandemic and the disruption to businesses and other organisations as a result of that pandemic. There appears to be no national security need that makes enactment of the Bill imperative when Parliament sits again to deal with the COVID pandemic. Ministerial self-aggrandisement, bureaucratic convenience and inadequate accountability should never be confused with what is necessary or just.

The Foundation considers that the Government *can* build legitimacy through meaningful consultation with civil society. Such consultation involves –

- substantive provision of information as the basis of informed public discussion, something absent from both the Bill, the 2nd Reading Speech and the Explanatory Memorandum
- timely provision of information about legislative proposals, especially where the proposed legislation is complex and where there is amendment of existing complex enactments
- greater assurance that meaningful supervision of law enforcement or other agencies will be established. Ongoing under-funding of the Commonwealth Ombudsman, presented in the Bill as the key supervisory agency, does not result in confidence.

3: Absence of demonstrated need

Given the preceding comments a core concern for civil society is the absence of any substantive information justifying the need for amendment to the *Telecommunications (Interception and Access) Act 1979* (Cth).

As in the past, civil society is presented with vague and unsubstantiated statements such the reference to a "lengthy process, which cannot keep pace with the fast moving requirements of the investigation and prosecution of serious crime". There has been no meaningful consultation with civil society regarding negotiations with the United States regarding that nation's *Clarifying the Lawful Overseas Use of Data Act* (aka the CLOUD Act). The Foundation notes a succession of studies warning of danger to Australian interests by entering into bilateral/multilateral agreements without sufficient consideration of needs and long-term impacts. Genuine community consultation over a period of more than a month is a basis for that sufficient consultation. Such consultation is entirely consistent with effective and legitimate law enforcement.

There has been no demonstration that existing processes are tangibly affecting law enforcement, ie investigation and prosecution, or precluding conviction of offenders. Civil society is instead simply told that yet another set of changes to privacy law is needed. Legal practitioners might be forgiven for thinking that the problem is one of inefficiency on the part of government agencies rather than a true need.

That scepticism is entirely understandable when observers recall instances where officials and ministers have recurrently provided assurances about a commitment to best practice or that all will be well, something demonstrably not the case when we remember RoboDebt, CensusFail, damning Australian National Audit Office reports on a range of large-scale information technology initiatives, problems with design/implementation of the MyHealth Record program amid denials by ADHA and last week's Centrelink failures.

It is incumbent on the Government to do more than say 'we need it' and for the Minister for Home Affairs (like a character in *Lord of the Rings*) to say "I wants it". If the Government provides substantive information that consultation will foster trust in both the proposed legislation and government policy development processes.

4. A framework for future abuse

The proposed legislation offers a framework for future abuse. It emphasises ministerial discretion and the discretion of other decisionmakers, with insufficient regard for proportionality (discussed below) and a grossly inadequate mechanism for oversight.

The Explanatory Memorandum indicates that the legislation will be given effect through bilateral and multilateral "like-minded foreign governments". (The Foundation notes reference by the Minister for Home Affairs to "The Bill's new framework" [sic] as "an essential precondition for Australia obtaining a proposed bilateral agreement with the United States" to implement that nation's CLOUD Act. Given references to terrorism and other crimes, and the tenor of Government statements about matters such as AML/CTF, civil society might legitimately wonder about Australia's relationship with like-minded governments – such as that of Saudi Arabia – that have been distinguished by a systemic disregard of human rights while providing assurances of trustworthiness.

The legislation will for example allow sharing of data with states such as the People's Republic of China (noted for its persecution of minorities such as the Uighurs and its current confinement without due process of several Australian citizens). Such sharing is unlikely to be rejected by a political appointee to the Administrative Appeals Tribunal and effectively oversighted by the Commonwealth Ombudsman (discussed below).

It is important to remember that the Bill seeks to enable "the exemption from Commonwealth laws restricting interception or disclosure" on the basis of a designated international agreement: a low threshold at odds with the Minister's reference to "robust privacy and civil liberty protections".

That threshold should be contextualised through reference to ongoing 'privacy creep' (ie drip by drip year by year erosion of privacy protection) and the regulatory incapacity of watchdogs such as the Commonwealth Ombudsman and Office of the Australian Information Commissioner.

5. Disregard of proportionality

The proposed legislation disregards concerns regarding proportionality in favour of bureaucratic convenience. It enshrines an undue degree of discretion by decision-makers, privileging form over substance.

The Foundation notes the statement in the Explanatory Memorandum that –

> In deciding whether to issue an IPO relating to interception, the decision maker must have regard to several matters including relevantly, how much the privacy of any person or persons would be likely to be interfered with. The decision maker must also take into account the availability and use of other means to achieve the objectives of the IPO, including how much the use of such methods would assist with or be likely to prejudice the investigation (e.g. by delay).

That regard might be cursory, particularly given that requests will typically (if not invariably) be directed to the Administrative Appeals Tribunal Security Panel and that requests will be granted immediately. (The immediacy is a stated justification for the Bill.)

The Foundation further notes the statement that

> This means that where there are other methods to access the necessary information that would be less intrusive on the privacy of the person, the relevant agency *may* be required to turn to those means instead of seeking an IPO for interception activities.

If there are other "less intrusive" methods those methods should be the default position, rather than simply considered and then rejected because they are inconvenient.

We have noted the lack of information regarding 'timeliness' or 'delay'. The supposed difficulty of obtaining authorisation is a traditional and hollow claim used by law enforcement agencies that seek a freedom from gaining a warrant from a judge. That claim confuses bureaucratic convenience with necessity. It disregards both the ease of obtaining authorisation and the importance of independent scrutiny by a judge, in other words by an entity that is independent of the Executive.

On that basis the Foundation is unpersuaded by the Explanatory Memorandum's explanation that the "less intrusive method" under consideration by the nominated AAT Security Division member will be "weighed against its effectiveness and potential to prejudice the Organisation in carrying out its functions (e.g. by delay)". Enshrining the "least intrusive method" offsets the likely permissiveness of the Ministerial Guidelines.

6. Public Interest Monitors

The Bill offers a token reference to two non-Commonwealth Public Interest Monitors. The Foundation characterises that reference as token because an effective a coherent national Public Interest Monitor regime is essential. As things stand there will be very uncertain monitoring in most state police forces and other entities, several of which have a history of institutional misbehaviour, disregard of the law and disregard of accountability (for example the 'Lawyer X' controversy in Victoria).

The Foundation notes the salience of truly independent, appropriately resourced and vigorous Monitors in all Australian jurisdictions. The activity of those entities is a foundation for the accountability and thereby trust in law enforcement that differentiates Australia from autocratic regimes where neither governments nor police/national security agencies have broad community support.

7. Reliance on the AAT

The Bill seeks to enshrine authorisation by a member of the Administrative Appeals Tribunal rather than by a court. Reliance on the AAT is inappropriate and of deep concern, particularly given community perceptions that the Tribunal is being influenced through appointments that reflect political affiliation. It is symptomatic of ongoing weakening of privacy protection.

The Explanatory Memorandum indicates that authorisation by the AAT will be the default position rather than the exception. It thus states –

> [18] Prior to the Organisation applying for an IPO, the consent of the Attorney-General must be obtained in writing, except in urgent circumstances where it may be obtained verbally. Once the Attorney-General's consent is obtained, the Organisation may then apply to a nominated AAT Security Division member for an IPO.
>
> 19. The nominated AAT Security Division member may only issue an IPO relating to interception where they are satisfied on reasonable grounds a particular person is using or is likely to use the communications service, and the extent to which information gathered under the order would be likely to assist the Organisation in carrying out its functions in relation to security.

We note the range of authorisations able to seek authorisation. We note the absence of information about any instances in which the Minister has refused consent. Given preceding comments we consider that authorisation should be granted by a judge in the first instance, rather than by a Tribunal Member, given the judiciary's independence of the Executive. Courts provide both an appearance of scrutiny and some substance.

As noted below, the Government has provided no indication that authorisation by judges is likely to result in delays or has historically been so delayed as to prevent effective law enforcement. If the perceived problem is the judiciary's workload that can be addressed through greater support for federal judges, a legitimate cost for public administration.

If the AAT is to be the default decisionmaker the Government should move to address community concerns regarding politicisation of that body through establishment of an independent commission responsible for judicial and tribunal appointments.

8. Destruction

The Bill deals with the destruction of records as part of the proposed Orders regime. The Foundation notes that the provisions enshrine an inappropriate level of subjectivity and that discretion means there is likely to be variations across the Australian jurisdictions.

The absence of information to the Australian community means that it will be impossible for observers outside the law enforcement space to discern the effectiveness of the provisions and whether there has been any malpractice.

9. Concerns re 'Likeminded Foreign Governments'

The Foundation notes the expectation of reciprocity in sharing data with governments of other countries under the proposed legislation and more broadly under bilaterals to give effect to for example the US CLOUD Act noted above.

The Bill's recognition of Australia's opposition to capital punishment is commendable. The Foundation however notes that several nations retain the death penalty, which is likely to be a feature of their legal regimes in future. Those nations include Japan, Saudi Arabia, the Peoples Republic of China and the United States. The Australian Parliament has recurrently expressed concerns regarding the justice systems in several nations, including arbitrary detention of Australian citizens in China and disregard by that nation's government of the human rights of minorities such as the Uighurs. There has been international attention to human rights abuses in Saudi Arabia and condemnation of the murder in the Saudi consulate of human rights activist Jamal Khashoggi.

The Foundation accordingly expresses its wariness about the efficacy of a "written assurance" by foreign governments to the Minister. Overseas and domestic political expedience means that such an assurance is an inadequate guarantee against Australia facilitating human rights abuses through sharing with states where abuses are a daily fact of life.

Given that law enforcement in other states is often not transparent the Foundation considers that the Australian government is unlikely to be able to verify compliance with what the Explanatory Memorandum characterises as "restrictions or conditions" that are "flexible as to the form, content and nature". Australia will, presumably, trust our "likeminded" foreign friends in the same way as the unfortunate Mr Khashoggi.

Importantly, given that the specifics of sharing will not be publicly available (and are likely to be inadequately supervised by the Commonwealth Ombudsman or other watchdogs, discussed below) the Australian community will not be able to determine whether the assurance is being subverted by the foreign government or the Minister.

10. Objections by providers

The Foundation notes the provision in clause 121 for objections by communication providers.

The efficacy of the objections arrangement is at best uncertain. The reporting arrangements must encompass information about the incidence, nature and outcomes of any objections.

11. Inadequate Remedy

The Foundation reiterates its call for a constitutionally-enshrined justiciable Bill of Rights, ie privacy protection that recognises the salience of privacy as a right under the international human rights framework (to which Australia has been formally committed since the 1940s) and that provides

people with an effective remedy where there is potential/actual serious invasions of privacy. The relevance and feasibility of the so-called privacy tort has been highlighted in a succession of law reform and parliamentary committee reports. It is consistent with law enforcement and the implied freedom of political communication.

The proposed legislation does not provide an effective remedy where there has been an abuse of privacy by law enforcement and other agencies or third parties. The Explanatory Memorandum refers to Australian courts retain jurisdiction for judicial review, ostensibly ensuring "that an affected person or a provider has an avenue to challenge unlawful decision making". Importantly, however, Orders are intended to be used without the knowledge of the person of interest. In practice a decision to issue an Order might only be challenged retrospectively, on the basis that the evidence was improperly or illegally obtained.

That is weak protection, particularly when contextualised with the inadequate supervision regime provided in the proposed legislation.

12. Inadequate Supervision, Ineffective Accountability

The Foundation expresses its strong concern regarding supervision by the Commonwealth Ombudsman under clauses 139 through 143, given the Government's ongoing reluctance to adequately resource the Ombudsman. As with the Office of the Australian Information Commissioner we note a fundamental problem with bureaucratic incapacity. Watchdogs need sufficient staff (especially staff with expertise) alongside a culture that enshrines proactive action and a willingness to speak out in the public interest.

On that basis we question claims that

> Oversight by the Commonwealth Ombudsman will also provide for an effective mechanism to ensure agency use of the powers in the Bill is compliant with the terms of the legislation, thereby bolstering the proper use of framework.

The Foundation recognises that the Inspector-General of Intelligence and Security (IGIS) will automatically have oversight under its existing legislation but notes criticisms by IGIS about government unresponsiveness and concerns regarding resourcing. We suggest that the proposed legislation will gain greater legitimacy if the Ombudsman reports direct to Parliament – a basic measure of accountability – rather than to the Minister, who is obliged to table a report in Parliament.

In considering that report we note the formulaic provision of statistics that are not contextualised and that take the form of activity counts. An evaluation of the proposed regime needs more that data about how many applications were made, withdrawn and refused. The Bill does not require designated communications providers to disclose the total number of IPOs given by Attorney-General's and only permits the disclosure of aggregate statistical information that cannot be broken down by agency that obtained the order or in any other way, for example by the type of order or type of data requested. It provides insufficient transparency and the Committee should adopt a robust approach in considering claims about

> highly sensitive information pertaining to law enforcement and national security investigations that could prejudice investigations or otherwise compromise law enforcement and national security outcomes.

The Australian public has a legitimate need to know the incidence of cooperation with foreign governments and other matters that do not provide specifics of investigations and thereby do not compromise law enforcement.

The potential embarrassment of Australian and foreign governments, as noted in a succession of judgments such as *Commonwealth v Fairfax* (1980) 147 CLR 39 and *RJCG v Director-General of Security* [2013] FCA 269, is not a justification for restriction of information. As Mason J stated in *Commonwealth v Fairfax*

It is unacceptable in our democratic society that there should be a restraint on the publication of information relating to government when the only vice of that information is that it enables the public to discuss, review and criticize government action.

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, SubCommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, Committees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby and Elizabeth Evatt, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies http://www.privacy.org.au/Papers/
- Resources http://www.privacy.org.au/Resources/
- Media http://www.privacy.org.au/Media/
- Current Board Members http://www.privacy.org.au/About/Contacts.html

- Patron and Advisory Panel http://www.privacy.org.au/About/AdvisoryPanel.html

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87) http://www.privacy.org.au/About/Formation.html
- Credit Reporting (1988-90) http://www.privacy.org.au/Campaigns/CreditRpting/
- The Access Card (2006-07) http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
- The Media (2007-) http://www.privacy.org.au/Campaigns/Media/