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

30 April 2020

Dear Committee Secretary,

RE: Telecommunications Legislation Amendment (International Production Orders) Bill 2020

The Australian National University Law Reform and Social Justice Research Hub ('ANU LRSJ Research Hub') welcomes the opportunity to provide this submission to the Parliamentary Joint Committee on Intelligence & Security (PJCIS) concerning the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (the Bill).

The ANU LRSJ Research Hub falls within the ANU College of Law's Law Reform and Social Justice program, which supports the integration of law reform and principles of social justice into teaching, research and study across the College. Members of the group are students of the ANU College of Law.

The opinions expressed in the submission reflect those of the authors, and do not necessarily reflect the views of their employers or the institutional views of the ANU.

Summary of Recommendations:

1. The dominant concern that underpins surveillance laws is the need to balance privacy and security concerns. While the international production orders scheme is appropriate, care must be taken in individual matters on a case-by-case basis.
2. Similar privacy protections to those in the Bill relating to control order International Production Orders (IPOs) should be extended to criminal investigatory and security IPOs.
3. Appropriate time is taken in the decision-making process and care is taken to ensure that it does not become a "rubber stamp" process.
4. The agencies able to apply for IPOs are specifically listed in a statutory provision within the IPO scheme divisions. The list should not allow for the addition to agencies by ministerial direction and should require PJCIS consultation prior to any amendment.
5. More funding is provided to the Commonwealth Ombudsman to allow them to perform the review function required under the IPO regime contained in the Bill.
6. The time frame allowed for notification of the Ombudsman be adjusted from 'within 3 months' to 'within 1 month'.
7. PJCIS to consider whether the creation of a federal Public Interest Monitor system to oversee the IPO framework (and other interception and access powers under the *TIA* Act) is appropriate.

8. Entry into a designated international agreement is carefully scrutinised by the PJCIS and OAIC. Appropriate time should be taken in these reviews to allow for open public consultation.

If further information is required, please contact us at anulrsjresearchhub@gmail.com.

On behalf of the ANU LRSJ Research Hub,
Authors: Andrew Ray, Bridie Adams and Kate Renehan
Editors: Jessica Hodgson and Thulasie Venkat
Under the supervision of: Dr. Damian Clifford, ANU College of Law

Introduction

This submission focuses on assessing whether the Bill[1] and the wider surveillance regime under the *Telecommunications (Interception and Access) Act 1979* (Cth) ('the *TIA Act*') appropriately balances the competing objectives of privacy and security. It also assesses whether the Bill accords with the level of transparency and accountability required by the principles of responsible and representative government in Australia.

1. Balancing Privacy and Security

Security measures, and particularly the domestic surveillance powers held by intelligence agencies, have increased markedly in many parts of the world since the September 11 attacks in the United States.[2] In Australia, powers of law enforcement agencies have increased through the passage of laws, granting:

- Access to metadata, that must be held by telecommunications providers for two years;
- Extended warrant schemes under the *TIA Act* and the *Crimes Act* allowing for greater access to information stored digitally (see especially s 3F *Crimes Act*);[3] and
- Greater powers to compel assistance from technology companies (in regard to accessing information) through the use of TARs, TANs and TCNs under the *TIA Act,* following amendments made at the end of 2018.

These laws have often been passed rapidly, with a lack of debate justified by the need of agencies to appropriately protect Australia from domestic and international threats. This lack of debate can

[1] Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (Cth) ('the Bill').
[2] See, eg, *Report of the Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age*, UNHRC, 27th session, UN Doc A/HRC/27/37 (30 June 2014).
[3] See our recommendation that Part IAA of the *Crimes Act* should be amended so that warrants issued under the *Crimes Act* against journalists or related parties include the protections contained in s 180T of the *TIA Act*: ANU Law Reform and Social Justice Research Hub, Submission No 38 to Senate Standing Committees on Environment and Communications, *Press Freedom Inquiry* (September 2019) 1–5.

lead to laws without proportionate safeguards being adopted resulting in implementations that go far beyond the scope of the original intention of Parliament – protecting Australia from serious threats. For example, metadata retention laws passed under the guise of combatting domestic terrorism and serious crime have been used by local councils to help enforce parking fines and catch individuals accused of littering.[4] Similarly, there is currently no limit on the length of time telecommunications companies can store metadata as there is no requirement for them to delete the data after the two-year retention period. Finally, the ability for the Minister to declare an organisation a law enforcement agency for the purposes of the metadata retention scheme is concerning, as it affords significant powers that harm individual privacy to ministerial discretion. In combination, these uses go beyond the original intention of the laws and highlight the existing limitations in the drafting and review process. It is also important to note that the laws were not amended following these unintended uses of surveillance powers.

Of further concern is the fact that privacy and security are often placed in a false dichotomy: that to ensure greater security, we *must* sacrifice our privacy and that catching a terrorist, therefore justifies extensive invasions of privacy. For example, following the 2017 London Bridge Attack, then Prime Minister Turnbull stated that '[t]he privacy of a terrorist can never be more important than public safety'.[5] These statements afford significant deference to security and fail to consider the harm to individual privacy through the use of these powers. For example, executing a warrant that allows an officer to search the phone and computer of a suspect exposes the private information of everyone who has contacted that individual. Although such encroachments on the private sphere of such individuals may be deemed necessary and proportionate to prevent a terror attack, without adequate procedural controls and through for instance mass surveillance techniques/technologies, every citizen is a potential suspect. This speaks against the "nothing to hide, nothing to fear" argument commonly used to justify such measures, instead, as outlined above, the burden should be on enforcement agencies to justify why requested powers are proportionate and necessary.

While using domestic surveillance measures to prevent serious crime, including domestic terrorism, is an appropriate objective, the same powers should not be available in all circumstances: for example, to local councils. Consequently, it is imperative for lawmakers to employ a framework on a case-by-case basis to ascertain when it is appropriate for such laws to be imposed. However, precisely which framework should be used to ensure that surveillance laws are appropriately balanced remains a vexed question.

We submit that while undoubtedly, security and the government's right to protect Australia is critical, so too is an individual's right to privacy. It is therefore essential that proposed laws balance these competing objectives in a manner *proportionate* to the threat or harm that they aim to prevent. The use of proportionality to assess proposed laws and decisions made under those laws is one that we feel appropriately balances the privacy of individuals and Australia's security.

[4] Harriet Alexander, 'Councils pry into residents' metadata to chase down fines', *The Sydney Morning Herald* (online, 15 November 2018) <https://www.smh.com.au/business/consumer-affairs/councils-pry-into-residents-metadata-to-chase-down-fines-20181114-p50fxr.html>.
[5] Commonwealth, Parliamentary Debates, House of Representatives, 13 June 2017, 6171 (Malcolm Turnbull).

1.1 Balancing Privacy and Security utilising a framework of proportionality

The Bill aims to permit law enforcement agencies and national security agencies to access stored communications, interception information and telecommunications data held by overseas organisations through the use of international production orders (IPOs). The Bill allows for requests on three grounds: security, law enforcement or enforcement of control orders. The need to access data stored overseas is clear and justified given the interconnected, global nature of communications today and especially noting the volume of data stored in the United States. However, we need to ask whether, in doing so, the Bill appropriately balances these access powers against an individual's right to privacy. Acknowledging that each case will be different, this is best assessed on a case-by-case basis. The Bill aims to do this through requiring a decision-maker (judge or nominated AAT member) to consider a range of factors when deciding to grant an IPO, including privacy, the likely value of the information and the security benefit of granting the order.[6] However, the Bill affords greater privacy protections in cases concerning IPOs granted in relation to a control order – justified on the basis that:

> [An] IPO [granted in relation to a control order] can be issued for purposes in connection with the monitoring of a person subject to a control order rather than in connection with an investigation into a specific serious offence … [7]

This greater protection requires a decision-maker to consider (in addition to the impact of granting the IPO on the privacy of any person) whether '[the interception or access of the communications] under an international production order … would be the method that is likely to have the least interference with any person's privacy'.[8]

The Bill does not justify why such protection is not available in *all* cases. If the information required by the agency in any IPO matter can be gathered in a less intrusive manner, that should be the preferred option. This should apply regardless of whether the IPO is sought in regard to a control order, criminal investigation or security matter. This is particularly the case in a criminal investigation, which is likely to take place *after* the harm has occurred.

Similarly, the use of nominated AAT members is of concern if their role is more a formality rather than substantive. The Explanatory Memorandum notes that AAT members are used so that the decision-making process can happen quickly and efficiently. Other submissions have raised concerns that this may suggest the process is a "rubber stamp" rather than members taking the careful consideration needed to balance the competing considerations raised above.

Noting the scope of "surveillance creep" in relation to the metadata retention laws, and that under the *TIA Act* the Minister can declare bodies to be enforcement agencies, we recommend that the IPO regime be restricted to a specified list of bodies and agencies included within the IPO provisions. This would require a legislative amendment to increase the bodies that have access to the IPO regime. We also recommend that any change to this list require consultation of the

[6] See, eg, the Bill (n 1) amendments to the *TIA Act* sch 1 s 60(5).
[7] Explanatory Memorandum, Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (Cth) [17].
[8] The Bill (n 1) amendments to the *TIA Act* sch 1 s 60(5)(f).

PJCIS in line with similar provisions in the *TIA Act*. This would increase the oversight of bodies able to access international data, but still allow agencies access to the IPO scheme. We believe this would appropriately balance the security needs while preventing unintended access to the IPO regime.

Given the importance of individual decision-makers, and the secrecy of the orders from the data subject, appropriate transparency and accountability measures must be in place to ensure that decision-makers are using their powers appropriately. This is addressed in detail below.

Recommendation 1: The dominant concern that underpins surveillance laws is the need to balance privacy and security concerns. While the international production orders scheme is appropriate, care must be taken in individual matters on a case-by-case basis.

Recommendation 2: Similar privacy protections to those in the Bill relating to control order IPOs should be extended to criminal investigatory and security IPOs.

Recommendation 3: Appropriate time is taken in the decision-making process and care is taken to ensure that it does not become a "rubber stamp" process.

Recommendation 4: The agencies able to apply for IPOs are specifically listed in a statutory provision within the IPO scheme divisions. The list should not allow for the addition to agencies by ministerial direction and should require PJCIS consultation prior to any amendment.

2. Transparency and Accountability Mechanisms

Transparency and accountability are key in ensuring that powers granted under the *TIA Act* are used appropriately. Transparency and accountability are cornerstones of Australia's democratic system and ensure that executive decision-makers are held to account. The importance of these objectives is heightened due to the discretion given to decision-makers, and the importance of their decisions in ensuring the IPO regime appropriately balances privacy and security interests in individual cases. The Bill accounts for this by providing for the Commonwealth Ombudsman to oversee the regime.

The Commonwealth Ombudsman, in their submission to this inquiry, noted that their advice was considered and that the Bill is designed in such a way that the Ombudsman has appropriate levels of oversight.[9] The Ombudsman did, however, suggest that they needed a commensurate increase in funding to manage this load. We mirror their calls for appropriate funding and note that the Ombudsman and similar agencies (such as the Office of the Australian Information Commissioner) have faced funding cuts in recent years. Without sufficient funding and staff, it is

[9] Commonwealth Ombudsman, Submission No 3 to Parliamentary Joint Committee on Intelligence and Security, *Telecommunications Legislation Amendment (International Production Orders) Bill 2020* (7 April 2020) 1.

unclear whether the Ombudsman can provide sufficient oversight to ensure that decisions under the IPO scheme are appropriate and proportionate to their objective.

We are also concerned about the timeframe provided to agencies to notify the Ombudsman and provide a copy of the IPO order. Given the general concern regarding the timeliness of the orders (indeed the delay in the present international information access scheme is the primary justification for the Bill), a similar degree of haste in reporting the orders to ensure compliance should be expected.[10] A shorter timeframe for the reporting of cases will allow Ombudsman reports to be tabled faster, so that the public can better see the impact and reach of the Bill.

The Bill expressly allows for oversight by Public Interest Monitors ('PIMs') in Victoria and Queensland (the two states who have PIMs enshrined in state law). The Explanatory Memorandum notes that 'there is scope to accommodate similar oversight bodies in the framework, should they be established in other jurisdiction in the future'.[11] Given the value in terms of oversight that PIMs provide and the importance of a consistent national approach to the IPO scheme, it may be more appropriate to implement a federal multi-stakeholder PIM system that oversees all IPO requests. This will ensure the use of the IPO framework is appropriate and consistent across all Australian jurisdictions.

Recommendation 5: More funding is provided to the Commonwealth Ombudsman to allow them to perform the review function required under the IPO regime contained in the Bill.

Recommendation 6: The timeframe allowed for notification of the Ombudsman be adjusted from 'within 3 months' to 'within 1 month'.

Recommendation 7: PJCIS to consider whether the creation of a federal PIM system to oversee the IPO framework (and other interception and access powers under the *TIA* Act) is appropriate.

3. International Co-operation Framework

Part 13 of the Bill creates a framework by which Australian companies and telecommunications providers can comply with international requests or orders made under a designated international agreement. It does so in a permissive manner, that essentially exempts the companies from obligations under the *TIA Act* and the *Privacy Act 1988* (Cth), by making compliance with such an order a disclosure authorised under the *TIA Act*.

We note that the Bill does not impose obligations on Australian companies to comply with those orders or requests. As they stand, these provisions do not pose any concerns regarding

[10] Noting that it is unclear why agencies need three months to report the use of the IPO scheme, such notification is not arduous and one month would likely afford sufficient time for them to prepare their report.
[11] Explanatory Memorandum (n 7) [30].

proportionality. Once again, this needs to be assessed on a case-by-case basis. Of concern is the potential for such international agreements (or the domestic laws of the countries Australia signs agreements with) to fail to appropriately and proportionally balance privacy and security interests. Precisely when, with whom and on what terms Australia will enter into a designated international agreement remains to be seen. Each of these arrangements will need to be considered carefully. In addition to review by the Parliamentary Joint Standing Committee on Treaties (PJSCT), we recommend that any entry into a designated international agreement is carefully scrutinised and assessed by the PJCIS and the Office of the Australian Information Commissioner (OAIC) and that such reviews consider (among other things):

- The domestic privacy protections available in the other jurisdiction, and whether they are equivalent to the protections afforded under Australian law;
- Whether the agreement allows for requests or orders to be issued in circumstances that afford lower protections than those under the current Australian framework;
- The circumstances under which Australian companies would be required to comply with the order and whether there is appropriate scope for Australian companies not to comply if they fear the information may be used to harm an individual or in a manner not commensurate to the security value of the information;
- The likely use of information by the foreign jurisdiction, especially whether surveillance measures have been deployed to prevent dissidents from raising valid concerns with the government;
- The adherence of the foreign jurisdiction to the rule of law and whether appropriate oversight mechanisms are in place;
- Whether the agreement provides for domestic reporting of requests made and granted similar to the reporting required under the IPO framework.

This could be conducted by way of independent reports to the PJSCT or a broader inquiry encompassing all three Committees, we make no recommendation as to the manner of inquiry.

We note that recent media reports have suggested that Australian data being collected by the COVID-Safe app is currently subject to subpoena in the United States due to the fact that Australia has not signed an Executive Agreement pursuant to the *CLOUD Act*. This impact is beyond the scope of this inquiry; however, we recommend that a detailed examination of what data collected by government is currently at risk of subpoena by overseas law enforcement agencies be conducted. We also recommend that the scrutiny process of any agreement is not rushed due to a perceived threat to COVID-Safe data, instead if necessary, an alternate data storage solution should be found.

Recommendation 8: Entry into a designated international agreement is carefully scrutinised by the PJCIS and OAIC. Appropriate time should be taken in these reviews to allow for open public consultation.

Yours sincerely,

Andrew Ray, Bridie Adams and Kate Renehan