THE ALLENS HUB
FOR TECHNOLOGY, LAW & INNOVATION

LAW BUILDING F8, UNSW SYDNEY NSW 2052 AUSTRALIA
+61 (2) 9385 2254 | ABN 57 195 873 179 | CRICOS Provider Code 00098G

30 April 2020

Parliamentary Joint Committee on Intelligence and Security
By email: pjcis@aph.gov.au

Submission

Review of the effectiveness of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 ('IPO Bill')

Genna Churches (Hub member), Michael Murdocca (UNSW Law student),
Monika Zalnieriute (Stream Lead), Lyria Bennett Moses (Director)
Allens Hub for Technology, Law and Innovation, UNSW Sydney.

About Us

The Allens Hub for Technology, Law and Innovation ('the Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law, the Allens Hub aims to add depth to research on the diverse interactions among technology, law, and society. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society and the broader community. More information about the Allens Hub can be found at http://www.allenshub.unsw.edu.au/. Our submission reflects our views as researchers and are not an institutional position.

Summary of Recommendations

We welcome the opportunity to submit to the review. Our recommendations, which focus on applying our research rather than providing a comprehensive analysis, are:

1. revise existing telecommunications data access and retention laws under the *Telecommunications (Interception and Access) Act 1979* (Cth) ('*TIA Act*') and the *Telecommunications Act 1997* (Cth) ('*T-coms Act*') for consistency with our international

human rights obligations under the *International Covenant on Civil and Rights* ('*ICCPR*')[1] and *Convention on Cybercrime*,[2] both for IPOs and for domestic access;

2. delay the IPO Bill until the reviews of the data retention regime[3] and *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) ('*TOLA Act*')[4] are complete to ensure compliance with US requirements for the bilateral arrangement under the '*US CLOUD Act*';

3. ensure the IPO Bill is consistent with the government's scheme for protecting COVIDSafe app data from access by domestic and international national security and law enforcement agencies;

4. ensure consistent protections for telecommunications data held domestically and data held offshore by making the domestic access regime consistent with the higher standards for an outgoing international production order ('IPO');

5. ensure the same protections are provided for both incoming and outgoing IPOs and that incoming IPOs are prohibited from being fulfilled where the investigation relates to a crime punishable by death;

6. provide a definition of 'telecommunications data' for the domestic metadata regime under either the *TIA Act* or *T-coms Act*;

7. confirm that a US CLOUD Act Agreement is necessary; and

8. change the terminology in the IPO Bill linking designated communications providers with stored communications and telecommunications data from a reference to data that is *held* to data that the provider is *legally and practically able to access*.

Complexity and Urgency

The Bill introduces further complexity to the *TIA Act* which is already complex, confusing and contradictory.[5] Failure to address existing ambiguities and complexity makes it difficult to determine whether the IPO Bill will meet its objectives of implementing a 'US satisfactory' framework for international production orders ('IPOs'). Given both TOLA and the metadata retention and access regime are being reviewed by the INSLM and PJCIS respectively, we recommend that it would be prudent to delay the IPO Bill to allow time to adopt recommendations from the INSLM and PJCIS that

[1] *International Covenant on Civil and Political Rights*, opened for signature, 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976).
[2] *Convention on Cybercrime*, opened for signature 23 November 2001, ETS No 185 (entered into force 1 July 2004).
[3] PJCIS on 'Review of the mandatory data retention regime'.
[4] INSLM 'Review of the Telecommunications and other Legislation Amendment (Assistance & Access) Act 2018 (TOLA Act)' reporting 30 June 2020 to the PJCIS on 'Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018' reporting 30 September 2020.
[5] Monika Zalnieriute and Genna Churches, *Submission to Review of the Mandatory Data Retention Regime Prescribed by Part 5-1A of the Telecommunications (Interception and Access) Act 1979 (CTH) ('TIA Act')* (Submission, The Allens Hub, 28 June 2019) 1; Churches and Zalnieriute, *Unlawful Metadata Access Is Easy When We're Flogging a Dead Law* (n 11); Churches and Zalnieriute, 'A Window for Change: Why the Australian Metadata Retention Scheme Lags Behind the EU and USA' (n 11); Genna Churches and Monika Zalnieriute, *Supplementary Submission to Review of the Mandatory Data Retention Regime Prescribed by Part 5-1A of the Telecommunications (Interception and Access) Act 1979 (Cth) ('TIA Act')* (Submission to the PJCIS No 28.1, The Allens Hub, 11 March 2020).

resolve inconsistencies between the proposed provisions for IPOs and the existing regime for metadata/telecommunications data within Australia ('domestic regime').

We also question the urgency surrounding the IPO Bill. Given the already complex nature of the telecommunications interception and access regime, we question the wisdom of rushing through another 216 pages of amendments to that regime. In particular, the current Covid-19 crisis will reduce the ability of the public, academics and industry to scrutinise the IPO Bill. We acknowledge and appreciate the PJCIS extending the time for submissions and understand its obligations to report, but caution that this speed during a crisis is likely to result in a poor legislative outcome.
New concerns surrounding the complexity of this area of law have recently been aired in the media with respect to the government's proposed contact tracing app for Covid-19. While we appreciate a ministerial determination was issued on 25 April 2020 seeking to protect the application data and national data store, we highlight that this can be revoked or altered at any time. It may also cease to apply prior to the deletion of all COVIDSafe data. Even if the data is stored in Australia, it may be accessible under the US CLOUD Act despite comments that the ministerial determination will 'trump' the US CLOUD Act.[6] The IPO Bill should be drafted to ensure that COVIDSafe data is not accessible to any domestic or foreign agency and to ensure that is does not interfere with protections for COVIDSafe data more generally. Without those protections for the app, any data stored in the US could be accessible under the IPO Bill and further opportunities for US access to the data even if stored in Australia may result.

We also highlight the repeated calls for a complete revision of the *TIA Act* and the *Telecommunications Act*. This would also provide an opportunity to align the domestic metadata regime with the requirements for a Cloud Act Agreement with the US, rendering many amendments under the IPO Bill unnecessary.[7]

Incompatibility of the Current Regime of Telecommunications Data Access with a US CLOUD Act Agreement

The US Code on *Wire and Electronic Communications Interception and Interception of Oral Communications* provides that executive agreements on access to data by foreign governments can only be made with foreign governments who 'afford robust substantive and procedural protections for privacy and civil liberties in light of the data collection'.[8] In particular, the *Code* states that foreign governments must have enacted laws which are consistent with chapters one and two of the *Convention on Cybercrime*[9] and:

> *adheres to applicable international human rights obligations and commitments or demonstrates respect for international universal human rights, including—*
>
> *(I) protection from arbitrary and unlawful interference with privacy*[10]

Australia has been criticised for insufficient protections for the right to privacy.[11] In particular, we lack legislation consistent with article 15 'conditions and safeguards' of the *Convention on Cybercrime*

[6] Max Koslowski, 'Coronavirus Australia: Health Minister Greg Hunt Says App Data Will Stay Here despite US Security Laws', *Sydney Morning Herald (online)* (28 April 2020) <https://amp.smh.com.au/politics/federal/coronavirus-app-data-will-stay-here-despite-us-security-laws-health-minister-says-20200428-p54o05.html>.
[7] Churches and Zalnieriute, *Unlawful Metadata Access Is Easy When We're Flogging a Dead Law* (n 11).
[8] *Wire and Electronic Communications Interception and Interception of Oral Communications,* 18 USC 119 § 2523.
[9] *Convention on Cybercrime* (n 2).
[10] *Wire and Electronic Communications Interception and Interception of Oral Communications,* 18 USC 119 § 2523.
[11] Joseph Cannataci, *Mandate of the Special Rapporteur on the Right to Privacy* (No OL AUS 6/2018, 12 October 2018) <https://www.ohchr.org/Documents/Issues/privacy/O_LAUS_6.2018.pdf>.

(which includes enacting various protections arising out of obligations under the *ICCPR*).[12] Further, the domestic regime for metadata retention and access pays insufficient regard to the right to privacy in that it lacks independent authorisation and a sufficiently high threshold of seriousness.[13]
There have been major shifts toward the protection of metadata around the world. In the US, the Supreme Court ruled in *Carpenter v United States*[14] that location metadata required a search and seizure warrant, the highest level of protection. In the EU, case law recognising blanket data retention regimes as incompatible with fundament rights is likely to be expanded, with an opinion from the Advocate General hinting that the Court of Justice of the European Union will continue or even strengthen its statements about data retention.[15] Rather than these amendments, which are required to conform to the requirements of a US CLOUD Act Agreement, amendments could go further to ensure that the domestic regime provides equivalent protections.

Currently, the IPO Bill creates a two-tiered system of metadata access. Under the domestic regime, metadata is accessible for the investigation of any law, by many agencies for anything from littering, the protection of public revenue and traffic offences, without independent prior authorisation or threshold of severity.[16] However, under the IPO Bill, only serious category one offences justify a warrant and the warrant application must be made by an enforcement agency.[17] The IPO Bill therefore creates a threshold of seriousness of the crime, the requirement that it must be related to criminal law and a warrant process. This two-tiered system suggests that an individual suspected of a serious class one offence with metadata in the US is afforded a greater level of privacy protection than ordinary Australians.

If legislators believe Australians are entitled to this level of protection under an IPO then we believe the same level of protection should apply to domestic metadata access. If the warrant requirement and threshold of severity can work in the IPO context, it is difficult to see why similar parameters cannot be placed on the domestic metadata regime which would result in Australia fulfilling its obligations under the *Convention on Cybercrime*, the *ICCPR* and the requirements for a Cloud Act Agreement.

IPO Bill Defines 'Telecommunications Data'/Metadata

Domestically there has been stiff resistance to defining 'telecommunications data' in the TIA Act. However, the IPO Bill provides clarification on the definition of telecommunications data. While we agree that defining telecommunications data is an important step, the definitions show already show inconsistencies between the domestic and IPO regime. For example, MAC addresses are specifically

[12] *Convention on Cybercrime* (n 2); *International Covenant on Civil and Political Rights* (n 1).
[13] Genna Churches and Monika Zalnieriute, 'Unlawful Metadata Access Is Easy When We're Flogging a Dead Law', *The Conversation* (12 October 2019) <https://theconversation.com/unlawful-metadata-access-is-easy-when-were-flogging-a-dead-law-127621>; Genna Churches and Monika Zalnieriute, 'A Window for Change: Why the Australian Metadata Retention Scheme Lags Behind the EU and USA', *AUSPUBLAW* (26 February 2020) <https://auspublaw.org/2020/02/26/>.
[14] *Carpenter v United States* (n 39).
[15] *Advocate General's Opinions in Case C-623/17 Privacy International, Joined Cases C-511/18 La Quadrature Du Net and Others and C-512/18 French Data Network and Others, and Case C-520/18 Ordre Des Barreaux Francophones et Germanophone and Others* (n 37); 'Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General' (2014) Joined Cases C-293/12 and C-594/12 *Court of Justice of the European Union* <http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&cid=8886631> ('Digital Rights Ireland'); *Joined Cases Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Watson C 203/15 and C-698/15* (Court of Justice of the European Union, 21 December 2016).
[16] See, eg, *Telecommunications Act 1997* (Cth) s 280; *Telecommunications (Interception and Access) Act* (n 16) Part 4-1; Churches and Zalnieriute, *Unlawful Metadata Access Is Easy When We're Flogging a Dead Law* (n 11); Churches and Zalnieriute, 'A Window for Change: Why the Australian Metadata Retention Scheme Lags Behind the EU and USA' (n 11).
[17] Telecommunications Legislation Amendment (International Production Orders) Bill 2020 cl 48.

included under the IPO regime, whereas domestically, law enforcement agencies and Home Affairs have stated that MAC addresses are not part of the *retained* data set.[18] However, we have argued that the current wording of the data set would not specifically exclude the retention of MAC addresses.[19] These inconsistencies now raise questions — does this mean that MAC addresses of telecommunications users will be accessible under an IPO, but not retained under the metadata retention regime?[20]

Incompatibility with Anti-Encryption Laws (TOLA Act)

To have a CLOUD Act agreement, countries which participate in a cross-border data access bilateral agreement with the United States must provide 'robust, substantive and procedural protections for privacy and civil liberties'.[21] Recognising this, the Chairman of the United States House of Representatives Judiciary Committee Jerrold Nadler recently advised the Minister for Home Affairs that there is ongoing concern among Congressional representatives that Australia does not satisfy this standard.[22] There are legitimate grounds for such consternation, particularly given that the *TOLA Act* does not provide robust privacy safeguards such as options to access independent judicial review with respect to most decisions made under the Act.[23] It is appropriate to note that decisions made under Part 15 of the *Act* cannot be reviewed under the *Administrative Decisions (Judicial Review) Act 1977* (Cth) and they are not made by a judicial authority.[24] As such, we propose that the *TOLA Act* be amended so that it requires judicial authorisation prior to the conferral of technical capability notices or technical assistance notices, principally so that there is proper oversight over whether they are provided for national security or law enforcement purposes and satisfy a high standard of reasonableness and appropriateness.[25]

Changes should be made to the *TOLA Act* in line with earlier bipartisan recommendations of the PJCIS which were not interwoven into the then-Bill of the for pragmatic reasons, namely to ensure the Bill's quick passage through parliament in 2018.[26] We propose amending the vague definitions of 'systemic weakness' and 'systemic vulnerability' contained in section 317B as they implicitly suggest,[27] from a legal standpoint, that deliberately weakening all messaging platforms with one backdoor would be impermissible although facilitating access to particular messaging platforms such as WhatsApp would be permissible. Specifically, we suggest broadening the scope of 'systemic vulnerability' and 'systemic weakness' so that they encompass any material risk that information may be accessed or used by an unauthorised third party, in line with the proposed amendments set out in the *Telecommunications*

---

[18] Commonwealth of Australia, *Official Committee Hansard, Parliamentary Joint Committee on Intelligence and Security* 28 February 2020.
[19] Zalnieriute and Churches (n 13).
[20] Commonwealth of Australia (n 45) discussions around MAC Addresses.,
21 Electronic Privacy Information Centre, *The CLOUD Act* (20 April 2020) EPIC <https://epic.org/privacy/cloud-act/>; *Wire and Electronic Communications Interception and Interception of Oral Communications,* 18 USC 119 § 2523.
22 Denham Sadler, 'Encryption Laws a CLOUD Deal Risk', Innovation Aus (online), 11 October 2019 <https://www.innovationaus.com/encryption-laws-a-cloud-deal-risk/>; .Department of Home Affairs, *Response to the Independent National Security Legislation Monitor (INSLM TOLA Review)* (February 2020) 6.
23 Michael Swinson, *Assistance and Access Act becomes Law Despite Industry Reservations* (17 December 2018) King & Wood Mallesons <https://www.kwm.com/en/au/knowledge/insights/assistance-and-access-act-becomes-law-despite-industry-reservations-20181217>.
24 Alexandra Wedutenko, *Cracking the Code: Understanding the Implications of Australia's New Encryption Laws on Your Business and Supply Chains* (7 March 2019) Clayton Utz <https://www.claytonutz.com/knowledge/2019/march/cracking-the-code-understanding-the-implications-of-australias-new-encryption-laws-on-your-business-and-supply-chains>.
25 Rohan Pearce, 'Proposed Changes to Australia's Encryption Laws Win Telco Backing', *Computer World* (online), 4 December 2019 <https://www.computerworld.com/article/3487699/proposed-changes-to-australias-encryption-laws-win-telco-backing.html>.
[26] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *The Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (2019) 1.4.
[27] *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) s 317B.

Amendment (Repairing Assistance and Access) Bill 2019.[28] Such amendments will be increasingly appropriate to ensure a well-synchronised approach to the collection of data among Five Eyes members in an environment where telecommunications companies such as Facebook are seeking to strike a balance between making some concessions to satisfy the investigatory demands of law enforcement agencies with respect to serious crimes while still preserving protections for their users so that private information is inaccessible by unauthorised third parties.[29] Likely forthcoming attempts by law enforcement and national security representatives to negotiate with telecommunications companies to find a pragmatic fusion between these two priorities is inherently delicate in nature, thus requiring Australia's legislative framework to properly ensure that it does not permit encryption back doors to be created in circumstances where they undermine encryption on a wider and more consequential scale.[30] To ensure that the PJCIS gives effect to Dr James Renwick's concerns set out in his opening statement at the Public Hearings in the INSLM Review, it is necessary to amend the words 'would or may in the future' in the proposed s 31ZG(4) which presently confers an unachievable standard, particularly because it is never possible to characterise the associated risks as completely avoidable.[31] It is also appropriate to provide for alternative dispute resolution options (as being explored by Dr Renwick) in the event where a DCP claims on a bona fide basis that a law enforcement or national security agency has issued an unreasonable Schedule 1 notice or request.[32] The current provisions indeed provide that the first point of call should be a court in the resolution of such a matter which may be inappropriate if that particular matter should be subject to absolute secrecy or encapsulates sensitive information.[33]

'Incoming' IPOs — When Australian Telcos Fulfil an IPO from an Overseas Jurisdiction

Part 13 of the IPO Bill relates to 'incoming' IPOs — that is a foreign jurisdiction seeking access to Australian data. Part 13 could be read as containing no protections for Australian telecommunications users when telcos *receive* an *incoming* IPO from an overseas jurisdiction. All matters at part 13 of the IPO Bill relating to stringency and conditions placed on an incoming IPO are undefined. While this part may be subject to international agreements, these agreements may be struck between the Australian executive and an external government and may not be subject to the scrutiny of Parliament. It is possible for such an agreement with an external country to permit the disclosure of content and/or metadata without a warrant or even an authorisation from enforcement agency. Such an arrangement would further erode privacy protections for Australian telecommunications users and may also expose those users to penalties beyond Australian acceptable limits such as capital punishment. This means that there must be strict protections of the requirements of an incoming IPO – this should include of warrant process for access to all Australian data (content and metadata), a threshold of serious crime, and the option to prohibit access to data where the crime carries the penalty of death.

[28] Telecommunications Amendment (Repairing Assistance and Access) Bill 2019 (Cth).
[29] Zak Doffman, 'Here is What Facebook Won't Tell You About Message Encryption', *Forbes* (online), 6 October 2019 <https://www.forbes.com/sites/zakdoffman/2019/10/06/is-facebooks-new-encryption-fight-hiding-a-ruthless-secret-agenda/#7321ff955699>.
[30] Julian Barnes, Katie Benner and Mike Isaac, 'Barr Pushes Facebook for Access to WhatsApp Messages', *The New York Times* (online), 4 October 2019 <https://www.nytimes.com/2019/10/03/us/politics/barr-whatsapp-facebook-encryption.html>.
[31] Dr James Renwick CSC, SC, 'Opening Statement' (Speech delivered at the Public Hearings in the ISLM Review at the Request of the Parliamentary Joint Committee on Intelligence and Security Concerning the Telecommunications and Other Legislation Amendment (Access and Assistance) Act 2018 (Cth), Canberra, 20 February 2020).
[32] Ibid.
[33] Ibid; Dr Renwick is also exploring an alternative model which would provide technical expertise to the decisionmaker.

It is also unclear whether telecommunications data sought under an incoming IPO can include both retained data under s 187 of the *TIA Act* or voluntarily retained data (i.e. telco retained data for business and other purposes). If access is permitted to the s 187 mandatorily retained metadata and is provided under an incoming IPO without a warrant or other authorisation, the proportionality of the two-year metadata retention scheme must be questioned.

Existing Inadequacies in Reporting Measures

Due to existing inadequacies around reporting measures under Australia's domestic data retention regime and the TOLA, we question if there is a compelling number of cases which require data from overseas to justify a US Cloud Act Agreement, and how these numbers and need has been determined.[34] For example, the PJCIS has highlighted the inadequate reporting measures under the data retention and access regime and our researchers, Bennett Moses and Churches have previously critiqued reporting mechanisms under the *TOLA Act*. These reporting regimes are vital for bodies such as the PJCIS to determine the effectiveness of these existing regimes and may provide insight on the requirement for further or different powers.[35] Answers to questions such as, how many cases of metadata access in the domestic regime are for serious offences, may provide insights on the volume of requests which would reach the IPO threshold, providing valuable information on the need of a US Cloud Act Agreement. These figures may also provide some insight into the perceived rush surrounding the IPO Bill.

Precision of Language

A crucial question in any legislation that creates obligations for entities in relation to data (including information and communications) is specifying the link between an entity and that data. To date, there are a wide variety of terms used in legislation including possess, acquire, obtain, kept, responsible for, control over, has access to, custody and holds.[36] These terms are sometimes accompanied by definitions, which are themselves often inconsistent between statutes. While lack of clarity in terminology may have been less critical in the past, new data practices including cloud computing and randomness in physical location of data storage make it essential that precise terminology is used.

In the IPO Bill, the word used to link entities to communications is "holds" (including variations such as "held" and "reasonable grounds for suspecting that … holds").[37] The verb 'to hold' and its derivatives suggest a physical grasp of an object, so are potentially confusing when used in relation to telecommunications data and stored communications. A file in a filing cabinet can be physically grasped or physically controlled (through access to the filing cabinet). But determining which entity 'holds' information stored on a server in the cloud pursuant to a contract granting control and/or access to different entities requires an assessment beyond physicality.

[34] Ibid; Lyria Bennett Moses, Genna Churches and Nicholas Parker, *Submission to the Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Submission, The Allens Hub, 25 October 2019). See inadequacies in reporting measures highlighted by the PJCIS particularly the line of questioning undertaken by Senator Dreyfus.
[35] Bennett Moses, Churches and Parker (n 48).
[36] Lyria Bennett Moses, 'Who Owns Information? Law Enforcement Information Sharing as a Case Study in Conceptual Confusion' (2020) *University of New South Wales Law Journal* (forthcoming). Can be made available to the Committee on request but cannot be published until the issue of the journal.
[37] See Telecommunications Legislation Amendment (International Production Orders) Bill 2020 Sch 1 Amendments to the Telecommunications (Interception and Access) Act 1979 inserting Sch 1 cll 39(2)(a), 48(2), 69(2)(b), 78(2), 98(2)(b), 107(2).

What the IPO Bill requires is a more precise term that captures the relationship with which the Bill is concerned, namely the link between telecommunications data or stored communications and designated communications providers.[38]. The best way to describe that relationship, in line with the intention of the legislation, is to refer to the provider's *ability to access* the relevant data or communication. In the case of a stored communication, this may not amount to full control (for example, a designated communications provider may not have the ability to alter the communication) and the provider may not have accessed the communication previously. Here, *ability to access* should be defined in terms of both practical and legal capability. This will help clarify the telecommunications data and stored communications for which a particular designated communications provider is responsible under the Act.

[38] Designated communications provider is defined in Telecommunications Legislation Amendment (International Production Orders) Bill 2020 Sch 1 Amendments to the Telecommunications (Interception and Access) Act 1979 inserting Sch 1 cl 2.