

Committee Secretary
Joint Standing Committee on Treaties
PO Box 6021
Parliament House
Canberra ACT 2600

21 March 2022


By email: jsct@aph.gov.au

Dear Committee Secretary

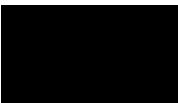
RE: Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime

Thank you for providing the opportunity to comment on the Access to Electronic Data for the Purpose of Countering Serious Crime Treaty ('the Treaty'). By way of background, I am a Visiting Fellow based at the Australian National University College of Law in Canberra and hold a Bachelor of Science and a Bachelor of Laws (Hons) from that institution. My primary research areas are artificial intelligence and data privacy law. I have, however, published articles and contributed to parliamentary inquiries in several other areas, including national security. My work also analyses parliamentary inquiry processes generally. A list of my current and forthcoming papers can be found here.¹

This submission reflects my personal views only and does not reflect the institutional view of the ANU College of Law, or the ANU more broadly.

If the Committee requires any further clarification or if I can assist further, please contact me directly 

Yours sincerely



Mr Andrew Ray
Visiting Fellow, ANU College of Law

¹ <<https://researchers.anu.edu.au/researchers/ray-ad>>. Where permitted by the publisher, my publications can be publicly accessed via ResearchGate: <<https://www.researchgate.net/profile/Andrew-Ray-4/publications>>.

Summary of Recommendations:

1. The Treaty be referred to the Parliamentary Joint Committee on Intelligence & Security and the Office of the Australian Information Commissioner to consider the wider security and privacy implications if the Treaty is entered into force.
2. In assessing the Treaty, the committee consider whether the Treaty provisions and the powers it provides to Australian and United States law enforcement and national security agencies are proportionate to the threat it seeks to combat.
3. The committee call for the underlying data justifying the need for faster access to overseas held data to be made publicly available. Or, alternatively, where national security implications prevent the full release of that data – that a redacted assessment justifying the need for the powers be released.
4. The committee consider whether the Treaty as it stands should be entered into force in circumstances where the definition of serious crime in the Treaty has a lower threshold than in the underlying Australian legislation (sch 1 to the *TIA Act*).
5. The committee consider whether additional oversight and reporting thresholds should be introduced in Australian domestic law prior to the entry into force of the Treaty.

Introduction

The Treaty reflects the culmination of negotiations between Australia and the United States to streamline the access to overseas held (or controlled) data by law enforcement and national security agencies to assist in the detection, prevention, investigation and prosecution of serious crime. In an Australian context, much of the preparatory work to the Treaty was performed through the passage of the Telecommunications Legislation Amendment (International Production Orders) Bill ('the IPO Bill') in June 2021. While it appears that the Government engaged in some limited consultation concerning the Treaty text, the National Interest Analysis notes that much of the consultation with civil society bodies occurred during the review of the IPO Bill in 2020 as the Treaty discussions were confidential.²

The IPO Bill had (relevantly) been reviewed by the Parliamentary Joint Committee on Intelligence and Security ('PJCIS') and the Parliamentary Joint Committee on Human Rights. I was one of the authors of a submission by the ANU Law Reform and Social Justice Research Hub³ to the PJCIS inquiry. That submission made a number of targeted recommendations to strengthen the oversight and privacy protections contained in the Telecommunications (Interception and Access) Act 1979 (Cth) ('*TIA Act*').⁴ I note that following that inquiry some amendments were made to the IPO Bill, however I repeat the recommendations contained in the ANU LRSJ Submission to the PJCIS as to further changes that could be considered to the *TIA Act* to increase the oversight and

² National Interest Analysis [2022] ATNIA 4, Attachment 1.

³ I understand that the ANU LRSJ Research Hub may be making a submission to this inquiry, I have not contributed to that submission.

⁴ ANU Law Reform and Social Justice Research Hub, Submission 17
<<https://www.aph.gov.au/DocumentStore.ashx?id=2de81706-05d5-40ad-b22f-c6554c1df8cc&subId=680367>> ('PJCIS Submission').

transparency of the IPO regime generally.⁵ Such changes should be considered *prior* to the Treaty being entered into force.

While such considerations are beyond the scope of the current inquiry, they highlight several underlying concerns with the *TIA Act* that should be considered before the Treaty is entered into force.

Of particular note is the fact that the Treaty is only being considered by the Joint Standing Committee on Treaties.⁶ As a result of that narrow referral, the wider security and privacy implications of the Treaty are not being formally considered by either the PJCIS or the Office of the Australian Information Commissioner. While, as noted above, no legislative amendment is required to implement the Treaty,⁷ it nevertheless will still enliven the powers contained in sch 1 of the *TIA Act*. Therefore, while Australian law is not changing, the powers available to Australian and United States law enforcement and national security agencies will increase when the Treaty is entered into force.

Given that change, the text of the Treaty ought to be referred to a wider review by both the PJCIS and the OAIC,⁸ to consider, amongst other matters, whether the current threshold of serious crime in the Treaty is appropriate.⁹ I note that comments from the Department of Home Affairs seem to anticipate that the Treaty will enter into force in late 2022. This would provide sufficient time for a wider inquiry to be conducted prior to that step occurring. Such a review should also consider whether the current oversight measures contained in the Australian domestic legislation are sufficient.

Referring the Treaty for further review is appropriate given that this is the first treaty that Australia is a party to that will enliven the powers contained in sch 1 of the *TIA Act*. Wide input from law enforcement and national security agencies as well as the general public should therefore be considered, including by other specialist parliamentary committees.

Broad Overview of the Treaty and its Rationale

Broadly, the Treaty aims to streamline the existing co-operation framework that exists between the Australian and United States governments and their respective law enforcement and national security agencies. In particular, the Treaty aims to ‘facilitate the exchange of electronic data, and protection of that data, between communications service providers, and law enforcement and national security agencies in Australia and the United States’.¹⁰ It does this by enabling authorised law enforcement and national security agencies to issue data production orders to telecommunications companies. Such orders would require those companies to provide data to

⁵ *Ibid*, see especially recommendations 4, 5, 6.

⁶ This was also recommended in the PJCIS submission.

⁷ National Interest Analysis [2022] ATNIA 4, [38]: “no further substantive legislative reform is required to implement the Agreement”.

⁸ This recommendation is further explained in ANU Law Reform and Social Justice Research Hub, Submission 17 see 6-7.

⁹ I will consider this matter further below.

¹⁰ National Interest Analysis, [3].

the respective law enforcement or national security agency. Any such orders must relate to data that would assist in the prevention, detection, investigation or prosecution of “serious crime”.¹¹

The National Interest Analysis notes that such powers are necessary as the current Mutual Assistance Regime¹² is not fit for purpose. With law enforcement and national security agencies indicating that they face significant delays in seeking access to information due to the resource intensive nature of the MLAT provisions, which requires direct government communication and use of domestic legal processes to gain access to the data.¹³

This means that MLAT requests can take up to 12 months to process, which, according to the National Interest Analysis is limiting the ability of law enforcement and security agencies to achieve convictions or otherwise delaying them taking appropriate action against alleged offenders.¹⁴ These concerns have (according to the National Interest Analysis) increased in recent years given the increasing use of data by law enforcement and national security agencies and the increasing amount of Australian data stored overseas.

The National Interest Analysis does not provide the data that provides evidence for the claim that delay in access to data is impacting prosecutions in Australia. At least for federal prosecutions, it is not apparent that publicly available statistics would support an assessment that convictions are being significantly impacted by any such delay. In particular, the CDPP has a very successful conviction rate, which reflects the practice of only pursuing cases where there are reasonable prospects of obtaining a conviction.¹⁵ It is also not apparent that increasing the amount of data available to be analysed by law enforcement and national security agencies will reduce the incidence of serious crime or enable those agencies to prevent, for example, terror attacks. In particular, efforts may be better suited to improving how data that can already be accessed is analysed, or how current data-gathering powers may be used more efficiently rather than increasing the *amount* of data available to these agencies.

It is also worth noting that, depending on the definition of serious crime, Australian law enforcement and security agencies already possess significant detention powers prior to any court action being taken. For example, in the case of terrorism offenders, agencies already possess powers to seek control orders to prevent a likely terror attack.¹⁶ As will be discussed further below, data access powers (like those that will be enlivened by the Treaty) are often justified by reference to the threat posed by terrorism offenders.

¹¹ Ibid, [4].

¹² As contained in the *Treaty between the Government of Australia and the Government of the United States of America on Mutual Assistance in Criminal Matters* (30 April 1997) (‘MLAT’).

¹³ National Interest Analysis, [10]-[11].

¹⁴ Ibid [12]-[13].

¹⁵ Commonwealth Director of Public Prosecutions, ‘Prosecution Statistics’ (Web Page) <<https://www.cdpp.gov.au/statistics/prosecution-statistics>>. The currently available data is for the 2019-2020 year.

¹⁶ Commonwealth Criminal Code div 104. Control orders can be sought (inter alia) where a senior AFP member ‘suspects on reasonable grounds that the order in the terms to be requested would substantially assist in preventing a terrorist act’. Control orders have in recent years however been sought for offenders being released from prison, and are being used less frequently before conviction.

The National Interest Analysis notes that the need for access to overseas-held data has increased in recent years given the number of data companies operating out of the United States. So much can be accepted. However, it is also worth noting that companies can store data in countries other than where they are headquartered. For example, Facebook is known to hold significant amounts of its data in data centers located in Ireland.¹⁷ It is therefore not apparent that a bilateral treaty such as the one being considered by the committee will fully resolve the issue, or that companies will continue to store data in Australia or the United States if the Treaty is entered into force. Indeed, if the Treaty encourages companies to store data in other jurisdictions or encourages individuals to avoid mainstream platforms that store data in the United States, the Treaty may harm data gathering efforts rather than aiding them.

Broadly, the Treaty continues the trend of placing privacy and security into a false dichotomy, with the general rationale being that if you have nothing to hide you have nothing to fear. As outlined in more detail in the PJCIS submission, such an approach oversimplifies the problem, and the burden should be on law enforcement and national security agencies to justify any increased data-gathering powers.¹⁸ Such a justification should focus on why such powers are needed, and how access to more data is necessary and proportionate to combat identifiable threats (in contrast to other measures such as improving data analysis methods or tools).

Notwithstanding the above, the Treaty does contain several important safeguards, including that the US cannot target Australian citizens or permanent residents¹⁹ and that Australian-sourced data will not be used for capital cases. One aspect of the Treaty that is of concern, however, is the relatively low threshold of serious crime contained in the Treaty text.

Definition of Serious Crime

It is worth considering what crimes the Treaty aims to combat by enabling faster (and easier) data sharing between Australia and the United States. The Revised Explanatory Memorandum to the IPO Bill repeatedly referred to serious crimes. For example, it stated at [2] that:

Almost every crime type and national security concern has an online element—agencies require electronic information and communications data not only for cyber investigations but also for investigations and prosecutions regarding violent crimes, human trafficking and people smuggling, drug trafficking, financial crimes, terrorism and child sexual abuse.

Similar references were made throughout the Revised Explanatory Memorandum to terrorism offenders (and other forms of serious crime), and the need to protect Australia from significant threats. This focus is reflected in Australia's enabling legislation. For example, the definition of serious offence found in s 5D to sch 1 of the *TIA Act* which defines serious offences that would

¹⁷ See generally *Facebook Inc v Australian Information Commissioner* [2022] FCAFC 9. Albeit in that case the Full Court of the Federal Court dismissed Facebook's appeal against interlocutory orders that its US branch could be served with the dispute.

¹⁸ See PJCIS submission generally, but especially pp 2-3.

¹⁹ See in particular art 7 which prevents the US from targeting Australian citizens, permanent residents or Australian companies. And similarly prevents Australia from doing the same to US citizens.

enliven the provisions permitting an eligible judge or a nominated AAT member from issuing an international production order.

That definition outlines a list of serious offences, and relevantly includes the following²⁰:

- (2) An offence is also a **serious offence** if:
 - (a) it is an offence punishable by imprisonment for life or for a period, or maximum period, of at least 7 years; and
 - (b) the particular conduct constituting the offence involved, involves or would involve, as the case requires:
 - (i) loss of a person's life or serious risk of loss of a person's life; or
 - (ii) serious personal injury or serious risk of serious personal injury; or
 - (iii) serious damage to property in circumstances endangering the safety of a person; or
 - (iiia) serious arson; or
 - (iv) trafficking in prescribed substances; or
 - (v) serious fraud; or
 - (vi) serious loss to the revenue of the Commonwealth, a State or the Australian Capital Territory; or
 - (vii) bribery or corruption of, or by:
 - (A) an officer of the Commonwealth; or
 - (B) an officer of a State; or
 - (C) an officer of a Territory; or

...

As highlighted above, for an Australian International Production order to be made, it must (generally) relate to a crime with a maximum penalty of seven years or more (or for the offence to fall into the list of specifically included crimes).

In a broader Australian context, crimes with a penalty of three years or more are not considered serious offences by either government or legal experts. For example, the *Crimes Act 1914* (Cth) defines a serious offence as one where there is a maximum penalty of five years or greater.²¹

In contrast, the Treaty defines serious crime as one where there is a maximum penalty of *three* years or greater.²² The difference between the Treaty definition and the definition in the underlying Australian legislation is not explained.

There was significant consultation by the Government on the form of sch 1 to the *TIA Act* prior to its implementation, with the list of offences contained in the IPO Bill tailored towards targeting serious offences. Such a targeted approach justifies the increase in the data-gathering powers of law enforcement and national security agencies, as it (appropriately) limits the use of those

²⁰ For brevity I have not extracted the entire section.

²¹ See section 23WA.

²² Arts 4(1) and 5(1).

powers to significant crimes where (in many cases) commission of the offence would result in significant harm to an individual or individuals or loss of life.

The lower threshold in the Treaty is therefore of concern for two reasons. First, it would enable the threshold in the Australian legislation to be more easily lowered (ie. by amending the definition of serious crime to mirror that contained in each of the relevant IPO agreements). Second, the lower threshold also seems to enable US law enforcement agencies to request data for lower-level offences than their Australian counterparts. In particular, the Treaty will enable US authorities to request access to data stored in Australia for offences where there is no clear risk of immediate harm or any resulting need for expedited access to data.

While access to such data would not impact on Australian citizens or permanent residents given the other safeguards in the Treaty, the rationale for only allowing instant and rapid access to data where significant harm may result from an offence applies equally to US citizens or other individuals in the US whose data is stored in Australia. The sharing of data as permitted under sch 1 of the *TIA Act* is not an insignificant power.

It is also worth noting that Australian courts will not be in a position to review United States issued requests, with such requests being made to the US Designated Authority who will itself assess whether the request complies with the Treaty (and Australian companies being required to comply).²³ While the need for rapid data sharing is (on one view) apparent for *serious* offences where there is the potential for loss of life or significant harm to occur, the three-year maximum penalty in the Treaty will not limit the use of international production orders to such offences.

Of particular concern, is the fact that the powers afforded by the treaty (and similar agreements) are regularly justified by reference to very serious crime (ie. terrorism and child exploitation material offences).²⁴ The use of such offences to justify the powers raises questions as to whether lower-level offences should be included, and whether expanding data collection powers for such offences is justified and proportionate.

A more proportionate approach would seem to be to have a higher maximum penalty in the Treaty, mirroring that contained in s 5D. Under such an approach where a law enforcement agency wanted access to data for a lower-level offence they would be able to submit a mutual assistance request under the MLAT. This is important, as by retaining a higher maximum penalty threshold in the Treaty, law enforcement and national security agencies would not be prevented from seeking access to data for their investigations. Rather, they would need to go through the mutual

²³ The corollary also applies, ie Australian requests will be made to the Australian Designated Authority. See generally Home Affairs, 'Australia-US CLOUD Act Agreement' (Web Page, 2022) <<https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/australia-united-states-cloud-act-agreement>>.

²⁴ See eg, comments made by the UK and the US on entering their own CLOUD Act Treaty: Nyman Gibson Miralis, 'The world's first CLOUD Act Agreement: The US and UK's new weapon against serious cross-border crime', *Lexology* (online, 30 March 2020) <<https://www.lexology.com/library/detail.aspx?g=3d9d670f-8114-4d91-bdc7-9c55da926bd8>>.

assistance scheme which affords Australian authorities far greater oversight of the use of Australian data by overseas agencies.