e:
t:

JOINT SUBMISSION
NSWCCL & AIIA

JOINT STANDING COMMITTEE ON TREATIES

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

18 March 2022

aiia
australian information industry association

About NSW Council for Civil Liberties

NSWCCL is one of Australia's leading human rights and civil liberties organisations, founded in 1963. We are a non-political, non-religious and non-sectarian organisation that champions the rights of all to express their views and beliefs without suppression. We also listen to individual complaints and, through volunteer efforts, attempt to help members of the public with civil liberties problems. We prepare submissions to government, conduct court cases defending infringements of civil liberties, engage regularly in public debates, produce publications, and conduct many other activities.

CCL is a Non-Government Organisation in Special Consultative Status with the Economic and Social Council of the United Nations, by resolution 2006/221 (21 July 2006).

Contact NSW Council for Civil Liberties

http://www.nswccl.org.au
office@nswccl.org.au
Correspondence to: PO Box A1386, Sydney South, NSW 1235

About the Australian Information Industry Association

The AIIA represents the depth and breadth of Australia's innovation technology companies.

Given the numbers of tech professionals employed by these companies, the AIIA represents a significant portion of the 750,000+ workforce of the Australian technology sector.

The Australian Information Industry Association (AIIA) is Australia's peak representative body and advocacy group for those in the digital ecosystem. We are a not-for-profit organisation to benefit members, and AIIA membership fees are tax deductible. Since 1978, the AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment for our members and to contribute to Australia's economic prosperity.

We do this by delivering outstanding member value by:

- Providing a strong voice of influence
- Building a sense of community through events and education
- Enabling a network for collaboration and inspiration; and
- Developing compelling content and relevant and interesting information.

The NSW Council for Civil Liberties (NSWCCL) and the The Australian Information Industry Association (AIIA) welcome the opportunity to make a submission to the Joint Standing Committee on Treaties in regard to the 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.

1 Introduction

1.1 The Clarifying Lawful Overseas Use of Data Act or **CLOUD Act** (H.R. 4943) is Federal law in the United States and was enacted in 2018.

1.2 On 24 June 2021 the Australian Parliament enacted the *Telecommunications Legislation Amendment (International Production Orders) Act* (Cth) (**IPO Act**) which enables Australian authorities to obtain international production orders to compel the production of data from entities with a presence in Australia, even if the data is stored outside Australia, and to access/receive that data.

1.3 On 15 December 2021 Australia and the United States announced an agreement[1] under the CLOUD Act (**Agreement**) intended to streamline the sharing of electronic data for law enforcement between the two countries. In conjunction with the IPO Act the Agreement will permit Australian authorities to obtain international production orders to compel the transfer of data held in the United States to Australia. The Agreement also gives reciprocal rights to United States authorities permitting them to compel the transfer of data held in Australia to the United States.

1.4 The NSWCCL and the AIIA agree with the policy objective of enhancing cooperation between Australian and the United States of America for the purpose of combating serious crime, including terrorism, but is concerned by the Agreement's impact on the privacy protections currently enjoyed by Australian residents, among other things, and makes this submission for the consideration of the Joint Standing Committee on Treaties (**Treaties Committee**).

2 Terminology used

In this submission we refer to:

(a) **Individuals**, meaning an individual resident in Australia to whom information transferred under the Agreement relates;

(b) **Orders**, having the same meaning as is given to that term in the Agreement; and

(c) **Service Providers**, meaning Australian-based companies, particularly social media companies, cloud service providers and telecommunications carriage service providers who may receive an Order.

3 Submissions

3.1 We have identified a number of significant privacy and other issues and concerns with the Agreement and discuss each of these in this Section 4.

International Orders and their impact on privacy protections for Individuals

3.2 There is a worrying lack of clarity and definitive research (see Section 5 below) as regards the operation of the Privacy Act vis-à-vis any Orders originating in the United States and to be implemented in Australia. Further analysis of the privacy impact of the Agreement, dare we say it, an independent privacy impact assessment (**PIA**), is required. Below we highlight our main concerns in this area.

3.3 The Australian Government (or for that matter any Service Provider) has little control, let alone oversight, over the process of executive and judicial decision-making that occurs in the United States in the process of issuing an Order targeting a Service Provider. This lack of oversight

[1] *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*, signed 15 December 2021.

and lack of independent assessment means there is scant assurance that Individuals' privacy has been taken into account.

3.4 Once an Order has been issued, the protections currently enjoyed by residents of Australia (i.e. Individuals) under the *Privacy Act 1988* (Cth) (**Privacy Act**) will, in practice, be of little use and be significantly eroded. In fact, the Privacy Act expressly exempts acts or practices done or engaged in outside Australia if the act or practice is required by an applicable law of a foreign country.[2] An APP entity (as defined in the Privacy Act) is effectively permitted to disregard the Australian Privacy Principles due to the IPO Act requiring and authorising the overseas disclosure.[3] This is despite wording in the Agreement purporting to maintain domestic privacy protections.[4] At the very least this will create a level of confusion that should not exist.

3.5 It is likely that the 'sidestepping' of the protections in the Privacy Act by the Agreement will mean, in the context of a disclosure of Individuals' personal information under the Agreement, the (a) erosion of existing privacy rights and (b) in practice, limited if any means to enforce what limited privacy protections there are.

3.6 In Australia there are key obligations/protections (primarily consent) relating to the collection, use and disclosure of 'sensitive information' which are not considered or provided for in the Agreement. This erodes the longstanding extra protections for sensitive information included in the Privacy Act by the Australian Parliament since the Privacy Act was passed.

3.7 The issue of an Order in or originating from the United States (and impacting Individuals) will be subject to a different threshold and fewer protections than in Australia for similar access, although because of the lack of research (or a PIA) we do not know the full extent of the differences. One example however, is that in the United States only a subpoena (and not a warrant) may be required to obtain release of older emails, which means that once an email reaches a certain date its use and disclosure may no longer be subject to United States privacy laws. This is different from the position in Australia where all emails containing personal information or sensitive information are protected equally. Under an Order originating from the United States (and enforceable in Australia) this will be permitted, thus, circumventing entrenched and longstanding Australian privacy protections.

Recommendation 1 — Build baseline privacy protections into the Agreement

Amend the Agreement to incorporate appropriate exemptions or baseline privacy protections. For example, the Service Provider the subject of an Order should be required to notify the Individual of the additional purpose for the disclosure of the Individual's personal information before or at the time the personal information is produced under an Order.

Data that has been made public

3.8 In addition, it is unclear how the words 'except to the extent that such data has already been made public'[5] will operate in practice and this may be subject to abuse. There is a broad range of reasonable interpretations as to what information is in the public domain.

3.9 The effect is that the practical operation of this provision of the Agreement can be significantly expanded by United States law enforcement agencies with limited legal and practical ability to challenge in the United States (and certainly not by the Individual – see paragraphs 4.15 to 4.18 below).

[2] Privacy Act, section 13D.
[3] Australian Privacy Principles 6.2(b) and 8.2(c).
[4] Arts 3.3, 3.4, 9.1.
[5] Art 9.2.

Recommendation 2 **Data in the public domain**

Incorporate clear guidance as to what amounts to 'data [that] has already been made public'.

Lack of warning for Service Providers

3.10 Our concern in relation to the regime created by the Agreement and IPO Act is that a Service Provider first learns about the Order after it has been issued and served, rather than when the agency is considering or applies for it.

3.11 At the point in time the Service Provider becomes aware of the existence of the Order, the risk of incurring a significant civil penalty for non-compliance with the Order timeline 'hangs over' them. This makes it more difficult for the Service Provider to, in practice, consider a challenge to the Order.

Recommendation 3 **Forewarning**

Incorporate a requirement to notify the proposed recipient Service Provider that an Order is 'on the way' with basic information about what the Order relates to.

Burden on Service Providers

3.12 Australian-based companies, particularly social media companies, cloud service providers and telecommunications carriage service providers (i.e. Service Providers) will be subject to a disproportionately heavy burden on receipt of an Order.

3.13 This cost may include the administrative burden of carrying out the request under the Order (that is, identifying, locating, extracting and readying the relevant data), seeking legal or other professional advice to ensure the legality of the Order before carrying it out and, in many cases, engaging additional capacity to actually manage the response to the Order.

3.14 This cost impacts are magnified for the many early- and growth-stage technology companies (i.e. Service Providers) that already play a significant role in Australia's crucial economic transition. Recent estimates suggest that the Australian tech sector contributes $167 billion to GDP per year and is responsible for 861,000 jobs.[6] The need to consider compliance with Orders under the Agreement (whether or not an Order is ever received) will have a dampening effect on this important sector.

3.15 The Agreement grants Service Providers (but not Individuals, as is the right given under the Privacy Act) the right to challenge an Order. However, doing so means additional costs to be borne by those Service Providers in circumstances where timing is against a challenge (see paragraphs 4.10 to 4.11).

3.16 Individuals, on the other hand, are not given any right to challenge an Order. The Individual is the biggest 'stakeholder' in relation to the impacts of an Order and has no right to challenge it (assuming they even had the means to become aware of the Order in the first place).

3.17 In some cases a Service Provider may feel they are required to challenge an Order under the Agreement for and on behalf of Individuals (that is, their customers), especially those Service Providers wishing to either build or maintain their reputation for their privacy-centric approach. That is, to fail to challenge may significantly reduce the customer goodwill they have been building.

3.18 In other cases Service Providers will not be in a position to (or may for some reason choose not to) challenge an Order for and on behalf of an individual. In such cases where the Service Provider has little or no incentive to instigate a challenge, the intended safeguarding effect of the right to challenge is rendered ineffectual and void given the most interested and most impacted person, the Individual, has no 'voice'.

[6] Tech Council of Australia and Accenture. (2021). *The economic contribution of Australia's tech sector*. https://techcouncil.com.au/wp-content/uploads/2021/08/TCA-Tech-sectors-economic-contribution-full-res.pdf.

Recommendation 4 **Cost-effective challenge mechanism**

Incorporate a cost-effective and straightforward mechanism for Service Providers subject to an Order to challenge it (that is, a place to go before or instead of commencing a court action with all of its attendant costs and complexity). Service Providers that take advantage of such a mechanism should also have the ability to involve the relevant Individual(s) in their challenge to the Order.

Conflicts with State/Territory surveillance devices laws

3.19 Further consideration is required as to the interplay of Service Providers implementing/complying with an Order and Australia's State/Territory surveillance devices legislation, which prescribe certain protections (above and beyond those under privacy law) in relation to specific means of collection of data/surveillance. A Service Provider may be in breach of these State and Territory laws in certain circumstances, depending on the means used to comply with an Order originating in the United States under the Agreement.

3.20 It is unclear, for example, whether a person who uses a surveillance device in breach of State/Territory surveillance devices legislation will remain subject to liability for their breach if they have complied with an Order. For example, will they be immune from prosecution for their unlawful surveillance under State or Territory law if it turns out that they could have complied with the Order another way of if it is 'useful' for the purposes of the Agreement (and the Commonwealth's interests under the Agreement)?

3.21 New South Wales surveillance devices legislation specifically provides for and permits the use of otherwise unlawful surveillance data for foreign law enforcement activities in certain specified cases with certain protections. More particularly, that legislation permits the use of 'protected information' in 'relevant [legal] proceedings' and provides that one category of 'relevant proceeding is a proceeding under the *Mutual Assistance in Criminal Matters Act 1987* (Cth) concerning an offence against the laws of a foreign country (e.g. the United States)[7]. The Agreement expands the extent to which surveillance devices laws that include privacy protections can be circumvented to support a foreign country's law enforcement activities (which activities would not be legal in Australia without a warrant).

3.22 The Agreement will therefore have the practical effect of removing any real resistance against and/or safeguards over the co-opting of surveillance devices located in Australia to conduct surveillance of Individuals (even surveillance that would generally be unlawful under State/Territory surveillance devices law) for United States law enforcement agencies and purposes.

Recommendation 5 **Clarify interplay with surveillance devices laws**

Either amend, or publish clear guidance as to the operation of, State/Territory surveillance devices laws in light of the IPO Act and the Agreement. Furthermore, the scope of the operation of the Agreement should be limited so as to exclude data gathered using surveillance devices in breach of applicable State/Territory surveillance devices laws.

Lack of transparency

3.23 An Individual is not notified and has no way of knowing about any transfer, sidestepping the core fundamental of transparency under the privacy guarantees given to Individuals by the Privacy Act. Transparency is about knowing what is collected, by whom, for what purpose and to whom the information is disclosed to enable the Individual to exercise their privacy rights if they wish.

3.24 The transfer will occur without the individual's knowledge so, even if an Individual had privacy rights under United States law, in practice the Individual would not be able to exercise those

[7] *Surveillance Devices Act 2007* (NSW), sections 4(1) and 40(3)(e).

rights as they are unaware of the transfer. There is no transparency to enforce their privacy rights or even lobby or petition the targeted Service Provider to resist the Order.

3.25 There is no provision for an Individual to be made aware of or challenge the transfer in Australia before its transfer or the subsequent holding or use of their information. If the Individual does challenge the subsequent holding and/or use of their personal information collected under a United States-originated Order (if they know about it), such challenge would have to take place in the United States under United States privacy law. This is both a significant disadvantage for Individuals and their personal information subject to an Order and erodes another core aspect of Australian privacy law, the right to make a complaint to the Office of the Australian Information Commissioner (**OAIC**) and appeal that decision in the Australian courts under Australian law.

Recommendation 6 **Right to know**

Incorporate a right for the Individual to be notified of the existence of an Order relating to them. The notification should be required to contain basic instructions as to how the Individual can lodge a complaint (see Recommendation 8).

Accountability and oversight

3.26 There is limited accountability or oversight in respect of (a) the issuance and transmission of Orders originating in the United States under the Agreement and (b) once the information is repatriated to the United States. While minimisation principles have been incorporated into the Agreement, it is not clear who or what provides any assurance that these principles have been observed. The history of privacy complaints to the OAIC is evidence that organisations/agencies often do not always comply with their privacy obligations unless required to do so by the regulator.

3.27 While the Agreement incorporates an obligation to implement targeting procedures (to limit what data is collected),[8] again there is no accountability or oversight (or 'umpire') in respect of how 'appropriate' such targeting procedures are.

3.28 While the Agreement incorporates procedures for minimising the acquisition, retention and dissemination of information,[9] there is no accountability or oversight in respect of how 'appropriate' or effective such minimisation procedures are and what is done with any information that is not relevant to or outside the scope of the relevant law enforcement activity.

3.29 Further, consideration is required into the roles of Australian and United States Government agencies in the administration of the provisions of the Agreement and what independent oversight there is over the issuing of Orders under the Agreement and what mechanism should be adopted.

Recommendation 7 **Public interest monitoring**

Appoint an independent public interest monitor (**PIM**) or similar with the role of providing oversight and reporting on the use of the Agreement. The PIM should have the power to make applications and oppose the transfer of information on public interest grounds. This is not a role that can be played by the 'Australian Designated Authority', as contemplated by the IPO Act, due to the inherent conflict of interest (i.e. playing both 'coach' and 'umpire').

The PIM should also have a role to play in a complaints mechanism under the Agreement (see Recommendation 8).

[8] Art 7.1.
[9] Art 7.2.

Recommendation 8 **Complaints mechanism**

The Agreement and IPO Act should have a complaint mechanism to facilitate enhanced accountability, procedural fairness and public confidence in the regime. The PIM should have a role to play in this complaints process.

Recommendation 9 **Annual reporting**

Each of Australia and the United States should be required under the Agreement to prepare a report for publication addressing the number of Orders issued by that party, the purpose(s) for which they were issued, the number of individuals impacted by the Orders, the number of challenges/objections and a summary of the outcomes of those challenges/objections and the purposes for which the data transferred was used.

The death penalty

3.30 Broadly, Australia and the United States have long-standing opposing views on the death penalty. Excluding the use of information transferred from Australia under a United States-originated Order for prosecuting individuals where the death penalty is sought by way of two one-page letters, rather than incorporating the exclusion into the Agreement itself, is not satisfactory given the gravity of this issue.

3.31 We do not consider that these letters provide a meaningful 'guarantee' as to the prohibition on the use of information transferred under the Agreement in death penalty cases.

Recommendation 10 **Death penalty prohibition**

Incorporate the death penalty prohibition into the body of the Agreement.

Freedom of speech

3.32 Broadly, Australia and the United States differ on freedom of speech and the instances in which it can be justifiably curtailed (e.g. prevention of hate speech). The two letters between Australia and the United States addressing this issue (for Australia-originated Orders) create a significant barrier for Australian law enforcement seeking to obtain information under the Agreement to prosecute individuals who may have committed an offence under Australian law on the grounds that this would raise 'freedom of speech' concerns in the eyes of the United States.

3.33 This problem is amplified due to the greater volume of electronic data stored on cloud servers in the United States as compared to the volume stored in Australia. That is, if Australian law enforcement cannot use evidence gained under Orders issued pursuant to the Agreement and delivered to service providers in the United States to prosecute hate speech, for example, then this will severely limit their ability to prosecute such and, contrary to Australian law, introduce or at least support a level of US-style 'free speech' that allows certain conduct that, as a society, Australians have sought through our Parliament to eliminate.

Termination rights in practice

3.34 The Agreement requires each of Australia and the United States to advise the other party where there are material changes in their domestic laws that would 'substantially frustrate or impair the operation of this Agreement'.[10] Arguably, this is a high threshold to meet and subjective to the country whose laws a changing.

3.35 Moreover, a country may fail to tell the other about a material change in its domestic laws.

[10] Art 3.1.

3.36 While either party may then exercise the termination right on receipt of such advice from the other party, it is not clear how effective this will be to protect Australia's and Australians' interests should the regulatory, political or cultural landscape evolve in the United States.

Recommendation 11 Reporting

Require each of Australia and the United States to provide a report to the other detailing all new, amended or repealed laws (directly or indirectly) impacting on the matters which are the subject of the Agreement.

Retrospective application

3.37 The Agreement can be used to facilitate the transfer of data relating to an offence committed before the Agreement came into force.[11]

3.38 Australia's strong and proud common law tradition, which is a central pillar of our society, disapproves of retrospective criminal laws.[12]

3.39 While the Agreement only permits use of the Agreement to facilitate the transfer of data on or after the Agreement's entry into force, it should not permit such use in relation to offences committed prior to the Agreement coming into force.

Recommendation 12 Retrospective application

The Agreement should be varied to remove Article 14.

4 A further remark

4.1 In preparing this submission we were unable to identify any study or 'gap' analysis of the differences in relevant laws (including as to privacy) between Australia and the United States. We hope that such a study/analysis was undertaken prior to Australia signing the Agreement and urge that these be made public. At the very least (and as required by all Australian Government agencies), we expect that a PIA by an independent entity was carried out and urge the PIA report to be published.

4.2 Although laws may change in the future (and the United States is required under the Agreement to notify Australia of changes to its laws materially impacting the Agreement), it is important that a study/analysis or PIA is conducted prior to entering into/ratifying the Agreement to obtain assurance of and as a starting level for interaction between the laws of Australia and the United States as facilitated by the Agreement.

5 Sources considered

We considered the following materials in preparing this submission.

(a) Department of Home Affairs. *Agreement between the Government of Australia and the Government of the United States on Access to Electronic Data for the Purpose of Countering Serious Crime – Regulation Impact Statement*. https://www.homeaffairs.gov.au/nat-security/files/cloud-act-agreement-signed.pdf

(b) The Office of Best Practice Regulation. (2022, January 28). *Agreement between the Government of Australia and the Government of the United States on Access to Electronic Data for the Purpose of Countering Serious Crime (AUS-US CLOUD Act Agreement)*. https://obpr.pmc.gov.au/published-impact-analyses-and-reports/agreement-between-government-australia-and-government-united

[11] Art 14.

[12] Australian Law Reform Commission. (2016, January 13). A common law principle. ALRC. https://www.alrc.gov.au/publication/traditional-rights-and-freedoms-encroachments-by-commonwealth-laws-alrc-report-129/13-retrospective-laws/a-common-law-principle-12/.

(c) Parliamentary Joint Committee on Intelligence and Security. (2021, May). *Advisory Report on the Telecommunications Legislation Amendment (International Production Orders) Bill 2020*. Parliament of Australia. https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/IPOBill2020/Report

Yours sincerely,

[redacted]

Michelle Falstein
Secretary
NSW Council for Civil Liberties

Contact in relation to this submission: Michelle Falstein
[redacted]