Eric Wilson
[redacted]

23 April 2020

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
Parliament House
Canberra ACT 2600

Dear JCIS members,

Re: Inquiry into the Telecommunications (Interception) Amendment Bill 2020

Thank you for an invitation to make a submission on this important legislation.

As described in my submissions to a previous enquiry on this subject[1], I am a software developer in the communications industry, who creates IT systems. I also run a start-up company, which for technical reasons, has cloud services system components operating in Australia and overseas.

Introduction

The Minister's Memorandum represents that Part 13 of the proposed Schedule 1 to the TIA (allowing foreign access to information stored in Australia) places no obligations on Australian service providers under Australian law[2]. This is despite the word "order" being extensively used in Part 13, even in it's heading. This is strange, since the Memorandum speaks of reciprocal arrangements with foreign countries and the bill provides for International Production Orders to be placed upon communications service providers overseas by Australian law enforcement authorities.

However, the Minister's letter of referral to the Chairman speaks of Australian communications providers responding to orders from a foreign country, and that the Committee should make its report quickly so we can partner with the United States under its Clarifying Lawful Overseas Use of Data Act ("U.S. CLOUD Act"). The inconsistency between the Memorandum and the Minister's letter may perhaps be resolved by Part 13 being described in the Memorandum as "part of the framework". Part 13 therefore seems to be part of a much bigger legislative scheme which the Australian public has not yet been informed about in a coherent manner. So here goes...

Section 2523 of the U.S. CLOUD Act referred to by the Minister provides powers to the executive government of the United States to enter into agreements with other countries. By the sound of his letter the Minister wants an agreement to be reached under this before the U.S. elections in November – tricky but doable I would say. The purpose of the U.S. CLOUD Act is to provide authorised countries power to order direct access to stored data in the United States, but only concerning non-US persons including non-US corporations. It is a requirement of the U.S. CLOUD Act that countries with whom agreements will be made (e.g. Australia) can demonstrate compliance with human rights. Reciprocal rights of data access are also required, which expressly includes the removal of any obstructing privacy law. However, it also prohibits the forwarding of information supplied under a production order, including it circling back into the United States.

1 I made two submissions to the Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018
2 See General Outline, item 8 of the Minister's Memorandum

Therefore the U.S. CLOUD Act provides a much better view of what this bill is about than the Minister's Memorandum. I believe it fair to say the bill is part of a legislative scheme, some parts of which have been enacted, some parts of which are yet to be revealed. The minimum we can assume is that the bill intends by the word "order" in part 13, for Australian communications service providers to have "production orders" (a U.S. CLOUD Act term) served on them directly by U.S. law enforcement and intelligence agencies. The United States reportedly entered into an agreement with the United Kingdom in October 2019, meaning the bill is probably intended to also allow orders from U.K. counterparts upon Australian communication services fairly soon too. However from my reading of the bill, a lot more needs to be done to get it into shape within the Minister's desired timeframe...

On it's face however, the bill countenances unspecified foreign governments directly ordering Australians to allow access to the private and confidential information of other Australians and foreigners. The bill fails to prohibit this as the U.S. CLOUD Act does in relation to the United States people, indeed part 13 would tend to help enable the escape of Australian intellectual property attached to emails for example. The major difference is a request by Australian authorities for information held in the U.S. about U.S. persons remains in the existing framework of mutual cooperation and not the U.S. CLOUD Act direct order system. International Production Orders (IPOs) directed to the U.S. can therefore be only about people residing outside the U.S. who are not U.S. citizens or companies (18 USC §2523(a), (b)(2), (b)(4)(A)&(B)) In this submission, I will therefore proceed on the basis of the unspecified open-ended nature of the proposed law of the Commonwealth (which needs amending) rather than the more restrained law of the United States; while keeping in mind the Minister's intention to somehow integrate a U.S. CLOUD Act agreement into it.

Although not entirely clear, it's also envisaged by the Memorandum that the new law is intended to provide the equivalent of an "underlying authorisation"[3] – so that a compulsory Technical Assistance Notice or a Technical Capability Notice could be served.[4] So the bill is the part of a legislative scheme which if valid, could require me to change my company's software at the behest of foreign powers! That is not good.

Part 13 is silent on what future government agreements, intended to be mentioned in the regulations, will allow foreign countries to put into their International Production Orders (or equivalent). This is critical, because *at least 15 provisions of the bill, many providing the most substantive and intrusive parts of its operation, turn on the contents of future unknown agreements*[5]. This is why it is so important to put a human rights framework around the decision-making *and the agreement-making process* as the U.S. CLOUD Act does well. The bill before the House on the other hand, needs to be improved to match this kind of integrity, as the U.S. CLOUD Act itself requires (18 USC §2523(b)(4)(B)).

For it's clear IPOs intended by the bill to be served on Australian service providers would not only be 'intercepts' sent to foreign police and others, but also coercive notices to produce historical records. Many if not most of these will be messages and attached documents sitting in storage in encrypted form to be accessed by foreign law enforcement from time to time. So if I were a foreign police chief, I would insist my country gets at least what the Commonwealth seeks to extract for our law enforcement agencies' use. Indeed, the Minister's memorandum states the bill's intention of

3 See point 8 of the Statement of Compatibility with Human Rights in the Minister's Memorandum.
4 By virtue of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018.
5 See section 4 2BBA(g)(m) of the bill, sections 1, 3, 21, 22(2), 31(3)(d), 33(2), 42(2), 49(3)(d), 51, 52(2), 63(2), 72(2), 82, 83(2), 92(2), 101(2), 120, 121, 128(g), 130(a)(g), 134(1)(c)(ii), 136(1)(c)(ii), 138(1)(a)(iii)&(e)(iv), 138(2), 139(2)(g), 167, 168 and 169 of proposed Schedule 1 to the TIA

allowing reciprocal arrangements as the U.S. CLOUD Act requires. Therefore in this submission I assume the other parts of proposed Schedule 1 to the TIA intended for Australian authorities to use, contain roughly the scenario for incoming IPOs hoped to be served by foreign agencies upon Australian service providers.

Without discounting the Minister's need for speed, as part of the legislative scheme, this bill suffers from four key problems which I believe should not be hastily overlooked:

- The unlawful conflation of ordinary State policing powers with national security powers which require substantially different tools and safeguards.

- Adoption of a controversial policy, that more and more backdoors inserted into civilian IT systems actually improves national security.

- That police matters don't require warrants issued by judges merely because the evidence is held in electronic form.

- That we can somehow allow foreign countries to issue orders to access our information unsupervised without compromising our sovereignty and economy (i.e. goes beyond the U.S. CLOUD Act).

I shall quickly summarise some main concerns before explaining the outcomes in detail and offering what I believe are practical solutions the Committee may wish to consider:

Inconsistent with 18 USC §2523(b)(4)(d)(iii) of the U.S. CLOUD Act, the bill as part of a 'framework' seeks to allow State police forces to go jurisdiction-shopping, presumably to Five Eyes jurisdictions for information. In so doing, the bill bypasses State legislation and State Courts where civilian privacy and confidentiality is better protected and mass surveillance prohibited. In this regard I cannot accept that section 34 of the Telecommunications Interception Act 1979 (Cth) can override the will of State Parliament Acts relating to warrants controlling State law enforcement agencies. Here's why, as I see it:

The Constitution and the Australia Acts 1986(Cth)(Imp) keeps Commonwealth and State Executives separated regarding control of law enforcement agencies except under section 119 in relation to domestic violence *against the State* with State Premier consent. But terrorism has been referred to the Commonwealth by Victoria (an other States). So for the bulk of Victorian criminal law offences, and for all offences investigated by Victorian authorities, section 15 of the Surveillance Devices Act 1999 (Vic) applies, requiring a judge or magistrate to issue a warrant. This Act binds the Crown in all capacities, thereby restraining the Premier also from entering into any agreement with the Commonwealth to the contrary. And the *exemption from penalty* for the police does not constitute a clear State *authorisation* for State police to use Commonwealth warrants[6]. Moreover the effect of section 34 is to bypass the Supreme Court of a State protected by the Constitution.

Therefore the bill should amend section 34 of the Telecommunications Interception Act 1979 (Cth) ("TIA") to also require an authorising <u>State Act</u> to use Commonwealth authorisations and warrants. To be clear I believe this issue only concerns outgoing IPOs from State governments.

6 Coco v R [1994] HCA 15; (1994) paras 8-12; Smethurst v Commissioner of Police [2020] HCA 14 (15 April 2020) 118-120

But at the heart of this legislative scheme beats a lie, which is also expressly incompatible with 18 USC §2523(b)(3) of the U.S. CLOUD Act. The lie is that encryption can be bypassed without creating systemic weaknesses. Our security services believe the risk of nefarious infiltration can be mitigated by IT management. This false assumption will be exposed later in this submission. However the U.S. CLOUD Act forbids agreements with countries that either limit decryption or require decryption capabilities. An acceptable compromise may be to ***implement encryption bypasses as installable /uninstallable hardware / software components, with coercive use being very rare and executed in a confined way, then uninstalling immediately so as not to disrupt U.S. CLOUD Act production orders.*** In that case, I believe the Commonwealth must be prepared to compensate since implementation would be non-trivial in many situations.

The bill also unreasonably expects AAT solicitors with little tenure or independent income, and perhaps no criminal law experience, to be up to assessing urgent applications pressed over the phone by senior law enforcement officers. Yet since my submissions of 2018 I have reconsidered and am now in favour of AAT hearings – I have read a very powerful dissenting judgement in the High Court arguing to keep the judiciary out of the law enforcement process and I now agree with that. However, 18 USC §2523(b)(4)(D)(iv) of the U.S. CLOUD Act requires judicial reasoning regarding "reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation"; Thus I believe ***AAT hearings must be conducted by senior people with <u>relevant experience</u> able to hold their ground, and difficult cases – such as whether to coerce decryption capability – being decided by two such members.***

The legislative scheme if enacted, would enable unsupervised trawling through this nation's correspondence (if utilised beyond the U.S. CLOUD Act) by foreign investigators – even if only to clear people's name – on the basis they would never pass on invaluable intellectual property and commercial secrets to their own nation's industry. Please wait a minute while I beat my head against my desk… Thanks, that feels much better now - no disrespect intended. I think a reasonable way to protect Australia's economic interest would be to ***prohibit outbound data transfers of non-Australian material as envisaged by 18 USC §2523(b)(4)(A)(B)(I) of the U.S. CLOUD Act.***

Yet even if it's true that more and more backdoors into IT systems will prevent and not enable crimes, with police and spies having common powers and fewer safeguards, informing foreign governments of our private information without sufficient supervision – supposing all this is good – this bill still has very serious shortcomings. In summary, even on its own terms, I believe the proposed law if passed without amendment, would create a technical and legal train wreck:

1. Systemic weaknesses in Australia's IT systems against national security
2. Incompatible with Minister's human rights statement
3. Opens a door for mass-surveillance
4. Improper conferral of judicial power upon ADA, AAT or justices in person
5. Acquires access / use of third party systems on unjust terms
6. Overreach into storage

Yet I think there are solutions to these serious problems available within the time frame if the Department gets on to it. So after examining the bill I will discuss its implications more broadly and conclude with a list of recommendations:

Systemic weaknesses in Australia's IT systems against national security

A person receiving an International Production Order under the proposed law would often be unable to comply except by circumventing encryption or other secure storage so as to provide 'material' such as 'text' as distinct from 'data' as the Schedule specifies[7]. The effect of this would impact service providers around the world who would struggle to meet the proposed requirements of such International Production Orders.

The implied requirement follows our security services' deeply flawed idea that more and more backdoors (covert access controls) will provide more and more security – see the bill's definition of 'access' for example[8]. This proposition assumes backdoors won't be infiltrated by malicious actors using seduction or intimidation, which of course they will be over time. For once installed, the proposed law doesn't mandate any backdoor removal, which can be operationally difficult to do. And it's cheaper to be ready for the next time, isn't it?

CASE STUDY: ***Folly of privileged government access***

Manning

Snowden

From 2010 onward, Chelsea Manning leaked 750,000 classified documents to Wikileaks, while in 2013 Edward Snowden leaked about 1.5 million secret documents to media outlets. Both worked for the U.S. government, Manning was a soldier, Snowden a contractor.

Of course in IT there's always a trade-off between convenience and security. Yet it's surprising Five Eyes governments had not prior to these leaks developed their own encrypted document management systems and deployed them widely. For even in 2003, granular document encryption became widely available to civilians in Microsoft Office to protect against such leaks. (Even in 1999, widely available application hosting, similar to Windows Remote Desktop, could have been used to greatly reduce file access to sensitive materials.) Such is designed to prevent documents being opened outside their network environment, removing bulk access or rendering it useless.

Unfortunately, governments have been slow to adopt encrypted document technology. Also, document conversion of existing information into encrypted form on such a vast scale is expensive. This meant IT management using access controls, such as network/file system permissions, instead of document encryption, remained a primary means of security for sensitive materials in many government organisations.

But humans have always been the weakest link in IT security, so it was only a matter of time before disgruntled persons with powerful access privileges made off with classified material. Yet had the documents all been encrypted, it's very likely neither Manning nor Snowden would have bothered misusing their access privileges, as there would have been little point.

This example demonstrates how access control offers very poor protection when a bad actor gains influence over a network administrator or becomes a network administrator, or highly privileged user – despite some regarding Manning and Snowden as heroes. But by now, everyone should agree, that routinely creating backdoors into encrypted information to provide access controls for government is a sure-fire way to repeat the Manning and Snowden disasters. Both of them worked for government security services and were considered trustworthy. They prove that putting more and more backdoors into IT systems for government access guarantees a degradation of security across the nation, by providing great opportunities for infiltration by adversaries.

Creating access controls to undermine encryption, then giving that access to foreign powers is national security suicide. The U.S. CLOUD Act strongly discourages it – see 18 USC §2523(b)(3).

7 See section 2, definitions of "message" and "materials" in section 2 of proposed Schedule 1 to the TIA

8 proposed Schedule 1 to the TIA, section 2 "access" (a) of the bill specifies *"access that is subject to a pre-condition (for example, the use of a password)"* – meaning backdoors to encrypted and/or securely stored text, voice, video etc.

So while the proposed law may provide a sugar-hit for short-term law enforcement, Australia may pay a very heavy national-security price as backdoor priveliges are inevitably compromised. Indeed, the proposed law makes no attempt to provide even the troublesome 'no systemic weakness' protection for Australia that the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* tries to create. This bill in its current form should therefore be rejected on national security grounds, notwithstanding ASIO's present views. Instead, ***the amendments should prioritise access, with temporary encryption circumvention only available in case of the highest-priority cases, which access mechanism must be quickly removed after each authorised use at Commonwealth expense.***

CASE STUDY:
Compromise of Australia's civil defence

Australia's 'sea lanes' to the rest of the world concern more than just shipping. Internet connections presently rely on undersea cables stretching thousands of kilometres. The ADF would be hard pressed to defend our data links from severance by hostile submarines. In this event, it must be assumed that civilian communications with the United States will be disrupted. Then access to U.S.-based code repositories will become limited or nonexistent for maintaining civilian IT infrastructure.

This problem would be difficult yet manageable if it were not for the Commonwealth's encryption bypassing laws. Since these were passed, I have noticed code repositories disappearing from our shores, probably because repository maintainers are well-informed about the perils of compromising encryption with backdoor privileges. As Australian-based code repositories disappear, updates to our systems relying on open source infrastructure simply break, leaving un-patched systems more vulnerable to potential adversaries.

So, where Australia's IT management detects this, it often gets around the issue by pointing our systems to update directly from U.S. servers instead: Houston we have a problem… how big? No one knows. There are reports that sometimes half of Microsoft's commercial data centre loads consists of application stacks containing substantial amounts of open source software; commercial loads on Amazon Web Services probably more so. And there are thousands of Australian companies who have their own open software stacks ranging from small servers in the corner to corporate data centres. I believe many of these now would have private repositories pointing to the United States for distribution to multiple internal systems here. Others have broken update routines and they don't even know. Many organisations will have a mixture of U.S. reliant and non-updating systems.

Back in the old days, before Australia's encryption bypassing laws, updates to repositories in places like universities could quickly replicate fixes across the nation to mitigate an ongoing attack. In an emergency, overseas links to obtain updates to these master repositories could have been quickly supplied through more robust military channels. But now, repositories might need to be set up in a hurry (a civil-defence capability we need to practice anyway) and critically, every open software stack will eventually need to be touched in multiple places to point to the new repositories. There probably aren't enough knowledgeable hands on keyboards in Australia to do this swiftly and comprehensively in an emergency. Therefore I believe the disruption of access to U.S. repositories we must expect during hostilities if they arise, will have a far greater impact than it otherwise would.

The bill's intended effect of allowing interception of Australian communications for production in the form of text to foreign agencies only perpetuates this chilling of open software repositories in Australia. This is because software developers and repository maintainers in this country may not be free to express their code in the most secure way possible. This discourages security software development here – we will not be able to fix things quickly ourselves. This might not only make defence production more open to cyber attack, but also create civilian supply chain issues taking much longer to resolve. This is all bad news for the civil defence of Australia. Making ourselves dependant on open software repositories in the United States, and thus more vulnerable to undefendable submarine attack, is as silly as say, basing our fuel reserves overseas… Wait, did I say something wrong?

Incompatible with Minister's human rights statement

The bill does not comply with the Minister's human rights standards set out in his Explanatory Memorandum. In some cases, the Minister has not considered the full extent of the bill in a human rights context critical to Australia's international reputation and the requirements of the U.S. CLOUD Act (discussed shortly). Also, as will be discussed, the failure of the proposed law to meet the Minister's standard of human rights would directly impact the utility of Australian communications providers to international customers, and the export of services contributing to Australia's national income.

The following tables below outline where the Minister's human rights standards and the bill's implementations do not match. The first table sets out human rights incompatibilities regarding both incoming and outgoing IPOs ("All Production Orders"). The second table relates to incoming IPOs (collecting data for foreign governments) only. The latter is relevant to the U.S. CLOUD Act too, because how Australian communication providers may be compelled to share information with other countries law enforcement agencies, which may relate to U.S.-persons, is important to the United States. I have compiled the tables on the Minister's terms irrespective of the validity or merits of what is proposed:

MINISTER'S HUMAN RIGHTS STATEMENT ALL PRODUCTION ORDERS		
	MINISTER'S STANDARDS	**BILL'S IMPLEMENTATION**
	Likely to assist the detection … of an offence which either carries a maximum penalty of at least 7 years imprisonment… or a series of listed specified other offences – item 12	Allows for a 3 year maximum term for unspecified offences concerning stored data, without justifying why stored data engages human rights less than intercepted data – see section 39(2)(d). **Minister's threshold not met.**
	Where there are other methods to access information less intrusive on privacy, the agency may be required to turn to those means instead of seeking an IPO – item 15	Minister's remarks for avoiding use of IPO do not relate to data storage IPOs – compare section section 39(3) with 5(f) & 6(f) **Human rights not fully considered.**

It is a requirement of 18 USC §2523(b)(1)(B) of the U.S. CLOUD Act that strong human rights protections are demonstrated by participating countries outside of the agreement negotiated with them. But except for anti-discrimination law and political freedom, it seems to me only Victoria and the ACT have suitable human rights enactments. Therefore leaving some of these considerations out of the Commonwealth's enabling legislation may cause the agreements to be rejected by U.S. Congerss during the 180-day review period (18 USC §2523(d)(2)). And the Minister is no doubt aware that a lurch to the left is possible in the wake of the pandemic there. It is therefore important that the bill adresses all the human rights areas the U.S. CLOUD Act requires. Furthermore, the Minister's standards set out in his Explanatory Memorandum need to be implemented not only for outgoing but also incoming orders to produce information collected in Australia. Therefore the following table is in addition to the above:

MINISTER'S HUMAN RIGHTS STATEMENT INCOMING INTERNATIONAL PRODUCTION ORDERS		
	MINISTER'S STANDARDS	**BILL'S IMPLEMENTATION**
	It's about criminal investigations and prosecutions – item 2	*Regarding incoming IPOs:* Also may include ongoing monitoring for control order supervision since this is the case with outbound IPOs: – see section 1 **Human rights not considered.**
	To more efficiently acquire data held in a foreign country – item 3	*Regarding incoming IPOs:* The bill also countenances exports of people's information held in Australia for use in unspecified countries – too broad to meet legality requirement. Allows voluntary disclosures by communications service providers without any protections for targets whatsoever. – see Part 13 **Human rights not considered.**
	No interference can take place except as authorised under domestic law – item 6	*Regarding incoming IPOs:* Is only a law for the negotiation of arbitrary agreements to be adopted by regulation – see 3(1)(3)(4), 182 of proposed Schedule 1 to the TIA. Does not prescribe minimum contents of such agreements – does not meet legality requirement. **Minister's standard not met.**
	Interference with privacy must be in accordance with the provisions – item 6	*Regarding incoming IPOs:* Is only a law for the negotiation of agreements to be adopted by regulation – see 3(1)(3)(4), 182 of proposed Schedule 1 to the TIA. Does not prescribe minimum contents of such agreements. **Minister's standard not met.**
	Must be proportionate and necessary in the circumstances – item 6	*Regarding incoming IPOs:* Is only a law for the negotiation of agreements to be adopted by regulation – see 3(1)(3)(4), 182 of proposed Schedule 1 to the TIA. Does not prescribe minimum contents of such agreements. **Minister's standard not met.**
	Tools they need to keep Australians safe – item 7	*Regarding incoming IPOs:* May also be used as tool by foreign powers against their citizens – see 3(1)(3)(4), 182 of proposed Schedule 1 to the TIA – does not meet legality requirement. **Human rights not considered.**
	To facilitate the government of a foreign country's access to private communications data, where an appropriate order is in place – item 8	Does not proscribe what is inappropriate for foreign governments to order – is arbitrary. Is only a law for the negotiation of agreements to be adopted by regulation – see 3(1)(3)(4), 182 of proposed Schedule 1 to the TIA. **Minister's standard not met.**
	The Australian Security Intelligence Organisation (the Organisation) to apply for an IPO – item 9.	*Regarding incoming IPOs:* Does not prescribe which foreign intelligence organisations may apply. Limited to Five Eyes? NSA included? CIA uses other provisions? Not enough detail – is not reasonable. Is only a law for the negotiation of agreements to be adopted by regulation – see 3(1)(3)(4), 182 of proposed Schedule 1 to the TIA. **Minister's standard not met.**

MINISTER'S HUMAN RIGHTS STATEMENT INCOMING INTERNATIONAL PRODUCTION ORDERS		
	MINISTER'S STANDARDS	**BILL'S IMPLEMENTATION**
	An interception agency includes, among others, AFP, ACLEI, ACIC, authorised state and territory police forces. – item 10	*Regarding incoming IPOs:* Does not prescribe classes of eligible overseas agencies for interception corresponding to Australian agencies – is not reasonable. Should U.S. EPA be allowed? Just asking. Is only a law for the negotiation of agreements to be adopted by regulation – see 3(1)(3)(4), 182 of proposed Schedule 1 to the TIA. **Minister's standard not met.**
	Control order IPO agency includes the AFP, the ACLEI, the ACIC, and designated state authorities under section 34 of the TIA. – item 10.	*Regarding incoming IPOs:* Does not prescribe classes of eligible overseas agencies requiring control orders corresponding to Australian agencies – is not reasonable. Is only a law for the negotiation of agreements to be adopted by regulation – see 3(1)(3)(4), 182 of proposed Schedule 1 to the TIA. **Minister's standard not met.**
	Only an eligible judge or nominated Administrative Appeals Tribunal (AAT) member may issue an IPO – item 11	*Regarding incoming IPOs:* Does not specify minimum standards of decision-making by foreign countries – is not reasonable. Is only a law for the negotiation of agreements to be adopted by regulation – see 3(1)(3)(4), 182 of proposed Schedule 1 to the TIA. **Minister's standard not met.**
	IPOs no longer than 90 days for interception agencies and control order IPO agencies – item 13	No proscribed limit for incoming IPOs – is not proportional. Is only a law for the negotiation of agreements to be adopted by regulation – see 3(1)(3)(4), 182 of proposed Schedule 1 to the TIA. **Minister's standard not met.**
	In deciding whether to issue an IPO relating to interception, the decision maker must have regard to several matters – item 14	Minister's remarks do not relate to data storage IPOs **Human rights not considered.** *Regarding incoming IPOs:* Does not proscribe regard for any of the matters – is not reasonable and is not proportional. Is only a law for the negotiation of agreements to be adopted by regulation – see 3(1)(3)(4), 182 of proposed Schedule 1 to the TIA. **Minister's standard not met.**
	Where there are other methods to access information less intrusive on privacy, the agency may be required to turn to those means instead of seeking an IPO – item 15	*Regarding incoming IPOs:* Does not proscribe regard for less intrusive means – is not proportional. Is only a law for the negotiation of agreements to be adopted by regulation – see 3(1)(3)(4), 182 of proposed Schedule 1 to the TIA. **Minister's standard not met.**
	The decision maker must consider the gravity of the conduct concerned – item 16.	*Regarding incoming IPOs:* Does not proscribe gravity of conduct consideration – is not reasonable. Is only a law for the negotiation of agreements to be adopted by regulation – see 3(1)(3)(4), 182 of proposed Schedule 1 to the TIA. **Minister's standard not met.**
	For an IPO relating to control orders, the decision maker must also take into account the likelihood that a person will breach a control order – item 16	*Regarding incoming IPOs:* Does not proscribe likelihood of breach consideration – is not proportional. Is only a law for the negotiation of agreements to be adopted by regulation – see 3(1)(3)(4), 182 of proposed Schedule 1 to the TIA. **Minister's standard not met.**

MINISTER'S HUMAN RIGHTS STATEMENT INCOMING INTERNATIONAL PRODUCTION ORDERS		
	MINISTER'S STANDARDS	**BILL'S IMPLEMENTATION**
	For IPOs relating to control orders, the decision maker must consider whether intercepting communications would be the method that is likely to have the least interference with any person's privacy - item 17.	*Regarding incoming IPOs for control orders:* Does not proscribe least-intrusive appropriate means – is not proportional. Is only a law for the negotiation of agreements to be adopted by regulation – see 3(1)(3)(4), 182 of proposed Schedule 1 to the TIA. **Minister's standard not met.**
	Once the Attorney-General's consent is obtained, the Organisation may then apply to a nominated AAT Security Division member for an IPO – item 18.	*Regarding incoming IPOs for foreign intelligence organisations:* Does not proscribe Attorney General-level sign off. Is only a law for the negotiation of agreements to be adopted by regulation – see 3(1)(3)(4), 182 of proposed Schedule 1 to the TIA. **Minister's standard not met.**
	The extent to which information gathered is likely to assist the Organisation in carrying out its functions – item 19.	*Regarding incoming IPOs for foreign intelligence organisations:* Does not proscribe functional criteria like the ASIO Act – is not reasonable. Is only a law for the negotiation of agreements to be adopted by regulation – see see 3(1)(3)(4), 182 of proposed Schedule 1 to the TIA. **Minister's standard not met.**
	An IPO in response for the Organisation can be no longer than 6 months – item 20.	*Regarding incoming IPOs for foreign intelligence organisations:* Does not proscribe any time limit – therefore is not proportional. Is only a law for the negotiation of agreements to be adopted by regulation – see 3(1)(3)(4), 182 of proposed Schedule 1 to the TIA. **Minister's standard not met.**
	Less intrusive method is then weighed against its effectiveness and potential to prejudice the Organisation – item 21.	*Regarding incoming IPOs for foreign intelligence organisations:* Does not proscribe any balance between intrusiveness and prejudice – therefore is not proportional. Is only a law for the negotiation of agreements to be adopted by regulation – see 3(1)(3)(4), 182 of proposed Schedule 1 to the TIA. **Minister's standard not met.**
	Ministerial Guidelines that the Organisation's actions should be proportionate to the gravity of the threat and probability of occurrence, and with as little intrusion into privacy as possible – item 22.	*Regarding incoming IPOs for foreign intelligence organisations:* Does not proscribe any balance between gravity, probability and privacy – therefore is not proportional. Is only a law for the negotiation of agreements to be adopted by regulation – see 3(1)(3)(4), 182 of proposed Schedule 1 to the TIA. **Minister's standard not met.**
	The decision maker has discretion to seek additional information from the relevant agency to further inform their assessment of the application – item 23.	*Regarding incoming IPOs:* Does not require any discretion for obtaining further information, therefore is not reasonable. Is only a law for the negotiation of agreements to be adopted by regulation – see 3(1)(3)(4), 182 of proposed Schedule 1 to the TIA. **Minister's standard not met.**
	"Of chief importance", a decision maker is restricted from issuing an IPO seeking B-Party interception unless the relevant agency has exhausted all other practicable methods.	*Regarding incoming IPOs:* Does not require any B-party test, therefore is not proportionate or neccesary. Is only a law for the negotiation of agreements to be adopted by regulation – see 3(1)(3)(4), 182 of proposed Schedule 1 to the TIA. **Minister's standard not met.**

In addition to human rights considerations, the CLOUD Act has a rule of law requirement. But the proposed law makes no distinction between rule-of-law, rule-by-law, sharia-law, one-party-rule or marshal-law jurisdictions as potential recipients of Australian-based messages and material. This means service provider reputation and goodwill created by their decision to come under Australia's highly-respected pluralistic rule-of-law, would be compromised, since the proposed law fails to implement a double-criminality standard. Potentially, orders could be made to assist investigations into publications of true and correct facts criminalised merely for causing some dishonour[9] or causing some religious disharmony[10]. Freedom of speech is also a requirement of the CLOUD Act (18 USC §2523(b)(1)(E), 18 USC §2523(b)(1)(B)(iii)(III)) which the proposed law does not address relating to incoming orders from non-U.S. countries, even relating to U.S. nationals.

I believe introducing the double-criminality standard as as one of the 'gravity' of conduct tests would help solve the incompatible crimes problem. The present lack of the double-criminality standard means online offerings based in Australia could be considered by many as low-integrity services, the servants of foreign powers; for the 3-year maximum or more prison threshold[11] is unreasonable and disproportionate because it admits into the legislative scheme all sorts of conduct that Australians don't regard as criminal.

Another aspect of the bill needing improvement is that there is little mention of factors going to the strength of the allegations behind an IPO application. The CLOUD Act requires that allegations be credible. Yet the level of credibility of allegations – such as reasonable suspicion or probable cause, are not part of the bill. To my mind this is a glaring omission.

SCENARIO: Obstruction of Congress

Obstruction of Congress includes persuading witnesses not to testify at a Congressional hearing – maximum penalty 30 years imprisonment under 18 U.S.C. 1512(b). This would be regraded as a 'serious offence' under the proposed law. So long long ago in a galaxy far far away…

A U.S. President was accused of "high crimes and misdemeanours" based on allegations made anonymously from within his administration. White House officials were also subpoenaed despite claims of a fishing expedition. The President considered it a kangaroo court. But the opposing party constructing articles of impeachment regarded the House of Representatives' part as a criminal investigation, since the Senate was responsible for the committal hearing 'trial'. Problem was, the investigation was semi-public in an election year, yet cross examinations would be not be allowed for the President to fully defend himself during the investigatory stage. So not wishing to assist, the President claimed executive privilege for all his people, telling them to stay away. In reply, the President was further charged with Obstruction of Congress...

It's obvious that even in rule-of-law jurisdictions, politically-charged investigations can occur. Therefore the bill should specify whether or not an allegation is made in a political context as an assessment criteria regarding the gravity of the conduct involved. This might be a hard call to make but would fortify the decision-maker if it were a listed criteria.

Likewise, political freedom of speech in Australia is protected by the democratic implications of the Constitution. But this is too finer point for practical decision-making in considering the merits of orders in an x-parte application (unknown to those under investigation) in perhaps pressurised

9 See Article 309 of the South Korean Criminal Act providing 3 years imprisonment (with or without hard labour) for defamatory true alleged facts and 7 years imprisonment (with or without hard labour) for untrue alleged facts.

10 See section 298A of the Malaysian Penal Code Act 2015 imposing 2-5 years imprisonment.

11 See definition of "serious category 1 offence" in section 2 and 153(v) of proposed Schedule 1 to the TIA, section 13(5), 39(2)(d) of the bill

circumstances. I believe the applicability of political rights (and religious freedoms if not enacted elsewhere soon) need to be spelt out in the bill, with ***a general human rights consideration for the AAT or eligible judge to take into account.***

Opens a door for mass-surveillance

The Minister's explanatory memorandum designed to have legal effect[12], states the very broad application of the proposed law is to *"assist the detection, prevention, investigation or prosecution of an offence"*[13]. This may be why the bill contains no requirement for reasonable suspicion or probable cause standard that a crime has occurred or even will occur, to obtain authorisation to intercept communications and send the data overseas – for the purpose of *crime pre*vention is *pre-crime*[14]. Nor is there any *requirement* that *incoming orders* supposed to be binding on Australian communications service providers concern particular persons rather than persons in general[15].

However the merits of assisting overseas countries to create surveillance societies are dubious, since both simple and sophisticated means to stay beyond the reach of the proposed law already exist today. These don't require a big adjustment on the part of criminals, yet would have a chilling effect on legitimate freedom of speech (contrary to the intent of the U.S. CLOUD Act – see 18 USC §2523(b)(1)(B)(iii)(III)), plus undermine public confidence in productivity-enhancing online systems that our economy so desperately needs. So ***the bill should not be passed until a standard of suspicion of crime is included regarding police investigations***. This should be allowable under the CLOUD Act – see 18 USC §2523(b)(4)(D)(iv). I also believe the ***'particular person' requirement must be in Part 13 for all incoming orders to Australia; and for outgoing orders tenure of AAT members should be strengthened by those members being judges of the Federal Circuit Court on secondment.***

Improper conferral of judicial power upon ADA, AAT or justices in person

In-line phone tap

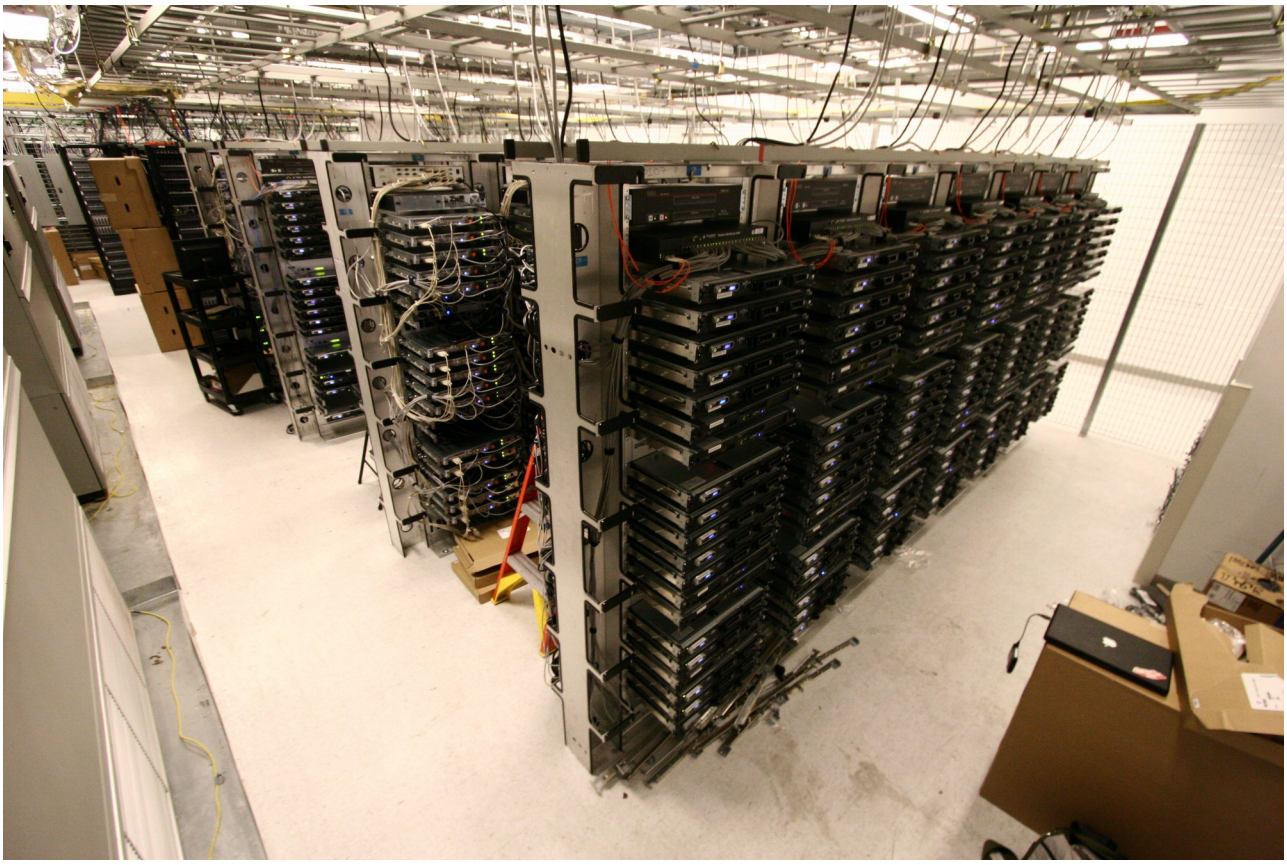
In 1979, when telecommunications interception usually only involved the installation of a 'wire tap' on a 'line' or simple monitoring at an exchange, the communications provider suffered little or no cost or risk to services. Indeed, the Federal Government owned the monopoly carrier anyway, formerly run by the Post Master General (PMG), and subsequently spun off into two Government entities - Telecom Australia and Australia Post. Data was transmitted using electromagnetism over copper wires using analogue modems with acoustic couplers (microphones and speakers). Texts were created by contacting one of Australia Post's call centres or filling out a form at a post office... for telegram transmission to another post office... to be picked up, or delivered by post... or if urgent, read out to the recipient over the telephone. Long text messages were sent over Telecom's phone lines and printed out using a 'telex' machine at both ends of the curcuit.

Yet whichever method of distance communications was used, the *telecommunications services* were controlled by Telecom Australia, the government monopoly, which also owned most connected devices. The first fax standard had not yet been devised; and the Integrated Services Digital

12 See section 15AB of the Acts Interpretation Act 1901 (Cth)
13 See items 12 and 45 of the Statement of Compatibility of Human Rights in Minister's explanatory memorandum
14 This conflicts with section 15 of the Surveillance Devices Act (1999) Vic in relation to forces of the State constitutionally separated from the forces of the Commonwealth in relation to non-violent crime.
15 See Part 13 of proposed Schedule 1 of the TIA Act

Network – a telephone system for data that medium / large companies could afford – was still about 10 years away. The genesis of the Internet was about 15 years away. So the effects of telephone interception on the property, rights and obligations of third parties if any, were negligible.

Today, practically nothing is the same as it was when the *Telecommunications (Interception) Act 1979 (Cth)* was enacted. Whereas in 1979 there was one service provider, in 2020 a multitude of businesses operate their own web sites to communicate materials and messages, each involving layers of other communications service providers to support them. So the vast array of digital services contemplated to be intercepted under the proposed new Schedule, involve vastly more complex interactions and mostly privately owned infrastructures.



Online services infrastructure

This means the associated costs and risks in attempting to circumvent security embedded within such IT systems, and somehow without creating systemic weaknesses, can be substantial. We are no longer talking about just splicing a wire into a line; it's no longer the negligible property rights of unknowing targets at issue, but the very substantial property of service providers upon whose systems the impositions of interception *for foreign governments* would now fall, with thousands and thousandths of orders issuing under a high-volume Commonwealth scheme.

Assisting foreign law enforcement regarding such foreign matters – sometimes miss-classified as serious offences by the proposed law[16] – could in some cases, tend to expose service providers to foreign penalties for conduct otherwise considered acceptable. While it's proposed that the decision-maker would consider the 'gravity' of alleged conduct[17], this only applies for the benefit of

16 ibid page 11, discussion of double criminality standard
17 See sections 30(5)(a)(ii) & (b)(ii), 39(3)(b) and 48(5)(b) of proposed Schedule 1 to the TIA

overseas service providers. The rights and obligations of Australian service providers as opposed to the claims of foreign governments/entities would undoubtedly be in play yet not considered by any Australian body. And in my or my company's case, the proposed law also recognises the public interest in the State of Victoria for the sake of International Production Orders, with a role for the Victorian PID included in such a proceeding[18]. Yet on my reading, anomalously, the Victorian PID would not be involved in an incoming order upon a communications provider in Victoria! That would only make sense if the request did not concern Australian entities as the U.S. CLOUD Act envisages.

Nevertheless, because a proceeding under the proposed law could order substantial interference to a service provider or multiple service providers, the rationale of the High Court's decision in *Grollo v Palmer 1995 HCA 26* seems remote. The reasoning, which regarded permission for telecommunications interception as only an administrative matter not involving controversies between parties and/or governments, was reflective of a much simpler telecommunications era.

But today, it seems the proposed law (the legislative scheme) contemplates civil conscription of people like me to do sometimes complex and risky things to private IT systems on behalf of foreign governments for the execution of their laws beyond the execution of the laws of the Commonwealth – a demand not previously considered by the High Court. At the very least, it's hard to see how the Court's unanimous requirement in *Grollo*, that *"without bias and fairly weighing the competing considerations of privacy and private property on the one hand and law enforcement on the other"*, could possibly be met. For the service provider concerned hasn't been given any opportunity to be heard regarding the order affecting his/her/its property. And the decision is final[19] unless an objection can be raised that the relevant agreement doesn't cover the circumstances of the case.

But the bill goes still further, seeking to also confer a power upon the Commonwealth Executive, to decide for an objecting service provider, if an order issued by the AAT or a judge, conforms to the treaty the Executive has legislated[20].

Repository of the judicial power of the Commonwealth: the High Court of Australia

This last point looks like an intrusion upon the judicial power of the Commonwealth which is vested by the Constitution in the High Court. That's because the Australian Designated Authority would be carrying out a judicial function since it has no discretion to alter the decision of the AAT / judge acting in person on the merits. It can only check to see if the International Production Order falls within the bounds of a treaty. That would be a judicial review not an administrative review. However even if it were an administrative review, it would be difficult to do lawfully, since the Australian Designated Authority charged with reviewing agreement compliance upon the service provider's application, would already have close confidential relations with the foreign government involved, plus a stake in the process running smoothly. How can the Australian Designated *Authority*, not

18 See section 28 of proposed Schedule 1 to the TIA
19 See section 124 of proposed Schedule 1 to the TIA
20 See section 120 of proposed Schedule 1 to the TIA

being independent as the U.S. CLOUD Act would also require, conduct an unbiased and fair hearing?

Thus the proposed law if enacted, could generate appeals or come under challenge, which should be avoided. Therefore, ***agreements to which the proposed law applied should be (a) be assented to by Parliament to be put into force (or in an emergency only, assented to by regulation) and (b) for IPOs and incoming orders, provide for judicial review on the papers (or video conference hearing) by an Australian Court;*** in the case of incoming orders this could be vis-a-vis 18 USC §2523(b)(4)(K) with the Commonwealth as a nominal party to the case.

Such a more conventional system of checks and balances guarding our civil liberties should not be jettisoned. If it needs to operate speedily as the Minister desires, it can and must be very well resourced. There are really no shortcuts to this in my opinion.

Acquires access / use of third party systems on unjust terms

The proposed access to computer systems involves the use of substantial property, and electrical power, under a legislative scheme of the Commonwealth. It seeks to provide the Commonwealth with the benefit of entering into international agreements and discharging its international obligations, plus the benefit to others of providing valuable and hard-to-get information to allow quid pro quo arrangements. But all this is proposed to be at the expense of uncompensated parties[21] such as myself or my company. And the costs may be very significant unless the principles of the U.S. CLOUD Act apply to the bill – not forcing the bypassing encryption – which they currently don't.

Strong IT security has access restrictions deeply embedded within systems precisely to prevent such encryption circumvention as the bill implies. Sometimes changing this, even if lawful and desirable, may well require custom software development, and/or temporary reconfiguration and deployment of components to suit. And this would need to be made more secure again once an order for its compromise is discharged. So it's unjust to expect me or any service provider to bear all the costs of such orders – especially on behalf of foreign powers.

In truth, even the Commonwealth's defence power cannot acquire property (my intellectual property, computer time and access) on unjust terms. So it would seem the bill in its current form breaches section 51(xxxi) of the Constitution by not providing just terms. In my view, ***it's only fair that a foreign Applicant should pay the cost of things compulsorily acquired if the principles of the U.S. CLOUD Act are not applied in the bill.*** The statement in the Memorandum that this bill as it stands, will cost the Commonwealth nothing, is incorrect.

Undermining national sovereignty

It's trite to say the Queen's prerogatives and capacities (and thus the Executive power of the Commonwealth without any authority given by Parliament) cannot give orders to anyone except the public service – unless a foreign invasion is on, or a plague (along side State Executive power).

For this is not like the case of military secondment where a lawful order of a Commonwealth officer is given to a person in the service of the Commonwealth to obey a foreign commander – the Constitution expressly authorises "control" of military forces. Civilians like me on the other hand, can only be pressed into service if a hot war activates the Executive's prerogatives or enlarges

21 See section 2 "designated communications provider"

Parliament's defence power. But this bill is about law enforcement not defence, and Part 13 is about foreign law enforcement at that.

CASE STUDY: Incompatible privacy laws

The investigation into Julian Assange would have certainly come within the definition of serious crimes under the proposed law. But in an alternative universe, would it have been just for Australain communications service providers to automatically hand everything over as the bill intends? Should Sweden be asked to join the IPO club by agreement with Australia?

It's ironic that Jullian Assange, champion of leaks, suffered the Swedish prosecution leaking highly prejudicial material containing salacious allegations against him. Even more astonishing however, was when the Chief Justice of Sweden visited Australia to give a lecture featuring the case of Julian Assange, even while the Swedish investigation dragged on. Despite howls of protest from the Australian Bar, the lecture went ahead in Adelaide under the cover of 'academic freedom'. Attendees we surprised to learn there would be no investigation into the leak from the Swedish prosecution, because in Sweden, laws protecting freedom of speech made any such investigation illegal.

But in the eyes of Australian law this was unjust, because everyone is entitled to the presumption of innocence until proven guilty before a court of law. This means in Australia at least, a person's reputation and honour should never be destroyed by leaky investigations.

Justice requires Australia to scrutinise the laws of jurisdictions proposed to become order isuers upon Australian communications services. Strict constraints on agreements should be imposed by the TIA Act. Currently there are none. But jurisdictions with leaky police investigations should not be given access to Australian communications.

So what this bill proposes instead, is to give the Commonwealth Executive a standing legislative power – a piece of Parliament – supposed to create agreements with foreign countries intended to be able to become binding instruments "in force" in Australian law[22] – simply by mentioning the existence of these agreements in the principal Act's regulations[23]. I understand these agreements to be legislative instruments of themselves because they would form a direct part of the scheme to purportedly command the obedience of civilian service providers - see section 124 of proposed Schedule 1 to the TIA for example.

Thus the bill seeks to provide the Commonwealth Executive with a purported new power to legislate rules by which foreign countries are supposed to issue orders directly to the people of the Commonwealth. It seeks to give the Executive a piece of parliament since the agreements constituting the rules can be amended at any time under section 182 of proposed Schedule 1 to the TIA, apparently without any need to update the regulations subject to Parliament! With respect, there's no way such an unusual arrangement could be covered by the *telecommunications* services power as the bill implies in section 20 of proposed Schedule 1 to the TIA.

22 See section 3(7) of proposed Schedule 1 to the TIA
23 See sections 3(1)(a) and 3(3)(b) of proposed Schedule 1 to the TIA

No legal sovereignty equals no sovereign borders!

It all sounds like this bill leads Australia down the very slippery slope of foreign control; yet I believe that if it were passed in it's current form and challenged, it would be found to be no law at all, commanding no obedience. This is because to the extent a foreign law enforcement agency attempts to execute the laws of the Commonwealth of Australia to order ordinary Australians around, the Commonwealth Executive is not carrying out the executive functions as the Constitution commands in section 61. Furthermore, Parliament's federal powers in section 51 of the Constitution, including the Telecommunications Services power are *"for the… good government of the Commonwealth"* not foreign countries – so Federal Parliament has no "International Production Order" power it could delegate to the Commonwealth Executive for it to legislate so that foreign powers can give orders to Australians, nor Australians to give orders to foreign powers. For Parliament's telecommunications services power is incapable of either ceding or taking national sovereignty.

Even if all this were not so, foreign public services are not subject to the Constitution of Australia, such as to the manner of appointment of public servants(s) (s116) nor to the High Court's jurisdiction (s71 & 75), and therefore cannot constitutionally act as order-issuing authorities under a law of the Commonwealth. The High Court is known to be particularly jealous of its judicial powers of administrative review in this regard.

Therefore I believe that while most of the proposed law may fall within the bounds of Commonwealth power, it does not fall within the bounds of the Executive Power of the Commonwealth acting alone legislating amendments to agreements in force. By way of comparison, the US CLOUD Act sets out a very detailed legislative approval process to avoid such issues in the United States, and to perhaps set a good example – see Act 18 USC §2523(d).

The bottom line is, the highest a foreign power can do on its own to order around ordinary Australians in Australia is (a) submit an extradition request to take the person to their jurisdiction or (b) request a competent Australian authority to make the order for them according to Australian law. Either way, I think it must be competent Australian authority that does the ordering. Thus I believe the answer to the sovereignty problem is similar to that of the judicial power issue:

- ***The agreements (including any amendments) with foreign countries should be approved by the Parliament;***
- ***A Commonwealth body should apply Australian executive power to incoming orders to execute the law of the Commonwealth;***
- ***Provide for judicial review on the papers (or video conference hearing) by an Australian Court;*** *in the case of incoming orders* vis-a-vis 18 USC §2523(b)(4)(K) with the Commonwealth as a nominal party to the case.

For in the end, security that sacrifices national sovereignty is no security at all.

Overreach into storage

My view is incoming "orders" for stored material is not properly a telecommunications issue. This is because in section 182 of proposed Schedule 1 to the TIA, the bill wrongly characterises section 51(v) of the Constitution as a general "Communications" power and states this as the Schedule's constitutional basis. But I read 51(v)'s broadest possible interpretation not as a "Communications" power but as a "Distance Communications ***Services***" power.

Not a telecommunications service

And because digital information is not postal, telegraphic or telephonic, the *subject matter* of the power must relate to today's communications service providers by virtue of its "other like services" limb. So already it can be seen the definitions of *storage* in section 2 of Schedule 2 of the bill may be in trouble, because some of them are directed merely towards a possible future use of data (copying and encoding for transmission) and not the *distance* communications service itself. By way of comparison, the defence power has a purposefull interpretation for defence of the Commonwealth and control of its forces, not merely directed at the armed services themselves but the wider object of defending the States from invasion. But section 51(v) is not directed to the wide object of "communications" generally but only to the regulation of certain services themselves.

Furthermore, close inspection of one's property is prohibited by law without statutory authorisation[24]. Access to a device is a question of possession of goods and subject to the law of trespass. For example, when Commonwealth police took a mobile phone to access its data without a valid warrant, it was said in Smethurst v Commissioner of Police [2020] HCA 14 (15 April 2020) at paragraph 120:

> "At the heart of the common law right to possession is the common law right to control access by others and thereby to exclude others from access. In protecting the right to possession, the policy of the common law is to protect the right to exclude others which is bound up in possession." (Emphasis added).

So the bill's definition of a "stored communication" as one that "*has been*" carried by a carriage service and "*is not being carried*" by a carriage service[25] – that is data merely held by the carriage service – this seems beyond power to me. The Parliament's post & telecommunications power only extends to what is necessary to the *services* of post and telecommunications. Thus contrary to the

24 See footnote 6 on page 3 of this submission
25 See section 2 of proposed Schedule 1 to the TIA "stored communication"

bill's definitions, it doesn't even extend to communications services providers if they are providing something separate from distance communications services – like merely the storage of data after transfer. The power sought to be relied on by the bill is directed towards services for the distance communications, not access to devices used in a different context which are personal property.

It seems to me the phrase "other *like*" services – like postal, telegraphic and telephonic, also must have public utility. I doubt they cover a case where a data-centre by private agreement aggregates information sent via a private optic fibre, stores it offline, to provide it in bulk on physical media for pick-up if needed. There is nothing in the Constitution of Australia granting the Commonwealth power to make laws regarding data storage[26] per se, nor a general power over any 'particular persons'[27], nor the regulation of carriage in general. Section 51(v) of the Constitution of itself cannot allow the Commonwealth an ongoing right to order access to a person's correspondence merely because it was once delivered by post, telegraph, telephone (fax) or other like services.

But section 7 of the bill goes a little further, asserting if data is backed up, and more data is downloaded, a right exists over what was previously backed up prior to the download! I think this would only be true if the technical service was delivered under an ongoing service agreement for that technical service, however the bill tends to conflate the dual meanings of 'service' found in the case law.

For example, the Australian Broadcasting Corporation offers television services within the meaning of section 51(v) of the Constitution. That doesn't mean if I record a show, the Commonwealth can demand a copy of that recording provided I watch the next episode, since even though the ABC is surely communications service provider, I have no ongoing service agreement with them between shows. I cannot sue the ABC if for some reason the show is cancelled for example. And if I buy a book from the ABC shop about that show, the Commonwealth has nothing to do with that book. This is true even though the ABC might be transmitting the TV show the book relates to even while I'm reading it, for there is no *distance communications* involved with the book in my hand. The position is even more clear in relation to downloads, because there is no property in information at common law, which is why we need privacy legislation.

So once a distance communications service has delivered, in both its technical and organisational senses, the Commonwealth's jurisdiction over the materials that were delivered ceases under 51(v) with the completion of the service. An analysis of internet protocols will reveal that different technical services complete at different times in the information life-cycle, and often (but not always) the organisational service providing to me the technical service will cease providing for me at that point too.

The CLOUD Act on the other hand is based on the U.S. federal commerce power (plus "necessary and proper" incidents), which although directed towards foreign, interstate and Indian commerce has been interpreted to co-mingle with intra-State commerce too. And in that foreign constitutional setting, commerce itself has been understood to be business generally. Data access is a condition of *business* transactions in and with the United States – even criminal business deals involved with Australia[28] – not limited to telecommunications services. So U.S. communications services must respond to production orders because there is an exchange of value involved in providing the service – a very broad power indeed. This is quite unlike the Australian trade and commerce power

26 Despite this the bill tries to regulate data storage – see section 7 of proposed Schedule 1 to the TIA

27 Hence section 20 of proposed Schedule 1 to the TIA professing reliance on Federal Parliament's Post & Telecommunications power.

28 See U.S. v Damion St Patrick Baston (11 Circuit Appeal 14-14444, 15-10923) 28 March 2016 which the U.S. Supreme Court declined leave to appeal.

which is more about regulating cross-border transactions and transport and doesn't co-mingle with intra-state trade and commerce. Additionally, the U.S. CLOUD Act seems to rely on a stronger concept of citizenship than is available to the legislative power of the Commonwealth, the latter relying on Australian residency; and possibly they have a less-powerful therefore less-jealous Supreme Court holding their federation together compared with the High Court of Australia.

The UK parliament's power on the other hand is plenary, having all the powers appropriate to a sovereign. I think a close enough equivalent in Australia is Federal Parliament's corporations power over telecommunications companies, because it's a mixture of Commonwealth power and referred power from the States – and the Sates more or less have the equivalent power of UK parliament within their jurisdictional spheres.

However in this case, the CLOUD Act only wields the U.S. Constitution's commerce power in relation to non-U.S. persons – it's *foreign commerce* aspect. I don't believe the external affairs power helps the Commonwealth here because there is no legal or physical relationship between an Australian communications service provider and the foreign agency making the "order". For example, in the case of extradition, the legal nexus is the pending charge laid against the person requested to be handed over. Nothing like that exists regarding foreign crimes and local telocs.

So I think the Commonwealth has a plentitunde of power for CLOUD Act reciprocation regarding corporations. As far as Australians are concerned, computer storage belonging to natural persons that is no longer part of a carriage service – e.g. disconnectedly stored for back-up purposes – subsists in the jurisdiction of the States, except if terrorism is involved[29]. I believe the bill needs to be amended to reflect this reality. The U.S. commerce power has it's problems too, so we will just have to see if the Americans can accept a little imperfection and use the Mutual Assistance arrangements in such cases. Therefore ***section 182 of proposed Schedule 1 to the TIA should be modified to also acknowledge the corporations power***.

Discussion

In this bill the criminal justice system of the future is being created to be inherited by our children. For it will not be long before the data ordered to be produced under such laws will feed machine learning and artificial intelligence to stay ahead of criminals. But as the internet-of-things becomes pervasive, backdoors in civilian IT systems will provide bad actors opportunity to use data in ways law enforcement are forbidden, potentially giving *them* the upper hand. On the other hand, where no circumvention of encryption is permitted, so that all communications are secret, the activities of artificial intelligence cannot be monitored by independent systems; we would not be able to confirm before it's too late, that artificial intelligence is working for us within acceptable bounds and free of infection. Thus we need to think very carefully when setting these trends of tomorrow.

Given the importance of exercising great restraint and considering the dangers of bypassing encryption, the bill if not changed to accommodate the CLOUD Act should include a provision making encryption-busting a last resort. Further, such a decision should be made by two judges, perhaps seconded to the AAT. The trouble is, bypassing the encryption of communications service providers creates unmet demand for privacy by people who don't trust the government – who are not criminals – to use readily available private alternatives. Such demand will spur developers to make these easier to use. Detecting criminals will be, and is fast becoming, like looking for a needle in a haystack. This is the result of the largess of mass-surveillance in the United States – a flawed policy – which for these reasons will ultimately prove counterproductive. However the employment

29 State power has already been referred to the Commonwealth regarding terrorism

of strong encryption in civilian systems the result of our own governments spying on us at least will harden our civilisation against others, so it's all good in the end I suppose.

In this submission I have tried to emphasise constitutionality (legality in human rights-speak) because dark forces of lawlessness will inhabit any grey area of law we leave open. Because the rule of law in defence of fundamental freedoms is what sets us apart from many others; we must not loose any of this in our cooperation with them; nor should we cede to the mind of lightening-fast machines that for which so much blood and treasure has been spent.

My views on the legitimate need for clear text access for the independent supervision of artificial intelligence activities is at odds with the U.S. Cloud Act's requirement of governments not coercing a means of decrypting information. However agreements under the scheme only last 5 years before review and I don't expect this problem to materialise before then. Nevertheless, it is something to watch and I would anticipate an exception will be needed for the monitoring of artificial intelligence activities in the next round.

I previously mentioned the Left of U.S. politics may object to an agreement with Australia if the bill does not address human rights as required for the U.S. Cloud Act by disallowance in Congress. But the previously-mentioned unconstitutional trampling of Australian State legislatures and Supreme Courts by a purported Australian federal law – section 34 of the Telecommunications Act 1979 (Cth) may not resonate with the Right of U.S. politics either.

But where the bill seems most deficient in meeting the rule-of-law country requirement of the U.S. CLOUD ACT, lies in the bill's lack of statutory control over the framing of designated agreements to be made with other countries – particularly in relation to incoming orders. There is no limit on what an order could be for: it could be an order invoking the breaking of an Australian service provider's encryption for example.

This is very concerning given it's undeniable many other countries' values differ significantly form our own. The Minister's Memorandum states agreements are to be struck with like-minded countries, yet the bill leaves open what such like-mindedness constitutes regarding incoming order requests. A change of government could see a change of like-mindedness also! The Minister's Memorandum also speaks or reciprocity, but the bill has no requirement of reciprocation, allowing one-way deals. I believe Australia should follow the CLOUD Act's lead on these topics, as I regard the U.S. approach to have been carefully thought through. Unlike the U.S. CLOUD Act (18 USC §2523(b)(1)(B)), the bill presently fails to ensure the Commonwealth Executive can only make agreements with other countries that:

(1) have robust substantive and procedural protections for privacy and civil liberties in light of data collection
(2) have adequate substantive and procedural laws on cybercrime and electronic evidence
(3) respect for the rule of law and principles of nondiscrimination
(4) have privacy rights
(5) have fair trials,
(6) support freedom of expression, association, and peaceful assembly
(7) prohibit arbitrary arrest and detention, torture and cruel, inhuman, or degrading treatment or punishment
(8) have procedures on how the government collects, retains, uses, and shares data, and effective oversight of same, with accountability and appropriate transparency
(9) don't firewall the internet
(10) aren't trying to grab our information

(11) don't force providers to bypass encryption

These are all taken from the CLOUD Act. And orders issued by the foreign government *"shall be in compliance with the domestic law of that country"* (18 USC §2523(b)(4)(D)(iii)) – which includes the Constitutional powers of the States in a federal system.

So before the U.S. Attorney General and Secretary of State can determine that an agreement with Australia is acceptable under the U.S. CLOUD Act, "credible information and expert input" must evidence that all the points above are met by *Australian governments* themselves. This is to show themselves worthy of trust, and not just in connection with the agreement but how non-US people are treated in relation to the data revealed. The bill is simply not fit for purpose until these matters are addressed.

The bill also provides insufficient constraints on executive power as to what will be in the agreements with foreign governments and how Australian communications service providers will be affected. The U.S. CLOUD Act on the other hand, put into my own words, provides in 18 USC §2523(b)(4)(D)(iv) that:

(a) Incoming "orders" will be related to serious crime or terrorism
(b) Incoming "orders" will specify a specific person or email address etc.
(c) Incoming "orders" will comply with the laws of the issuing country
(d) Incoming "orders" be subject to independent review
(e) Incoming interception "orders" will last only for a reasonable time and be for information which cannot otherwise be reasonably obtained
(f) Incoming "orders" cannot be made for limiting free speech
(g) Outgoing information will be checked
(h) Outgoing information will not be irrelevant to a crime
(i) The country issuing an incoming "order" will grant reciprocal rights
(j) The country issuing an incoming "order" will allow compliance inspections
(k) Any incoming "order" can be cancelled if it doesn't meet these criteria

Section 3 and Part 13 of proposed Schedule 1 of the TIA contain exactly no such restraints on the Commonwealth Executive making intrusive data-sharing arrangements with foreign "competent authorities". The bill's lack of restraint regarding powers proposed to be given to the Commonwealth Executive actually speaks against certification by the U.S. Attorney General and Secretary of State under the terms of the U.S. CLOUD Act (18 USC §2523(b)(1)(B)(ii) & (iii)). I think this is a major flaw in the bill as it stands today.

Additionally, the multiple instances of legislative overreach proposed in the bill that I have tried to identify would if correct, present a minefield to agencies trying to collect evidence in a lawful manner. This could easily result in the unintended unlawful collection of data leading to criminals escaping conviction, or having convictions reviewed and declared unsafe causing the release of those alleged criminals onto the streets. Where the bill tries to bypass the High Court's supervision of the Commonwealth Executive by wholly outsourcing its functions to foreign government agencies, the problem with unlawfully obtained evidence could become international. This would be very embarrassing for both Australia and the United States.

The U.S. CLOUD Act on the other hand, takes great care to stay within the rule-of-law. Reading it I realised how much righteous thought went in. It may be historic – no doubt it's highly strategic. This type of arrangement offers the people of the Commonwealth protection from unregulated intrusion by reciprocal nations. To them, our data is our data. This allows us to focus on protecting ourselves from those who think otherwise. ***The bill should be diligently amended to meet the***

requirements of a U.S. Could Act-qualified government according to 18 USC §2523(b)(1)(B)(ii) & (iii), and hold the United States to the same high standard to which they propose to hold us. Likewise, we should also impose the same constraints on our executive government as they have on theirs. I think such reciprocity is a very healthy principle for Five Eyes countries to adopt more generally, and I note the Minister agrees with the principle of reciprocity.

Recommendations

The following recommendations arise from the foregoing:

1. Section 34 of the Telecommunications Interception Act 1979 (Cth) ("TIA") be amended to require an authorising State Act to use Commonwealth authorisations and warrants.
2. Amend the legislative scheme so that AAT members issuing warrants or authorisations have relevant experience and are made judges of the Federal Circuit Court on secondment.
3. Amend the legislative scheme to mandate any encryption bypasses or backdoor privilege is
   (a) not used except in life-threatening situations
   (b) implemented as installable / uninstallable hardware / software components
   (c) executed in a confined way
   (d) uninstalled immediately after the authorisated activity is completed
   (e) decided by two judges on secondment to the AAT
4. Preserve Australia's economic interests by prohibiting outbound data transfers of non-Australian material as envisaged by 18 USC §2523(b)(4)(A)(B)(I) of the U.S. CLOUD Act.
5. In any decision, the AAT consisting of judge/s on secondment should also consider:
   (a) Double-criminality standard
   (b) The credibility of the allegations
   (c) The reasonableness of a suspicion of crime
   (d) Any political context
   (e) Any freedom of speech context
   (f) Any other human right or fundamental freedom consideration
6. Designated agreements must be approved by Parliament (or in an emergency only, temprarily assented to by regulation)
7. In Part 13 of the proposed Schedule 1 of the TIA:
   (a) Incoming orders be made subject to judicial review on the papers, or video conference hearing, by an Australian Court (vis-a-vis 18 USC §2523(b)(4)(K) with the Commonwealth as a nominal party to the case).
   (b) Foreign Applicant to compensate for costs of installation or de-installation of any encryption bypasses or backdoor privilege
   (c) After reviewing according to the criteria in item 5, a Commonwealth body should apply Australian executive power to incoming orders to execute this Part as a law of the Commonwealth

8. Section 182 of proposed Schedule 1 to the TIA should also acknowledge the corporations power.
9. The bill should be diligently amended to be substantially similar to 18 USC §2523(b), to:
   (a) meet the requirements of a U.S. CLOUD Act-qualified government;
   (b) hold the United States to the same high standard to which they propose to hold us; and
   (c) impose the same constraints on our executive government as they have on theirs in regards to agreements which can be entered into.

Thanks again for your invitation to me to make a submission,

Sincerely,
Eric Wilson
Software developer