Eric Wilson
[redacted]

03 May 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 – Response to Submitters' issues

I would also like to provide further information regarding issues raised by the Department of Home Affairs, Attorney General's Department, LECC and ASIO, further to my previous input invited by the Committee:

ARE ORDERS AND REQUESTS THE SAME THINGS?

The Department of Home Affairs' submission treats the enforcement provision of the bill as applicable to outgoing (extraterritorial) orders from Australia – see items 36-38 of the Department's preliminary submission. However the definition of *International Production Order* in the bill, to which the civil penalty regime of sections 124-126 applies, is not so limited: According to section 2, this term "International Production Order" could apply to any order issued under the Schedule, which scheme according to section 1, expressly includes incoming orders "issued by the competent authority of a foreign government".

Moreover, where the bill refers to outgoing orders, only the relevant parts of proposed Schedule 1 are mentioned – see section 111(1) and 112(1) of the proposed Schedule 1 for example. So the ordinary meaning of the word 'order' as would apply in Part 13, certainly speaks of compulsion, and is therefore repeatedly specified separately from a mere 'request' in part 13 of proposed Schedule 1. Thus the clear text of the bill proposes a basis of coercive orders purportedly to be made against Australian service providers by foreign governments; or at the very least, the basis of agreements with foreign governments allowing coercive orders to be made on Australian service providers to be potentially prosecuted against us in overseas courts.

Therefore if the Department is serious about Part 13 being only permissive in nature, as stated in the Minister's memorandum when dealing with Part 13, ***all occurrences of the word "order" in Part 13 should be removed and a provision inserted that an incoming order shall be taken to be only a request.***

JUDGES OR NOT?

The submission of the Attorney General's Department tries to address the issue of warrant-less authorisations being issued administratively by judges or AAT members. These are said to be acting in person and not with judicial power though a court. Even if such is sufficient to issue complex orders upon private third-party

service providers, respectfully, the Attorney General's Department has missed the point: The purpose of the AAT is to provide decisions on the merits using subject-matter experts. And when it comes to issuing orders to infringe upon fundamental freedoms and invade privacy rights, those subject-matter experts are indeed judges. That is because even if authorisations can be issued administratively, such weighty decisions are regarded by the law as quasi judicial[1].

So when describing administrative decision-making in relation to interception warrants – the very concept upon which the Attorney General's Department's submission seeks to rely – the joint judgement of four High Court justices states[2]:

> *"Yet it is precisely because of the intrusive and clandestine nature of interception warrants and the necessity to use them in today's continuing battle against serious crime that some impartial authority, accustomed to the dispassionate assessment of evidence and sensitive to the common law's protection of privacy and property (both real and personal), be authorised to control the official interception of communications. In other words, the professional experience and cast of mind of a Judge is a desirable guarantee that the appropriate balance will be kept between the law enforcement agencies on the one hand and criminal suspects or suspected sources of information about crime on the other. It is an eligible Judge's function of deciding independently of the applicant agency whether an interception warrant should issue that separates the eligible Judge from the executive function of law enforcement. It is the recognition of that independent role that preserves public confidence in the judiciary as an institution.*
> ***In other countries the same view has been taken of the desirability, if not the necessity, for judicial issuing of a warrant to authorise secret surveillance of suspects in criminal cases"*** [Emphasis added]

The High Court then drew support for its view from European, United States and Canadian cases and New Zealand statute law. So rule of law countries have a legitimnate expectation that any IPOs issuing from Australia will have been approved by a real judge.

So I believe if IPO's are regarded as administrative decisions, they are best done in AAT colours[3]; yet decided by a judge to ensure sufficient independence from executive influence. For while it's true a judge could be transferred out of AAT secondment, at least that judge's income would not depend on his or her performance as perceived by the government of the day as an AAT member's might be. And since Australia's international reputation will be affected by the IPOs we issue, we owe it to ourselves to set a high standard of propriety around this process.

1 See Mason and Deane JJ at paragraph 13 in Hilton v Wells [1985] HCA 16; (1985) 157 CLR 57 (14 March 1985);
2 Grollo v Palmer [1995] HCA 26, see paragraphs 20-22
3 See Grollo v Palmer [1995] HCA 26, see paragraph 37

AS AGAINST FOREIGN INTERFERENCE

Having read ASIO's submission I believe the powers proposed for ASIO by the bill are appropriate. If it means information gathered by ASIO can be passed on to prosecutors as evidence admissible in court the bill could greatly assist in the fight against foreign interference. However the bill is designed to also allow power similar to ASIO be given to foreign agencies, and I have previously expressed reservations about that. Therefore at least ***a list of countries with whom such designated agreements can be made should appear in the proposed Schedule 1,*** instead of this being left up to the Department of Home Affairs alone to decide.

VPNs – ELEPHANT IN THE ROOM!

The submission to the Committee by the Law Enforcement Conduct Commission countenances the bill will bypass encryption to allow plain text communications data be sent directly from service providers. Likewise ASIO's submission raises this expectation. We are repeatedly told by agencies this is necessary because most internet traffic is now encrypted. But we are also told by agencies that Huawei must be banned from all 5G networks because otherwise China could see too much information. So which or what is true?

The only way I can reconcile these two positions is to note that Australian security services are presently in favour of broad encryption circumvention, therefore it's safe to assume their preferred telecommunications hardware vendors are reasonably amenable to such backdoors. In other words, the ban on Chinese vendors would be in favour of backdoors controlled by other countries' vendors. Notably, most of these non-Chinese vendors are not Five Eyes countries either. Even if they were, I hope it has become self-evident that we must wean ourselves off Manning-Snowden style privileged access controls in favour of distributed IT security by encryption, since humans are the weakest link in IT security – see my previous letters to the Committee about this.

I believe this battle of the infrastructure back doors – China v Europe – is a manifestation of 20th Century telco thinking because it's inconsistent with today's digital technology stack. Telephony, with its tell-tale signalling, is almost dead and will soon be buried by 5G. For example, all social media platforms already operate above the Internet Protocol layer, and every modern mobile device is already capable of virtual private networking above the Internet Protocol layer. This means the idea of a fixed phone number assigned to handset hardware by which communications can be tracked or intercepted is merely a fading marketing ploy. For I recall when the Internet started, a person's telco, their modem supplier (a computer shop), and internet service provider were often all different companies. Then marketing departments discovoured it's easier to sell these as 'bundled' products/services. Yet these days, common subscriber-based virtual private networking (VPNs) or Web proxies, operate above all such marketing bundles, so that no employee working for a telco or its hardware suppliers need see what's really going on.

So the best way to ***deal all foreign communications hardware out of Australia's intelligence game may be by mandating virtual private networking everywhere, by moving all communications up the layered protocol stack.*** We've had technology to do this at scale for many years. Trouble is, VPNs also deal police out of the meta-data game, hence their desire for International Production Orders to be served on foreign communications service providers. But virtual private networking also connects us to countries which would never qualify as U.S. CLOUD Act-style participants. Therefore one wonders about the utility of the bill given it's so easy to bypass simply by shopping around a bit. This leads me to suspect an agenda for further legislation preventing virtual private networking to non-U.S. CLOUD Act-style international services to guarantee meta-data availability for local police via IPOs. If so, that agenda should be put squarely on the table for parliamentary debate now, not rammed through later amid a Christmas-break / election security scare, or even a pandemic. Respectfully, I believe the Australian public vis-a-vis Federal Parliament deserves far more respect from our public service.

For as it presently stands within the legislative scheme, this bill prolongs the worst of all worlds – idiosyncratic and expensive bans on overseas technology; backdoors used for foreign countries potentially endangering national security and intellectual property; and a supposed international crime-fighting net that allows big fish to swim straight through using VPNs. Therefore ***we need full disclosure by the Department of Home Affairs as to what additional measures will be required to sure up the needs of national security and crime fighting, balanced against the needs of privacy and industry*** – to make this bill and its interaction within the legislative scheme, into a workable 'framework'. Without such disclosure the Parliament is really flying blind when asked to vote on a bill as a disconnected piecemeal measure of a much bigger framework.

FURTHER RECOMMENDATIONS

Based on the above I respectfully wish to add the following to my recommendations:

12. The Department of Home Affairs provide a clear picture of any additional interception or access measures or restrictions intended to be included in the legislative scheme to allow the bill's operation to be properly understood in context.
13. All occurrences of the word "order" in Part 13 should be removed and a provision inserted that an incoming order shall be taken to be only a request.
14. A list of countries with whom designated agreements can be made should appear as a provision in the proposed Schedule 1.

Once again I thank the Committee for its invitation to make a submission;

Sincerely,

Eric Wilson

Software Developer