27 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 – Additional information

I would also like to provide some information regarding an issue helpfully raised in the Western Australia Police submission, further to my previous submission invited by the Committee:

The bill's definitions twice mention "upload"[1], however this kind of language is already obsolete and there is no definition of "user" to qualify such "uploads". Why is this important? The "Internet of things" ("IoT") for which 5G is designed, allows systems to be more geographically disbursed. This means whether something is considered to 'upload' or 'download' can be relative to which device is used as the reference point. A simple similar example are widely available chat programs on mobile phones today which connect 'peer-to-peer' so that text and video calls don't go through any central exchange – providing far better performance and network efficiency. In this case, both ends of the conversation may be considered to be 'uploading' depending on who does what. (That is why I used both 'upload' and 'download' examples in my previous submission.) So as will be seen, the word "upload" in section 7 of the proposed Schedule 1 of the TIA could be over-burdensomely intrusive into IoT / 5G applications.

I believe the Committee should also consider that modern IT systems have many layers of encryption. At the bottom of the stack, blocks of zeros and ones written to storage devices are encrypted to protect against maintenance technicians swiping their data. At the top of the stack, end-user passwords are encrypted for traversing the Internet so that middlemen cannot get into email accounts etc. In between these extremes, operating systems can encrypt data on a per-user basis, to prevent IT administrators accidentally accessing information held by a user or group. Applications may also encrypt individual files or pieces of information so that it cannot be accessed except on authorised devices for example. And of course, as information is transferred over the Internet it is

1 See "Stored communications" (f) and "Telecommunications data" (g) of section 2 of the proposed Schedule 1 to the TIA for example.

very often encrypted. So for safety, the infrastructure for these layers of encryption is often located on different equipment administered by different people (even different service providers) over different networks.

(The Committee will appreciate I have greatly simplified the above for brevity but believe it's a reasonable description for the purposes of lawmaking.)

So what law enforcement wants is the password for accounts, or a real-time copy of what is happening or has happened with an account, because this bypasses all layers of encryption and the safety of having multiple IT administrations; in order to produce clear text and video, files etc. And therein lies a problem, because proper modern IT systems ***do not*** keep passwords to get into people's accounts!

What they keep is a mathematically calculated representative "hash" of passwords, which cannot be reverse-engineered – it's the laws of mathematics guarding our nation's secrets not human access controls. So should an extra layer of manual access control (IT management) be implemented to intercept passwords to provide the information law enforcement needs? This axiomatically creates systemic weakness, because now we are trusting people interposed between users and their data not just mathematics. And as soon as we start trusting people, we expose ourselves to the Manning and Snowden problem, who both worked for government – see my previous submission to this enquiry about that.

Fortunately, there is a way to limit the systemic security problem. Personal identifiers such as email or network addresses can be used to redirect the traffic of *particular persons* to a weakened replica of a password system (for example) so that we only have to trust human access control regarding those individual accounts specified in the warrant. This is why the U.S. CLOUD Act requires personal identifiers. Thus I would think the Western Australian Police could expect they will receive everything a communication service provider has regarding such a warrant. The U.S. CLOUD Act's prohibition only relates to coercing development of a new capability but communications service providers already have as much for the processing of court orders etc.

But what if an app uses peer-to-peer connections to communicate directly between parties? Again, a specific personal ID will be used to redirect the device or app to weakened software updates that allow access. The least-intrusive method would target the communications app and not the whole

device, which in my view is beyond the distance communications services' power of the Commonwealth anyway. (Whole device access involves the law of trespass and possession according to the High Court[2]).

I regard the above arrangements to be what the U.S. CLOUD Act intends – more than enough for normal police work. But what if police want not only relevant information but also the end-user's password itself? This is a bridge too far, because it would provide an ability for police access beyond the time limit of a warrant – unless target/s are forced to reset their password, which would likely tip them off. Therefore in the vast majority of cases, the least-intrusive access will not involve any disclosure of passwords or the mathematical representation of them, and will not trespass upon the device either, only relevant communications apps. (A computer access warrant can be applied for if more is required.)

Flag hoisted at a police station in Victoria under freedom of expression, honouring China's National Day, reportedly for the 5th year. But under the bill, the "Telecommunications (Interception) Act 1979 - Declaration of agency - Police Force of Victoria" would if valid, allow International Production Orders to issue upon U.S. communications service providers regarding Chinese users. This is proposed to be ***without the supervision of a judge*** *as is sensibly required under Victorian law, since executive governments (including Federal) often change...*

However, the bill goes much further, conflating ordinary policing such as previously described, with counter-terrorism or espionage. For example, what if there is no known specific personal identifier but only a code name referring to an up-comming attack? It would be highly desirable to do a global search using that code name to find the personal identifiers involved in the plot. This does not involve merely redirecting network traffic to a weakened version of a password system, but weakening a system generally by providing access credentials capable of bypassing a substantial part of a system's encryption to do a global search – thereby creating systemic weakness.

As I have mentioned in my previous submission, this is not a suitable power for police. And for those to whom such a power is suitable, de-installation of the required hardware and/or software immediately after the order is executed should be mandatory.

2 Smethurst v Commissioner of Police [2020] HCA 14 (15 April 2020)

Under no circumstances should such a systemic weakness be allowed to remain, and such a serious intrusion should only be authorised by two judges in my opinion. For across a distributed 5G environment such interference could be extensive. And under no circumstances should a foreign actor be allowed to order such a systemic weakness into any Australian communications system. It's just too dangerous for national security, as Manning and Snowden have taught us well – I hope!

Of course it's no answer to say that only communications service provider staff would be asked to make the interceptions or obtain required materials; for they are just as vulnerable to infiltration as government if not more so via corporate ownership.

In view of the above, I would like to add the following recommendations to my previous submission:

10. That the legislative scheme be amended so that only ASIO be allowed to:
(a) apply for a warrant or authorisation without providing a specific personal identifier; or
(b) apply for a warrant or authorisation which includes the provision of password information; and
(c) in case of either (a) or (b) requires two judges to approve, and must be limited to a specific and credible life-threatening lead.

11. That the legislative scheme be amended so that:
(a) the least-intrusive methods be considered in every application if not already mandatory; and
(b) only relevant apps or programs will be involved in any application.

Errata: In recommendation 4 of my previous submission, "non-Australian" should read "Australian"; and for recommendation 8, "Section 182" should read "Section 20".

I hope the above information is of assistance to the Committee. If a hearing is held I would be pleased to give a demonstration of the Internet of Things (IoT) to aid in understanding the environment in which the bill is intended to operate.

Thanks again for the invitation to make a submission,
Sincerely,

Eric Wilson
Software Developer