Dr James Renwick CSC, SC

Independent National Security Legislation Monitor

OPENING STATEMENT[1]

PUBLIC HEARINGS IN THE INSLM REVIEW AT THE REQUEST OF THE PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY CONCERNING THE *TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE AND ACCESS) ACT 2018 (*CTH)

Introduction

1. I begin by acknowledging the traditional custodians of the lands that we are on, and paying my respects to Elders, past and present. I am the current Independent National Security Legislation Monitor or INSLM and these are public hearings conducted under s 21 of the INSLM Act for the purposes of my review into the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (TOLA Act). I have decided it is not necessary to require evidence for this hearing to be given on oath or affirmation.

2. The hearing is being transcribed and it is also being live streamed.[2] I welcome those watching this online. I welcome all who are here, particularly those who have travelled a long way, all witnesses and members of the media. Understandably, there is much interest here and overseas in this review.

3. I am happy for photos and filming during my opening and during the opening statements given by any witnesses but I would ask that you do not take photos while evidence is being given as it can be distracting. I thank our hosts for providing this venue and for facilitating the smooth running of the day. Sitting next to me are my:

    a. Principal Adviser, Mr Mark Mooney;

    b. Counsel Assisting, Ms Laura Johnston; and

    c. Mr James Anderson, Senior Lawyer from the Australian Government Solicitor.

4. I begin with some context. I then set out my tentative views. During these hearings I welcome debate about them and my assumptions - in other words, this is a good time for witnesses to say that I have misunderstood technological issues or that I am proposing something which is unworkable or misconceived or otherwise wrong. Similarly for those watching online, please feel free to send supplementary submissions, but please do it soon, within the next week or so. I will be making a speech at the Lowy Institute in Sydney on 5 March where I will likely set out my further thoughts. See: https://myaccount.lowyinstitute.org/events/2020-lls-5-march

5. For those who don't know me or my role, I am a self-employed barrister and independent statutory office holder appointed by the Governor-General. My statutory functions require me to review the operation, effectiveness, and implications of Australia's counter-terrorism and national security legislation (s 6(1)(a)); and to consider whether it contains appropriate

[1] Check against delivery. Embargoed until delivery from 0845 on 20/2/2020.

[2] https://eavs.com.au/inslmhearing/

safeguards for protecting the rights of individuals, remains proportionate to any threats, and remains necessary (s 6(1)(b)). I have Royal Commission like powers and I have used them so I have a full picture about how the intelligence agencies and the police are using their TOLA powers.

6. I have produced eight reports which are on my website.

7. Usually, I produce reports of my own motion or at the request of the Prime Minister or the Attorney-General. This is the first time I have received a request from the Australian Parliament's Parliamentary Joint Committee on Intelligence and Security (PJCIS).[3]

8. When TOLA was enacted in December 2018 there was a short time for consultation before it became law and there was concern, even anger, expressed about the lack of time for consultation and about the terms of TOLA, especially by designated communications providers or DCPs[i] who, under the Act, cover the full range of those involved in communication over the world wide web of content and data. Some say the lack of consultation means TOLA should now be repealed in its entirety. I do not think that is realistic. Instead, I seek to answer the questions required by my role: principally, how has the law operated, is it effective in its stated aims, are there adequate safeguards, and if not what amendments should now be made.

9. I can say something immediately though about the position of the State and Territory ICACs[4] who do vital work as integrity agencies. I accept their evidence that they are affected like the police by the phenomenon of 'going dark' but they find themselves in a worse position than the police as they currently have no access to powers under Schedule 1, including when they may need to investigate police themselves.

10. Although time prevents me from producing an interim report, but noting that the Parliament may take some months to consider the reports by me and the PJCIS, I consider that the ICACs have the same need as the police to have urgent access to TARs and TANs on the same terms and with the same safeguards as the police, for as long as the police have such access. In other words, I formally commend to the PJCIS the idea of immediately recommending such powers with a view to prompt legislation to that effect; if additional safeguards (or new limitations or even repeal) are recommended concerning police powers, I think it almost certain I would equally recommend them for the ICACs. I understand that the urgent need is for TARs and TANs not the more controversial TCNs which I will therefore defer for consideration in my report.

11. In March 2019, the Chair of the PJCIS referred TOLA to me for review. This referral to the INSLM by the PJCIS is the first of its kind and I hope it will not be the last as our roles complement each other. I will report to the PJCIS no later than 30 June so that my review is available to assist the PJCIS' upcoming review of the legislation, due by 30 September.

12. I note the intense media, industry and public interest in the TOLA Act. For the first time as INSLM, I have consulted with industry and technology advocacy groups, alongside my usual engagement with government agencies, the legal profession and civil society. Questions of trust, access and privacy have been consistent themes throughout this review.

The Threat Landscape

13. As usual, I begin these public hearings with a summary of threats on counter-terrorism and national security. My website contains greater details, but in very short summary:

[3] https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security

[4] Which have various names.

a. the espionage and foreign interference threat has significantly increased,

b. the risk of an onshore terrorism attack remains at the 'probable' level it has been since 2014[5] - that threat comes mainly from radical violent Islamists but there is also some radical, violent, right-wing activity, and

c. The external terrorist landscape also continues to evolve, for example I expect ISIL will continue to shock and surprise.

14. However, in this inquiry I must look beyond these areas to crime more generally because the near universal use of the World Wide Web for legitimate private, commercial and government communications attracts criminals and other bad actors. (When I speak of *the web* I am conscious that it is fragmenting, if it has not already separated, due to the extensive firewalls in China, Russia and other places.)

15. To give a few examples of illicit activities on the internet, not limited to Australia:

a. ISIL has made very effective use of it to publicise, proselytise, and direct terrorism;

b. The Christchurch shooter live streamed his atrocities on social media;[6]

c. There is large scale theft of private data and corporate intellectual property;

d. There is local and transnational organised crime, money-laundering, trafficking of illicit drugs and arms and child sexual exploitation, including on the dark web which facilitates the commission of such crimes anonymously and thus with impunity.

e. Nation states and their proxies continue to engage in espionage and foreign interference: as former Director-General of Security, Duncan Lewis remarked last year *"the current scale and scope of foreign intelligence activity against Australian interests is unprecedented."*[7] But they also work on their capacities to engage in cyber-attacks such as Computer Network Attacks not only, say, to disable access by another country's military to its computers and web servers, but also to have kinetic effects for example by releasing dam water, turning off power to hospitals, or attacking a stock exchange's records. It is no accident that such conduct is capable of amounting to a 'terrorist act' under the Criminal Code.[ii] The New York Times' '*Privacy Project*'[8] provides many examples of such behaviour, and also of the large scale theft of private data and corporate intellectual property – as do the unsealed

[5] https://www.nationalsecurity.gov.au/securityandyourcommunity/pages/national-terrorism-threat-advisory-system.aspx which states that 'Australia's National Terrorism Threat Level remains Probable. Credible intelligence, assessed by our security agencies, indicates that individuals or groups continue to possess the intent and capability to conduct a terrorist attack in Australia.'

[6] There is an ever-increasing link between terrorism and the internet. The attack by an Australian in Christchurch was by a perpetrator who conducted the attack alone. However, he drew inspiration from a global network of like-minded individuals who often disseminate and discuss their views online. The phenomenon is not new. Christchurch turned into a seminal event in the history of such terrorism for its lethality and use of technology to maximise impact, in particular the live streaming of the attacks on social media. In turn, that use of technology led to the swift enactment of the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* and also a number of international initiatives led by Australia to limit and prevent the internet from being a safe haven for terrorist and violent extremist content and activity.

[7] https://www.asio.gov.au/asio-director-general-duncan-lewis-address-lowy-institute.html

[8] https://www.nytimes.com/series/new-york-times-privacy-project

indictments filed by the US Department of Justice against, for example, members of the Chinese People's Liberation Army.[9]

16. One answer to the bad actors - at least those who steal property, data or identities - is to increasingly encrypt content and metadata, whether at rest on a device or in motion (such as a phone call). Although there may be no bright line by *content* I mean texts, emails, phone calls and pictures; and by *metadata*[10] I mean such things as when an email was sent, the sender and recipients, their locations, how it was sent, how it is stored, and also what web sites have been visited, what apps used, and so on.[11]
17. There seems little doubt on the evidence I have received that the so-called 'golden age' when such unencrypted content (or, to an increasing extent, metadata) could easily be read and comprehended by police, integrity and intelligence agencies acting with lawful authority has gone. Instead, they now speak of a virtual world which has gone 'dark', gone 'spotty' or even gone 'different' and in large part this is what led to passing the TOLA Act.
18. Some critics of the TOLA Act say that encryption is vital for lawful internet use on which commerce (such as banking, online shopping and business communications) and personal interaction including on social media depends, and that TOLA will seriously undermine encryption. While I am very grateful for all submissions, I am wary of the idea that there is a binary choice between encryption and, say, law enforcement. Instead, I agree with statements countering that idea which come from two very different sources.
19. There is the distinguished Encryption Working Group assembled by the Carnegie Endowment and Princeton University[iii] which recently said that it:

    '… rejects two straw men—absolutist positions not actually held by serious participants, but sometimes used as caricatures of opponents. These are: first, that we should stop seeking approaches to enable access to encrypted information [but second,] that law enforcement will be unable to protect the public unless it can obtain access to all encrypted data through lawful process.

20. And Sir David Omand, a former head of GCHQ, in his recent book,[12] *Principled Spying,* says:

    As with all hard public policy issues, there is no easy way of reconciling conflicting ethical concerns. Place the security of personal data and one's anonymity on the Internet above all else and law enforcement is shut out, the rule of law is undermined, and crime, terrorism, and cyber attacks flourish. Insist on a right of access to all encrypted data for law enforcement and intelligence agencies—for example, through controlling or weakening encryption standards—and confidence in the Internet as a secure medium will be lost, and fragmentation of the Internet will spread.[13]

---

[9] For one example in 2018 see 'Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years': https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal

[10] Sometimes called telecommunications data.

[11] A mandatory data retention regime is prescribed by Part 5-1A of the TI Act and it requires carriers, carriage service providers and internet service providers to retain a defined set of telecommunications data for two years, ensuring that such data remains available for law enforcement and national security investigations. The law is being reviewed by the PJCIS: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Dataretentionregime

[12] Omand and Phythian, *Principled Spying, the Ethics of Secret Intelligence*, Oxford University Press, 2018.

[13] In the Chapter on *Digital Intelligence and Cyberspace* at P 144.

21. As I have consistently said, just as in the physical world we do not accept lawless ghettos where the law does not apply, so also it should be in the virtual world: thus intrusive surveillance powers – certainly, conferred by law and with clear thresholds and safeguards – which already apply in the physical world should in principle apply in the analogous virtual world unless there are good reasons to the contrary. But I am tending to the view that because so much data and content which we do not know about is contained on our mobile phones and computers - not least because it is generated by designated communication providers as they seek to monetise our personal information - that there should be at least as great scrutiny and safeguards as there were pre-TOLA before such information is made usable under TOLA.

Pre-TOLA

22. Prior to TOLA, when it was often sufficient to obtain what was contained in unencrypted form on, or passing through, a mobile phone or computer, as content or data, four main Australian laws were used, namely the:
    a. *Surveillance Devices Act 2004* (SD Act),[14]
    b. *Australian Security Intelligence Organisation Act 1979 (*ASIO Act),
    c. *Telecommunications (Interception and Access)* Act 1979 (TI Act), and
    d. *Crimes Act* 1914.
23. For example, the AFP and ASIO might
    a. Under the *TI Act*: seek access to telecommunications data, stored communications that already exist, or the interception of communications in real time/data in motion. That access might be given by a telecommunications provider without the need to seize the actual mobile phone.[15]
    b. Under the *ASIO Act:* a Computer Access Warrant could authorise covert access and copying of what is in a computer(including a phone);
    c. Under the *Crimes Act*: [16] AFP constables executing warrants either in respect of premises[17] or in respect of a person[18] could search for and seize 'evidential material'[19] - which includes things 'in electronic form'[20] and to move a thing found at warrant premises 'to another place for examination or processing'.[21]

24. The critical safeguards for the grant of these intrusive powers were and are as follows:
    a. *Permission* for access to data was granted by warrant issued by an independent eligible judge or Tribunal member for the AFP, and by the Attorney-General for ASIO – metadata access can usually be authorised by an agency head as it is seen as less intrusive.
    b. *Complaints* could be made to the Ombudsman for the AFP, or the IGIS for ASIO.

---

[14] A data surveillance device, a listening device, an optical surveillance device or a tracking device.

[15] A named person warrant might allow all of an individual's landlines or mobile services to be intercepted or accessed. A 'B Party warrant' allows interception of communications with people communicating with a criminal suspect.

[16] And Customs, now Australian Border Force Officers have significant powers as well.

[17] *Crimes Act 1914* (Cth) (Crimes Act) s3C(1).

[18] Crimes Act s3C(2).

[19] Crimes Act s3F(1)(c), in respect of a warrant in force in relation to premises.

[20] Crimes Act s3C(1).

[21] In certain circumstances: Crimes Act s3K(2).

c. *Decisions could be judicially reviewed*: there being a constitutionally entrenched[iv] right to judicially review decisions of officers of the Commonwealth, our constitutional founders having had in mind the US Supreme Court case of *Marbury v Madison*[22].

d. *Review of the laws themselves* could be undertaken by me as INSLM and the PJCIS.

The changes made by TOLA

25. TOLA is very complex but let me try and focus on its essence. There are 5 schedules. Most submissions focus on Schedule 1 although all schedules are significant.

26. In Schedule 1, the response to 'going dark' is really twofold. First, either by request in a technical assistance request (TAR) or by compulsion in a technical assistance notice (TAN) a designated telecommunications provider - a term which is designed to cover the whole spectrum of entities and people which are involved in the communication of content and data, whether it is hardware manufacturers, software or app manufacturers, cloud providers, and telecommunications companies – must, for example, make the unintelligible content or data intelligible or accessible, or do another listed act or thing, but only if they have an *existing capability* to do so, and when they do so they cannot be sued civilly for doing so and they do not commit a criminal offence.

27. Second, by way of a technical capability notice (TCN), an agency may request the Attorney General to grant a compulsory notice requiring the DCP to *create a new capability* which the DCP does not then have to allow the content or data otherwise obtained by warrant or authority to be made intelligible or accessible, or to do another listed act or thing. The same civil and criminal protections apply. The latest Annual Report regarding the TI Act reveals that "Two agencies used powers under Part 15 of the *Telecommunications Act 1997* to request technical assistance from designated communications providers. Five technical assistance requests were given by the AFP, and two were given by NSW Police." I have or will review all uses of Schedule 1 powers to date. I have also reviewed ASIO's use of the TOLA powers but am limited in what I can say in public.

28. Can I make this point however? Nothing I have seen to date suggests there has been any form of 'mass surveillance' as a result of TOLA; in fact, what I have seen to date suggests that TOLA has allowed for pre-existing intrusive powers to now be used in a more targeted or limited fashion against persons of interest to make content or data otherwise obtained by warrant or authority to be made intelligible or accessible, or to do another listed act or thing.

29. But, and it is a large 'but', none of the Schedule 1 powers can validly authorise (nor civilly protect the relevant DCP) if the requested act or thing would create a *'systemic weakness'* or *'systemic vulnerability'*. I will return to these notions, which are controversial.

30. Unlike the underlying warrants or authorisations, TANs are not granted by an eligible judge or independent tribunal member but are simply granted by the agency head or their delegate, a departure from the normal course of an independent eligible judge or tribunal member in relation to a coercive power affecting privacy.

31. Similarly, the Attorney-General issues a TCN although a retired judge with technical assistance can be requested to give a report to the Attorney which must be considered but is not binding upon the Attorney.

32. I then turn to the submissions which are on my website. Perhaps the majority have focused on three main areas for reform:

    a. The definitions in the TOLA Act of *systemic weakness* and *systemic vulnerability* and related definitions, and how disputes concerning the application of these statutory terms can be resolved;

[22] 5 US 137; see, e.g. https://www.law.cornell.edu/supremecourt/text/5/137

b. Where the current TOLA decision makers are the Attorney-General or agency heads, should they instead be current or retired judges or Tribunal members, assisted by technical experts who understand the effect of the exercise of particular TOLA powers on privacy and on the effectiveness of encryption.

c. Better record keeping requirements, and clear statements of review rights when compulsory powers are used, so that affected people and entities can exercise those rights, including when complaining to the Commonwealth Ombudsman or the Inspector-General of Intelligence and Security.

33. I will be exploring these issues in these hearings.

34. An argument I have heard is that the pre-TOLA laws have worked perfectly well and that Schedule 1 powers merely make existing laws 'technology proof' in the sense that the content or data has already been lawfully obtained, it is 'just' a matter of making it comprehensible. I remain to be convinced of this as a matter of law and practice for at least two reasons.

    a. First, I ask, isn't the main point of the TOLA Act that 'going dark' has created a large problem for police, intelligence and integrity agencies to which the pre-existing law is an insufficient answer? An eligible judge granting access to encrypted content can assume the privacy impact is slight; but if a Schedule 1 power is to be used to make data intelligible or accessible, for example, it is significant. Why shouldn't both be granted in the same way?

    b. Second, doesn't the complexity of technology and the fact most people don't know what the data and content on their mobile or computer says about them mean that in order to keep oversight up to date the British model of retired judges with distinguished scientific advisers should be used, or something similar, e.g. the Security Division of the Administrative Appeals Tribunal (AAT)?

Systemic weakness or systemic vulnerability

35. The second issue is the concept of 'systemic weakness' or 'systemic vulnerability'[23]: are those definitions right, and how are disputes about whether there is such a weakness or vulnerability to be resolved? None of the powers under Schedule 1 can be used in such a way as to create a systemic weakness or vulnerability. If they do, they are invalid which means the obtaining of the information by the agency would be unlawful but also the protection from being sued by customers of the DCPs would also fall away; so the definitions are critical.

36. You will see from many of the submissions that there is criticism of the definitions. I am inclined to give statutory examples in each definition of what is or is not such a weakness or vulnerability. The challenge I set for all submitters is to come up with better definitions than exist now. I note there is a current bill in the Senate which does just that and I am interested in hearing from witnesses at this hearing as to whether that is seen as an improvement.[v] May I offer these tentative observations on that Bill:

    a. It helpfully focuses on prohibited effects;

[23] S 317B provides:

> *systemic vulnerability* means a vulnerability that affects a whole class of technology, but does not include a vulnerability that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.
>
> *systemic weakness* means a weakness that affects a whole class of technology, but does not include a weakness that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.

b. It might usefully make clear that it seeks to protect effects which would unnecessarily compromise the privacy of customers but also risk compromise of the DCP's products security and the security of the DCP's general users;

c. I ask whether the use of the words 'would or may in the future' in proposed s 31ZG(4) creates an unattainable standard because such a risk can never be ruled out?

37. The other aspect of this issue is how to adjudicate a bona fide dispute between an intelligence, integrity or police agency on one hand and a DCP on the other about whether a Schedule 1 notice or request crosses the line. Such disagreements are bound to happen at some stage and it is undesirable that either the agency or the DCP have court as their first call: either a criminal prosecution in the case of the agency, or a civil case by the DCP seeking a declaration that the line has been crossed and the purported obligation need not be complied with.

38. In each case, in either a criminal or civil court, this would result in the disclosure or the risk of disclosure of what are likely to be current police, intelligence or integrity operations on the government side and highly sensitive intellectual and commercial property of the DCPs on the other. The courts are designed in principle to operate openly and are not designed to hear such matters in complete secrecy.

Possible solutions

39. I have met with IPCO in the UK, including its head Sir Brian Leveson, its very senior retired judges and its distinguished technical advisers.[vi] IPCO provides a double lock whereby warrant and authorisation applications are ineffective unless IPCO finds, having reviewed the material put before the minister or agency head, that the application is for example, lawful, reasonable and proportionate. It has been very well received. My conversations on both sides of the Atlantic Ocean made clear that IPCO was critical to the UK obtaining a Cloud Act agreement from the United States, which Australia also seeks. It is one possible model. Also, in the UK, they have a Technical Advisory Board allowing in effect a private binding arbitration with a retired judge presiding and a technical expert appointed by the agency and another by the DCP to determine such matters as whether a request is technically feasible.

40. Another model which has already operated successfully for many years in Australia is the AAT.

41. The AAT is independent of government, headed by a Federal Court judge and its Deputy Presidents are either other Federal judges or senior lawyers. It grants certain warrants and reviews certain decisions of ASIO.

42. I have in mind that an application for at least a TAN and a TCN and possibly also a TAR could go to for approval to the Security Division of the AAT which is accustomed to dealing with highly sensitive or secret information about intelligence agencies. If the DCP has no objections it need not appear. If it does, for example as to whether the request is reasonable or proportionate or creates a systemic weakness, that could be resolved in a hearing or prior to a hearing using one of the ADR processes currently available in the AAT. Because there may be highly technical questions to be determined, a Presidential member would sit with a person with eminent scientific or technical expertise who would be appointed as a part-time senior member. To the extent they could publish their decisions these would guide agencies and DCPs alike. Appointment to the AAT of a group of, say, half a dozen technical experts whose expertise would cover the gamut of technical knowledge likely to come up could also with advantage be appointed to assist the Inspector-General of Intelligence and Security and the Ombudsman in their audit functions and this is in effect is what occurs in the United Kingdom. I look forward to comments on this possible model.

43. As to the other schedules, I do not want to suggest that the schedule 2-5 are unimportant, to the contrary, they have however received less attention in submissions. The written opening summarises key effects of these schedules.

44. I look forward to hearing evidence from all witnesses on some or more of these matters over the next couple of days before moving to conclude my review. I now welcome the Director-General of Security to give evidence.

Canberra
20 February 2020

Appendix

45. *The main reforms made by Schedule 2 are as follows:*

    a. *empowering the Attorney-General to authorise ASIO, in a computer access warrant, to intercept communications for the purpose of doing anything specified in the warrant, thereby removing the need for ASIO to obtain a separate warrant under the TIA Act for the interception;*

    b. *empowering the Attorney-General to authorise ASIO, in a computer access warrant, to remove a computer or other thing from premises to do to the computer or thing anything specified in the warrant;*

    c. *empowering ASIO to remove a computer or thing from premises for the purpose of executing a computer access warrant;*

    d. *empowering ASIO to do anything reasonably necessary to conceal the fact that something has been done in relation to a computer under a computer access warrant or related authority;*

    e. *empowering the Attorney-General to authorise a law enforcement officer to apply for a computer access warrant at the request of a foreign government.*

46. *Schedule 3 amends the warrant powers in Part IAA the Crimes Act (Cth) for police constables in particular in respect of data held in or accessible from electronic devices. Schedule 3 does not amend any other parts of the Crimes Act, nor any other legislation. There are related powers given to the police, the Australian Border Force and ASIO, in Schedules 3,4 and 5 which are designed for example to require a person to provide their password to their mobile phone once there is already separate authority to look at that phone. The idea of unlocking a computer or phone is readily understandable but it is extremely important for public confidence that these intrusive powers are properly regulated and subject to proper oversight.*

47. *The reforms effected by Schedule 4 concern Australian Border Force Officers. Prior to TOLA, the Customs Act empowered an ABF officer to apply to a magistrate for an 'assistance order' compelling a person with a particular connection to a computer to provide 'any information or assistance it is reasonable and necessary' to access, copy or convert into electronic form data held in a computer or data storage device. Following TOLA, that power continues to exist. Schedule 4, in essence,*

    a. *introduces a power for ABF officers to obtain a search warrant in respect of a person;*

    b. *expands the ABF's powers in respect of electronic items and access to data in connection with the execution of a search warrant in respect of premises;*

    c. *increases the time during which a computer or data storage device moved from warrant premises by the ABF for examination or processing may be retained for that purpose; and*

    d. *amends offence provisions and maximum penalties that apply where a person fails to comply with an assistance order.*

48. *Schedule 5 deals the provision of assistance to ASIO, either voluntarily or under compulsion. The amendments that Schedule effects protect those who assist ASIO, by engaging in certain conduct, against civil liability for that conduct, either at the request of the Director-General or by voluntary disclosure. Further, it empowers the Director-General to request the assistance. Schedule 5 entered into force on 9 December 2018.*

49. Prior to the amendments effected by TOLA, the ASIO Act empowered the Attorney-General to confer on a person protection from civil or criminal liability where the person was engaged in authorised 'special intelligence conduct'.[24] *However, ASIO did not have any more general power to confer immunity from civil liability on a person assisting ASIO in any other capacity or for any other purpose.*

---

[i] TELECOMMUNICATIONS ACT 1997 - SECT 317C

Designated communications provider etc.

For the purposes of this Part, the following table defines:

(a) designated communications provider ; and

(b) the eligible activities of a designated communications provider.

Designated communications provider and eligible activities		
Item	A person is a designated communications provider if ...	... and the eligible activities of the person are ...
1	the person is a carrier or carriage service provider	(a) the operation by the person of telecommunications networks, or facilities, in Australia; or (b) the supply by the person of listed carriage services
2	the person is a carriage service intermediary who arranges for the supply by a carriage service provider of listed carriage services	(a) the arranging by the person for the supply by the carriage service provider of listed carriage services; or (b) the operation by the carriage service provider of telecommunications networks, or facilities, in Australia; or (c) the supply by the carriage service provider of listed carriage services
3	the person provides a service that facilitates, or is ancillary or incidental to, the supply of a listed carriage service	the provision by the person of a service that facilitates, or is ancillary or incidental to, the supply of a listed carriage service
4	the person provides an electronic service that has one or more end-users in Australia	the provision by the person of an electronic service that has one or more end-users in Australia
5	the person provides a service that facilitates, or is ancillary or incidental to, the provision of an electronic service that has one or more end-users in Australia	the provision by the person of a service that facilitates, or is ancillary or incidental to, the provision of an electronic service that has one or more end-users in Australia

---

[24] ASIO Act s35K.

6	the person develops, supplies or updates software used, for use, or likely to be used, in connection with: (a) a listed carriage service; or (b) an electronic service that has one or more end-users in Australia	(a) the development by the person of any such software; or (b) the supply by the person of any such software; or (c) the updating by the person of any such software
7	the person manufactures, supplies, installs, maintains or operates a facility	(a) the manufacture by the person of a facility for use, or likely to be used, in Australia; or (b) the supply by the person of a facility for use, or likely to be used, in Australia; or (c) the installation by the person of a facility in Australia; or (d) the maintenance by the person of a facility in Australia; or (e) the operation by the person of a facility in Australia
8	the person manufactures or supplies components for use, or likely to be used, in the manufacture of a facility for use, or likely to be used, in Australia	(a) the manufacture by the person of any such components; or (b) the supply by the person of any such components
9	the person connects a facility to a telecommunications network in Australia	the connection by the person of a facility to a telecommunications network in Australia
10	the person manufactures or supplies customer equipment for use, or likely to be used, in Australia	(a) the manufacture by the person of any such customer equipment; or (b) the supply by the person of any such customer equipment
11	the person manufactures or supplies components for use, or likely to be used, in the manufacture of customer equipment for use, or likely to be used, in Australia	(a) the manufacture by the person of any such components; or (b) the supply by the person of any such components
12	the person: (a) installs or maintains customer equipment in Australia; and (b) does so otherwise than in the capacity of end-user of the equipment	(a) any such installation by the person of customer equipment; or (b) any such maintenance by the person of customer equipment
13	the person: (a) connects customer equipment to a telecommunications network in Australia; and	any such connection by the person of customer equipment to a telecommunications network in Australia

	(b) does so otherwise than in the capacity of end-user of the equipment	
14	the person is a constitutional corporation who: (a) manufactures; or (b) supplies; or (c) installs; or (d) maintains; data processing devices	(a) the manufacture by the person of data processing devices for use, or likely to be used, in Australia; or (b) the supply by the person of data processing devices for use, or likely to be used, in Australia; or (c) the installation by the person of data processing devices in Australia; or (d) the maintenance by the person of data processing devices in Australia
15	the person is a constitutional corporation who: (a) develops; or (b) supplies; or (c) updates; software that is capable of being installed on a computer, or other equipment, that is, or is likely to be, connected to a telecommunications network in Australia	(a) the development by the person of any such software; or (b) the supply by the person of any such software; or (c) the updating by the person of any such software

[ii] By s 100.1(2) of the Criminal Code, an essential element of a terrorism offence is action that:

(a) causes serious harm that is physical harm to a person; or

(b) causes serious damage to property; or

(c) causes a person's death; or

(d) endangers a person's life, other than the life of the person taking the action; or

(e) creates a serious risk to the health or safety of the public or a section of the public; or

(f) seriously interferes with, seriously disrupts, or destroys, an electronic system including, but not limited to:

(i) an information system; or

(ii) a telecommunications system; or

(iii) a financial system; or

(iv) a system used for the delivery of essential government services; or

(v) a system used for, or by, an essential public utility; or

(vi) a system used for, or by, a transport system.

[iii] https://carnegieendowment.org/programs/technology/cyber/encryption states:

'The Carnegie Endowment for International Peace and Princeton University have convened a small group of experts to advance a more constructive dialogue on encryption policy. The working group consists of former government officials, business representatives, privacy and civil rights advocates, law enforcement experts, and computer scientists. Observers from U.S. federal government agencies attended a select number of working group sessions. Since 2018, the working group has met to discuss a number of important issues related to encryption policy, including how the relevant technologies and uses of encryption will evolve in the future.'

Its document 'Key Takeaways from the Encryption Working Group's Paper on "Moving the Encryption Policy Conversation Forward" states:

'The working group rejects two straw men—absolutist positions not actually held by serious participants, but sometimes used as caricatures of opponents. These are:

(1) that we should stop seeking approaches to enable access to encrypted information

(2) that law enforcement will be unable to protect the public unless it can obtain access to all encrypted data through lawful process.

We believe it is time to abandon these and other such straw men. More work is necessary, such as that initiated in this paper, to separate the debate into its component parts and examine risks and benefits in greater granularity. There will be no single approach for requests for lawful access that can be applied to every technology or means of communication. Mobile phone proposals should be evaluated against adherence to core principles. The working group has identified core principles against which to judge proposals for mobile phone encryption access. The group agrees that proposals should, at a minimum, adhere to these principles.

- *Law Enforcement Utility*: The proposal can meaningfully and predictably address a legitimate and demonstrated law enforcement problem.
- *Equity*: The proposal offers meaningful safeguards to ensure that it will not exacerbate existing disparities in law enforcement, including on the basis of race, ethnicity, class, religion, or gender.
- *Specificity*: The capability to access a given phone is only useful for accessing that phone (for example, there is no master secret key to use) and that there is no practical way to repurpose the capability for mass surveillance, even if some aspects of it are compromised.

Few public statements from national governments, for example, have distinguished between approaches for data at rest and data in motion. Similarly, when groups raise concerns about undermining encryption, they tend to emphasize the general risks versus those related to specific applications of encryption.

Key Takeaways from the Encryption Working Group's Paper on "Moving the Encryption Policy Conversation Forward"

[iv] In *Graham v Minister for Immigration and Border Protection; Te Puia v Minister for Immigration and Border Protection* [2017] HCA 33 (6 September 2017) the plurality (Kiefel CJ, Bell, Gageler, Keane, Nettle And Gordon JJ) stated (citations omitted):

38. Resolution of the issue concerning s 75(v) of the Constitution requires a return to first principles.

39. As the plaintiff's argument with respect to inconsistency correctly apprehended, all power of government is limited by law. Within the limits of its jurisdiction where regularly invoked, the function

of the judicial branch of government is to declare and enforce the law that limits its own power and the power of other branches of government through the application of judicial process and through the grant, where appropriate, of judicial remedies.

40. That constitutional precept has roots which go back to the foundation of the constitutional tradition of which the establishment of courts administering the common law formed part. By the time of the framing of the Australian Constitution, the precept had come to be associated in the context of a written constitution with the decision of the Supreme Court of the United States in Marbury v Madison. The precept has since come to be associated in the particular context of the Australian Constitution with the decision of this Court in Australian Communist Party v The Commonwealth. There Dixon J referred to the Australian Constitution as "an instrument framed in accordance with many traditional conceptions, to some of which it gives effect, as, for example, in separating the judicial power from other functions of government, others of which are simply assumed", adding that "[a]mong these I think that it may fairly be said that the rule of law forms an assumption". There also Fullagar J observed that "in our system the principle of Marbury v Madison is accepted as axiomatic, modified in varying degree in various cases (but never excluded) by the respect which the judicial organ must accord to opinions of the legislative and executive organs".

41. Acceptance by the framers of the Australian Constitution of the principle in Marbury v Madison was combined with a desire on their part to avoid replication of the actual outcome in that case. The outcome had been that the Supreme Court had held that Congress lacked legislative power to authorise the Supreme Court to grant mandamus to compel an officer of the United States to perform a statutory duty.

42. The upshot was the inclusion within Ch III of the Constitution of s 75(v), which confers original jurisdiction on the High Court in all matters in which a writ of mandamus or prohibition or an injunction is sought against an officer of the Commonwealth, and of s 77(i) and (iii) in so far as those provisions empower the Commonwealth Parliament to confer or invest equivalent statutory jurisdiction on or in other courts. The power of a court exercising jurisdiction under, or derived from, s 75(v) to grant a writ of mandamus or prohibition or an injunction against an officer of the Commonwealth is a power to enforce the law that limits and governs the power of that officer.

43. What follows from the inclusion of s 75(v) in the Constitution is that it is "impossible" for Parliament "to impose limits upon the quasi-judicial authority of a body which it sets up with the intention that any excess of that authority means invalidity, and yet, at the same time, to deprive this Court of authority to restrain the invalid action of the court or body by prohibition". The same is to be said of the impossibility of Parliament imposing a public duty with the intention that the duty must be performed and yet depriving this Court of authority by mandamus to compel performance of the duty imposed and of the impossibility of Parliament imposing a constraint on the manner or extent of exercise of a power with the intention that the constraint must be observed and yet depriving this Court of authority by injunction to restrain an exercise of that power rendered unlawful by reason of being in breach of that constraint.

44. The presence of s 75(v) thus "secures a basic element of the rule of law".

[v] The *Telecommunications Amendment (Repairing Assistance and Access) Bill* 2019 would provide as follows:

317ZG Designated communications provider must not be requested or required to implement or build a systemic weakness or systemic vulnerability etc.

(1) A technical assistance request, technical assistance notice or technical capability notice must not have the effect of:

(a) requesting or requiring a designated communications provider to implement or build a systemic weakness, or a systemic vulnerability; or

(b) preventing a designated communications provider from rectifying a systemic weakness, or a systemic vulnerability.

(2) The reference in paragraph (1)(a) to implement or build a systemic weakness, or a systemic vulnerability, includes a reference to implement or build a new decryption capability.

(3) The reference in paragraph (1)(a) to implement or build a systemic weakness, or a systemic vulnerability, includes a reference to one or more actions that would render systemic methods of authentication or encryption less effective.

(4) The reference in paragraph (1)(a) to implement or build a systemic weakness, or a systemic vulnerability, includes a reference to any act or thing that would or may create a material risk that otherwise secure information would or may in the future be accessed, used, manipulated, disclosed or otherwise compromised by an unauthorised third party.

(5) The reference in subsection (4) to otherwise secure information includes a reference to the information of, about or relating to any person who is not the subject, or is not communicating directly with the subject, of an investigation to which the relevant technical assistance request, technical assistance notice or technical capability notice relates.

(6) The reference in subsection (4) to an unauthorised third party includes a reference to any person other than:

(a) the person who is the subject of, or who is a person communicating directly with the subject of, an investigation to which the relevant technical assistance request, technical assistance notice or technical capability notice relates; or

(b) the person that issued, or asked the Attorney-General to issue, the relevant technical assistance request, technical assistance notice or technical capability notice.

(7) Subsections (2), (3) and (4) are enacted for the avoidance of doubt.

(8) A technical assistance request, technical assistance notice or technical capability notice has no effect to the extent (if any) to which it would have an effect covered by paragraph (1)(a) or (b).

[vi] IPCO issued a press release stating in part:

- **Australia's terror legislation watchdog consults UK partners**

20/11/2019

Last week, Australia's Independent National Security Legislation Monitor (INSLM), Dr James Renwick, visited London as part of his national security consultation.

During his visit, Dr Renwick met with the UK's Investigatory Powers Commissioner, Sir Brian Leveson, to learn more about the UK's use and oversight of investigatory powers. Dr Renwick also met with the Technology Advisory Panel (TAP), which provides information on the impact of changing technology and developments in the use of investigatory powers that could limit privacy interference.

Sir Brian Leveson, the Investigatory Powers Commissioner, said:

"I was delighted to welcome Dr Renwick to IPCO and to share with him the ways in which the Investigatory Powers Act provides the assurance of oversight in this very difficult area, providing an appropriate balance between privacy and security.

"I hope that what this country has done will assist Australia as it grapples with similar issues."

Dr James Renwick, Australia's INSLM, said:

"Many of Australia's agencies do not require a judicially-issued warrant to undertake their activities, and increasingly, Australian civil society is calling for such authorisations.

"Learning how IPCO, its judicial commissioners and the Technology Advisory Panel work to review intrusive warrants, often involving complex technology, has been immensely helpful in my consideration of how such a model might work in Australia."

Sir Bernard Silverman, Chair of the Technology Advisory Panel, said:

"In an increasingly digital world, the Technology Advisory Panel performs an important role in providing Judicial Commissioners with the fullest possible scientific and technical awareness in carrying out their crucial duties. "It is a pleasure to be able to share our experiences with our Australian counterparts and exchange ideas on how best to support oversight processes in both our nations."