Dr James Renwick CSC, SC

Independent National Security Legislation Monitor

WHAT ARE THE RIGHT ENCRYPTION LAWS FOR AUSTRALIA?

LOWY INSTITUTE, SYDNEY, 5 MARCH 2020[1]

In 2019 the Parliamentary Joint Committee on Intelligence and Security referred to me as INSLM for review the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth). As I move to finalise the report of the review, due no later than 30 June 2020, I here discuss possible models whereby the interests of individuals, organisations, business, intelligence, police and integrity agencies might be reconciled. Separately, I publicly announce my intention to consider what statutory amendments might be necessary to avoid any repetition of the wholly secret criminal proceedings involving 'Alan Johns'.

Introduction

1.1. It is an honour to be speaking at the Lowy Institute for the second time in a year, and my last time as INSLM, as I finish in that role on 30 June. In June last year I spoke[2] here about the INSLM role and its origins, and the counter-terrorism and counter-espionage threats: I refer you to that speech and also to my latest Annual Report which was tabled last week in Parliament and is on www.inslm.gov.au: suffice to say that:

- the espionage and foreign interference threat has increased,
- an onshore terrorism attack remains at the 'probable' level it has been since 2014,[3] and
- I expect ISIL will continue to surprise.

1.2. I also note the important comments by the Director-General of Security at the inaugural Annual Threat Assessment held at ASIO's headquarters last week, which I was privileged to attend.[4]

1.3. I also spoke here about my review concerning the loss of citizenship for terrorist activities.[5] The resulting report was delivered in August to the Attorney-General, the Hon Christian Porter MP, and led to a government response within weeks in the form of amending legislation: the key points of difference between my recommendations and the government's response are now being considered by the Parliamentary Joint Committee on Intelligence and Security (PJCIS).[6]

---

[1] Check against delivery. The views in this are my own.

[2] https://www.inslm.gov.au/sites/default/files/Lowy%20Institute%20Renwick.pdf

[3] 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.'

[4] https://www.asio.gov.au/director-generals-annual-threat-assessment.html

[5] Report to the Attorney-General: Review of the operation, effectiveness and implications of terrorism-related citizenship loss provisions contained in the Australian Citizenship Act 2007.

[6] Review of the Australian Citizenship Amendment (Citizenship Cessation) Bill 2019: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/CitizenshipCessat

1.4. As I am being hosted by Dr Shanahan today may I acknowledge his important work in this area, including his recent analysis with Jennifer Percival in the report: the 'Typology of Terror'.

1.5. The PJCIS is perhaps not as well-known as it should be given its importance.[7] One of its principal functions is ensuring, by the conduct of statutory reviews, that national security and counter-terrorism law remains necessary, proportionate and effective. It complements and bolsters my role as INSLM.[8] Indeed, it has been common for my reports to inform the work of the PJCIS as it considers whether such laws should be enacted, amended or repealed.[9] Although we each can and do hold public and private hearings, a key difference is that my 'Royal Commission' like powers give me access *as of right* to all relevant material regardless of national security classification.

1.6. In 2019 the PJCIS for the first time used its powers to refer a review to me,[10] namely of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)* (TOLA Act). I must report to it no later than 30 June, it must report to the Parliament no later than the end of September.[11]

1.7. When I spoke here last year I foreshadowed three principles which would – and still do – guide my inquiry. They are drawn in part from my former UK counterpart Lord David Anderson QC's report *A Question of Trust*.

- *First*, 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: in this context it means 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.
- *Second*, what the law permits and forbids must be clear.
- *Third*, oversight and safeguards are vital.

1.8. A few weeks ago I held public hearings: the transcript is on my website.[12] I have also consulted widely with industry both large and small, human rights groups,

---

ion. The Government has also now responded to my 2018 Report to the Prime Minister as to the Prosecution and Sentencing of Children for Terrorism Offences: https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;adv=yes;orderBy=date-eFirst;query=Dataset%3Atabledpapers%20Decade%3A%222020s%22%20Year%3A%222020%22;rec=1;resCount=Default

[7] It is constituted under section 28 of the Intelligence Services Act (ISA).

[8] I independently review the operation, effectiveness and implications of national security and counter-terrorism laws; and consider whether such laws contain appropriate protections for individual rights, remain proportionate to terrorism or national security threats, and remain necessary.

[9] Although the object of the INSLM Act is for the appointed INSLM to 'assist Ministers in ensuring that Australia's counter-terrorism and national security legislation' meet these requirements, this should be updated to reflect the fact that I also assist the PJCIS in that task.

[10] By s 7A of the INSLM Act the PJCIS may refer to me any matter which it 'becomes aware of in the course of performing its functions … and … considers should be referred' to me. By operation of ss 6(1) and (1A) of the INSLM Act I was thus required, independently, to consider the 'operation, effectiveness and implications' of TOLA and also, to the extent I considered it necessary and appropriate, of my own motion, any of the '*counter-terrorism and national security legislation*' as defined in the INSLM Act, and 'any other law of the Commonwealth to the extent that it relates' to that defined list.

[11] *Telecommunications (Interception and Access) Act 1979, s 187N.*

[12] https://www.inslm.gov.au/sites/default/files/2020-02/INSLM%27s%20Opening%20Statement%20-%20TOLA%20Public%20Hearing.pdf

civil society, police, intelligence and oversight bodies both here and in the UK and the USA.

1.9. Here in Australia, and internationally, there is great interest in, and strong views about, TOLA, which is seen as far reaching and novel in its scope. The short period allowed for consultation on the TOLA Bill clearly caused lingering disquiet, even anger. Some say that brevity of itself means that the TOLA Act should be repealed, with consultation to begin again, not least as a way of regaining trust. Realistically, I do not think that is likely nor do I think it is appropriate to recommend it.

1.10. Other submitters, perhaps the majority, have focused on three main areas for reform, which are also my focus:

- The definitions in the TOLA Act of *systemic weakness* and *systemic vulnerability*, and how disputes concerning the application of these statutory terms can be resolved.
- Where the current TOLA decision makers are the Attorney-General or agency heads, replacing them with current or retired judges, assisted by technical experts who understand the effect of the exercise of particular TOLA powers on privacy and on the effectiveness of encryption.
- 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 by complaining to the Commonwealth Ombudsman or the Inspector-General of Intelligence and Security.

Context of TOLA's enactment

1.11. Because this is such a technical area it is impossible today to discuss the full context, legal and technological. But let me try and discuss the key concepts.

1.12. First, let me start with some definitions.

- When I speak about the *World Wide Web*, I acknowledge it is fragmenting, if it has not already separated, due to extensive firewalls in China, Russia and elsewhere. (I also note the increasing importance of the *Internet of Things* now that we have 'smart' cars, fridges and so on.)
- By data "content" I mean such things as texts, emails, phone calls, videos and pictures.
- By "metadata" I mean such things as when an email was sent, the sender and recipients, their locations, how it was sent, how it was stored, and what websites have been visited, what apps were used and so on.
- Sometimes data is 'in motion' for example a phone call as it is being made; sometimes it is 'at rest', such as when either content or data is stored on a device or in the 'cloud'. [13]

[13] 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

1.13. Let me to say something about the context of the TOLA Act, and that is not easy as it includes dynamic events, not yet fully understood.

1.14. For example, today's Australian newspaper said:

> *Home Affairs Minister Peter Dutton will meet security ministers from the Five Eyes intelligence alliance in Washington on Thursday, in a bid to finalise a global agreement that would force Facebook and Google to help shut down live streaming and sharing of child sex abuse.*
>
> *The top-level forum to be hosted at the White House will coincide with the introduction of a bill today to the Australian parliament that would enact mirror laws with the US CLOUD Act.*
>
> *This would allow reciprocal rights for both US and Australian security agencies to issue warrants for data held offshore by cloud providers in hunting down terrorists and child sex networks.*[i]

1.15. Just this week the AFP Commissioner wrote that 'The AFP has an urgent need for a legal framework that provides faster and more effective access to electronic data held or controlled overseas, where it is critical to Australian investigations and prosecutions.'[ii] So it may be effective diplomacy as well as good law reform to adopt this model here.

1.16. And indeed, the first item of business in the House of Representatives today was the introduction of the *Telecommunications Legislation Amendment (International Production Orders) Bill 2020.*

1.17. Other events include the following.[14]

1.18. There is the near universal use of the web in Australia and comparable countries for legitimate private, commercial and government communications.

1.19. As our digital footprints grow with our web searches and purchases online, and our communications by texts and emails, and on social media, those entities who provide our means of using the web – called designated communications providers (DCPs) in TOLA – analyse, and then profit from having, our personal and commercial information, for example by 'data mining' it using proprietary algorithms. The ubiquity of the web has led to the largest 'tech titan' DCPs having enormous (although opaque) power, which is in some ways greater than many nation states.

1.20. The full extent of their monetisation of personal and commercial information is unknown and perhaps unknowable, and so, although I accept that reputable companies do seek and obtain consumers' consent, there may be no real capacity to give informed consent to it by any consumer. Such developments alone have led to demands for greater privacy rights, including what in the European Union has been called the 'right to be forgotten'.[15] They have also led, in Australia, to increased interest from regulators, including the national competition regulator, the Australian Competition and Consumer Commission (ACCC) which has, for example:

---

[14] This draws on my opening remarks at my recent public hearings.

[15] See, eg the EUCJ decision of *Google Spain SL, Google Inc. v Agencies Española de Protection de Dates, Mario Costean González* (2014) and the EU General Data Protection Regulation: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

- Taken Google to the Federal Court alleging it made false or misleading representations to consumers about the personal location data Google collects, keeps and uses;
- Concluded its important *Digital Platforms Inquiry* which among other matters found that 'the market power of Google and Facebook has distorted the ability of businesses to compete on their merits in advertising, media and a range of other markets';[16]
- Proposed far-reaching reforms aimed, among other matters, at protecting quality Australian journalism and also ensuring a realistic way of consumers giving fully informed consent to private providers as to the use of private data.

1.21. The fact that there is now a greater range of information about each of us in existence than there ever has been before, and that we do not fully know or understand what personal data *is* on our phones or computers, nor which commercial entities have access to it or use it, are facts that remain highly relevant to my review because, if we are ignorant about, say, what is on our mobile devices and how its content is used commercially, we equally cannot fully comprehend in advance how it might be used in a later investigation or prosecution by police, intelligence or integrity agencies who might obtain the data or content by legally authorised compulsion.

1.22. To give an analogy with the physical world, if my paper diary or notebook is seized under warrant, or even if my house is searched, I know and can comprehend what is being searched and seized. But if my computer or mobile phone is seized and fully accessed for example by decryption of all passwords, I probably will not know even approximately what it contains nor how it might be used. Nor for that matter, might a judge issuing a warrant fully comprehend these matters, at least without access to some really good technical advice.

1.23. So if this is an example of where the analogy between the virtual and physical worlds breaks down, one consequence is that it cannot be assumed that old and apparently robust safeguards, developed over many years for the use of police and intelligence powers in the physical world, remain adequate.

1.24. So far I have just spoken about lawful use. The universal use of the web attracts criminals and other bad actors and thus the internet and the world wide web is increasingly where the age-old struggle between police and criminals, and spies and intelligence agencies, is carried on, and in new ways.

1.25. For example:

- ISIL has made very effective use of the web to publicise, proselytise, and direct terrorism;
- The Christchurch shooter live-streamed his atrocities on social media;[17]
- There is large scale theft of private data and corporate intellectual property;
- There is local and transnational organised crime, money-laundering, trafficking of illicit drugs and arms and child sexual exploitation, including in

[16] https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platforms-inquiry

[17] 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.

the dark web which facilitates the commission of such crimes anonymously and thus with impunity.

- Nation States and their proxies continue to engage in espionage and foreign interference but they also work on their capacities to engage in cyber-attacks such as Computer Network Attacks which not only allows nation states and their proxies 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 Australian law.[iii]
- The New York Times' *Privacy Project*[18] provides many examples of such behaviour, and also of the large scale theft of private data and corporate intellectual property – as do the unsealed indictments filed by the US Department of Justice against, for example, members of the Chinese People's Liberation Army.[19]

1.26. The response by both legitimate and bad actors to these activities has been to almost universally encrypt content, and to encrypt some metadata. The evidence I have received is that the so-called 'golden age' when content could immediately be read and comprehended by police, integrity and intelligence agencies has gone. Instead, they now speak of a virtual world which has gone 'dark', gone 'spotty' or even gone 'different' and this change was a key impetus for the TOLA Act.

There is no binary choice between encryption and policing or intelligence work

1.27. Not only are the topics I have mentioned vast and complex, but they sometimes attract strident overstatement based on extreme or improbable examples.

1.28. So I am very grateful for the clear and informed thinkers in this field, a number of whom have made submissions. May I quote from two. First, the Encryption Working Group assembled by the Carnegie Endowment and Princeton University[20] recently said:

---

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

[19] 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

[20] 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

'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; and

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

1.29. Similarly Sir David Omand, a former spymaster as head of GCHQ, in his recent book,[21] *Principled Spying,* wrote:

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.[22]

I agree with both statements: the choice is not binary.

Pre-TOLA

1.30. The context having been sketched out, what, then, does TOLA change, and how, if at all, should it now be amended? Let me continue to use the familiar example

---

(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"

[21] Oman and Phytin, *Principled Spying, the Ethics of Secret Intelligence*, Oxford University Press, 2018.

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

of the mobile phone (rather than be diverted into such matters as the detail of computer networks.[23])

1.31. In substance, for many years before 2018 there have been federal laws permitting law enforcement, intelligence and integrity bodies to obtain the mobile phone itself and to search and copy the content and data on the device, and to intercept and access content and data in motion (such as what was said in a phone call).

1.32. There is a patchwork of lengthy and frequently amended Acts which allows this, but in essence it is to be found in four main Acts: the *Surveillance Devices Act 2004* (SD Act),[24] the *Australian Security Intelligence Organisation Act 1979 (ASIO Act), the Telecommunications (Interception and Access)* Act 1979 (TI Act), and the *Crimes Act* 1914. The legal scheme rapidly gets more complex. But in substance, prior to TOLA the AFP and ASIO, for example, might:

a. Under the *TI Act*: seek access to telecommunications data, stored communications that already exist, or the interception of communications in real time. (That access might be given by a telecommunications provider without the need to obtain the actual mobile phone.[25])
b. Under the *SD Act* or the *ASIO Act:* a Computer Access Warrant which could authorise covert access and copying what is in a phone (or computer);
c. Under the Crimes Act: [26] AFP constables executing warrants either in respect of premises[27] or in respect of a person[28] could search for and seize 'evidential material'[29] - which includes things 'in electronic form'[30] and to move a thing found at warrant premises 'to another place for examination or processing'.[31]

1.33. What then are the safeguards at the federal level?

a. *Permission* for such access is granted by warrant issued by an independent eligible judge or Tribunal member for the AFP, and by the Attorney-General for ASIO. (Looking at police approvals, the application process is not centralised and there are insufficient details publicly available about who approves, how long they take to do so, how many applications are knocked back and for what reason. Very little is publicly known about the ASIO process although some secret statistics are made available to a limited audience, including me.)
b. *Complaints* can be made to the Ombudsman for the AFP or the IGIS for ASIO.
c. There is a constitutionally entrenched[iv] right to judicially review decisions of officers of the Commonwealth under the TOLA Act in Australia, our founders having had in mind the US Supreme Court case of *Marbury v Madison.*[32]

---

[23] There are real technical complexities here which time prevents me from dealing with: to give one example considered by the Carnegie/Princeton group it is important to distinguish between data in the cloud, data in motion, and data on devices.
[24] A data surveillance device, a listening device, an optical surveillance device or a tracking device;
[25] 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.
[26] And Customs, now Australian Border Force Officers have significant powers as well.
[27] *Crimes Act 1914* (Cth) (Crimes Act) s3C(1).
[28] Crimes Act s3C(2).
[29] Crimes Act s3F(1)(c), in respect of a warrant in force in relation to premises.
[30] Crimes Act s3C(1).
[31] in certain circumstances : Crimes Act s3K(2).
[32] 5 US 137; see, eg https://www.law.cornell.edu/supremecourt/text/5/137

d. Certain laws can be reviewed by me and the PJCIS.

TOLA

1.34. In Schedule 1 of TOLA, 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 DCP[v] must make the unintelligible content or data intelligible, or do another 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.[vi]

1.35. Next, by a technical capability notice (TCN), an agency may request the Attorney General to grant a compulsory notice 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 decrypted, for example. The same civil and criminal protections apply.

1.36. 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'*.

1.37. 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 significant departure from the normal course of an independent eligible judge or tribunal member as the issuer. The Attorney-General issues a TCN (and TANs for ASIO) 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.

1.38. (In Schedule 2 the position is similar with, for example, Computer Access Warrants.

1.39. 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.[vii])

What might be done?

1.40. My current views are as follows.

1.41. First, as to *necessity*, I agree that 'going dark' has created a large problem for police, intelligence and integrity agencies, so justifying a proportionate but not absolute legislative response. (I have already announced that for so long as the police have access to TARs and TANS so should the State and Territory ICACs, who have said how important these powers are to their work in ensuring integrity in government administration, including for police.)

1.42. Second, there is at least some evidence that the law is either *effective* or capable of being made effective, especially in relation to the powers in Schedules 2-5, and for the TARs and TANs in Schedule 1. The publicly available material does not show that TANs have been used, because requests have been complied with

voluntarily, but the use of TARs shows TANs are capable of being effective. There is however no public evidence that the more intrusive TCN which is for the creation of a new capability has yet been used.

1.43. The real question for me is whether any of these powers are proportionate to the undoubted threats - especially of criminality - that exist. And the answer to that question must focus on the thresholds and safeguards for their use.

1.44. Where in Schedules 2-4, the powers are expanded, for example, to require a password to be provided to a mobile phone but that power is safeguarded because it is granted by the same independent person, say, a judge, that previously granted access to the underlying content, then the power is more likely to be proportionate to the threats.

1.45. In contrast, approval by agency heads or the Attorney-General is what makes the Schedule 1 powers look like outliers. I think it is wrong to minimise the significance of the new Schedule 1 powers as merely making existing laws 'technology proof' by giving access to content which the authorities already have.[viii] The key impetus for Schedule 1 was that content was no longer readable or comprehensible especially because of encryption.

1.46. So my clear starting point is that where the encrypted content can only be obtained by judicially approved warrant or authority, the same thresholds and levels of approval should apply for giving unencrypted access. Thus TANs and TCNs should be issued, or at least subject to a 'double lock' approval system, by a judge, serving or retired rather than an agency head or the Attorney.

1.47. Next, I think the same rules should apply to TARs even though they are voluntary because of their likely impact upon the rights of third parties who do not know and cannot consent to the TAR.

1.48. The next question is whether the technical complexity of what is being authorised requires senior lawyers with access to top level technical advice. I think it does and there is an excellent operating model to look to in the United Kingdom.

IPCO

1.49. In November, I had the privilege of meeting with the Investigatory Powers Commissioner's Office, or IPCO, in the UK. It arose from my counterpart's report, "A Question of Trust." It is now headed-up by Sir Brian Leveson, a famous and senior ex-judge, and there are 15 senior retired judges, and some very distinguished technical advisers.

1.50. It works in this way: there is a double-lock system, so that if you can imagine a warrant or authorisation application is given first to the Minister, the same paperwork is then given to IPCO. IPCO doesn't look at all the matters the Minister looks at, for example, effects on international relations, but does ask, *looking at the same material the Minister did*, is the application lawful, proportionate, and reasonable? And if it's not, then the request is ineffective hence the 'double lock'.

1.51. Having spent time with both IPCO and security and police agencies in the UK, I can say it's been very well-received, not least because it has raised the level of trust. My conversations on both sides of the Atlantic Ocean in the US and the UK, made it clear to me that IPCO was critical to the UK obtaining a CLOUD Act agreement from the United States. Australia seeks such an agreement as I noted earlier.

1.52. What if Australia wants to use something which already exists rather than create an IPCO? Well, there is something which already exists, and has done for a long time, and that is the Administrative Appeals Tribunal (AAT); it is independent of government, headed by a Federal Court judge, its Deputy Presidents can be other federal judges or senior lawyers, and it already grants some warrants, and already reviews some ASIO decisions.

1.53. So one possibility is that an application – for at least a TAN, TAR and TCN – could go for approval to the Security Division of the AAT, which is accustomed to dealing with highly sensitive or secret information. Now, a DCP which doesn't object to a TAN or a TCN needn't appear; if it did object, for example, as to whether the request was reasonable or proportionate, or created a systemic weakness, you could resolve it at a contested hearing. You could also use one of the alternative dispute resolution processes currently available in the AAT.

1.54. Because there is a lot of technical material to be understood, the Presidential Member could, with advantage, sit with an eminent scientific or technical expert who would be appointed as a part-time member. To the extent they could publish at least some of their reasons, that would guide agencies and DCPs alike.

1.55. There would also be a central registry which would ensure the security of classified materials, and awareness of similarity with previous applications.

1.56. Appointment to the AAT of say, half a dozen distinguished technical experts whose expertise would cover the likely range of technical questions in issue is desirable, and they could also have a joint role working as consultants for the IGIS and the Ombudsman in their respective audit functions. This is effectively what happens with IPCO.

1.57. I consider that these difficult and important decisions should be made by judges of the higher courts; there may be something to be said for appointing them for a single, non-renewable term. The new bill produced today is also highly significant, as I understand it, for the first time some ASIO authorisations are to be issued by the AAT, rather than the Attorney-General. If this becomes the law it may be irresistible that the Attorney no longer issue other ASIO warrants on authority.

1.58. In the written paper I note some other matters.

1.59. [The role of the Ombudsman and the Inspector General of Intelligence and Security for police on the one hand and intelligence agencies on the other is absolutely vital. In order for them to do their job given the large number of times some of the powers in TOLA or related powers are being used I will make a series of recommendations about keeping proper statistics which are available to them so they can better perform their task. I will also recommend that there be a standard or prescribed form of notice under Schedule 1 of TOLA which will let the DCP, which will not always be a large or sophisticated corporation, understand their rights and duties and also the limitations for example on the protections available to them. I expect those categories of recommendations to be relatively uncontroversial.

1.60. The second and much more difficult category is the idea of systemic weakness or systemic vulnerability and in the case of all the powers under Schedule 1, TARS, TANs and TCNs, they can't be used in such a way as to create a systemic weakness or vulnerability. If they do, they are invalid so the obtaining of the information by the agency would be unlawful but that invalidity also means that the protection from being sued by customers of the DCPs would also fall away so that definitions are critical.

1.61. You will see from many of the submissions to the inquiry that there is criticism of the definitions. The challenge I have set for all the DCPs and other submitters is to come up with better definitions than exist now. One way of doing so would be to give statutory examples of what is or is not for example a systemic weakness and put it in the statute rather than in a supplementary explanatory memorandum. Another option may be to very significantly alter the definitions. I invite people to come up with better definitions and justify them and I will consider them along with my technical advisers. I note there is a current bill in the Senate which does just that and which I will consider.

1.62. 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 as their first call either a criminal prosecution in the case of the agency or a civil case seeking a declaration that the line has been crossed and the purported obligation need not be complied with.

1.63. 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. I again note the potential significance of today's Bill.

1.64. Where there is no agreement, I recommend that the Attorney General no longer have a role in relation to issuing the TCNs but rather the TANs and the TCNs can only be issued by again the Security Appeals Division of AAT constituted by in each case a presidential member and a senior member who is an eminent scientific or technical member.]

1.65. A guiding principle of the exercise of any coercive power is that it must be exercised lawfully, responsibly and appropriately. These values are underpinned by the higher value of trust. Any scheme involving the use of coercive power must have the necessary checks and balances not only to ensure that agencies exercising those powers make correct and lawful decisions, but that such decisions are seen to be made. It is only through doing so that agencies will instil and inspire the community's trust in their exercise of new powers in our sceptical age.

New Inquiry

1.66. In December last year it came to public attention that federal criminal proceedings in the ACT Supreme Court had been held in a closed court by an order made under section 22 of the *National Security Information (Criminal and Civil Proceedings) Act* (NSI Act). The court order prohibited the disclosure of the nature of the offending or the provisions under which the defendant had been charged or convicted.

1.67. The publicly known facts reveal that there has been an apparently unique set of circumstances whereby a person known as Alan Johns was charged, arraigned, pleaded guilty, sentenced, and served his sentence with minimal public knowledge of the details of the crime – we know only that is was for 'mishandling classified

information'. The Attorney-General advises that 'the matter is unique in my experience, and I am not aware of any other similar cases.' I agree with him. Wholly closed criminal proceedings do indeed appear to be unprecedented in Australia, save possibly during the World Wars.

1.68. To be clear, this matter was quite different from cases where there are in criminal proceedings:

a. Temporary non-publication orders to protect the administration of justice, for example by keeping the fact of a conviction, or the nature of evidence given, in open court confidential, so as not to prejudice the fair trial of the accused or a co-accused;

b. Permanent non-publication and related closed court orders to protect the identities of a person whose identity is protected by common law or statute;

c. Orders made by a court setting aside a subpoena or refusing access to a document on the grounds of public interest immunity privilege in which case such material is not received into evidence at all.

1.69. Criminal proceedings, in this case involving the judicial power of the Commonwealth, differ from civil proceedings or a private arbitration not least because of the public interest in the administration of criminal justice. This means that the circumstance that the Attorney-General and the accused agreed on secrecy orders is the beginning of the argument, not the end of it. Very many accused have an interest in their criminal proceedings and sentence not being known as it adversely affects their reputation and may affect their treatment by other prisoners.

1.70. The public interest in open justice is particularly strong in criminal proceedings. I understand that the interests of justice even in criminal matters may require modification of the open justice principle: see, eg *Hogan v Hench* [2011] HCA 4; *T v The Queen* [2019] HCA 40.

1.71. I stand by my statement to the Senate this week as follows: '*As far as we know there has never been another case, at least in peacetime in Australia, where all of it has been conducted in secret. That is something significant and different, and for my part, I would not like to see it repeated.'*

1.72. In order to ensure that the law permits suppression orders which are proportionate and only made to the extent necessary, I ask whether the NSI Act should require that, or at least require the court to consider whether:

a. a contradictor, such as media interests, or a special advocate (such as is now provided for in control order matters) should be heard,

b. at least some details of the charges and orders should always be publicly known,

c. reasons should always be given by the presiding judge for the exceptional step of departing from the strong presumption of open criminal justice. I will consider whether amendments to the NSI Act or indeed any other federal statute or rule should be recommended to avoid a repetition of these apparently unique facts. I will report on this matter in my final Annual Report which I will deliver by the end of my term

1.73. I now invite submissions as to amendments to the law to avoid a repetition of these apparently unique facts.

1.74. In conclusion, I reiterate what I said in my last Lowy speech which is that I look forward to the remainder of my time as INSLM, a role in which I am privileged to serve.

Dr James Renwick CSC SC

5 March 2020

---

[i] Simon Benson 'Five Eyes closes on tech child sex deal' https://www.theaustralian.com.au/nation/politics/five-eyes-closes-on-tech-child-sex-deal/news-story/0464b5e9e4681db8c57be0c011192830

[ii] The Australian 3/3/20: Police need faster access to overseas information to fight crime and keep Australians safe: Reece Kershaw.

[iii] 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.

[iv] In *Graham v Minister for Immigration and Border Protection; The Puja v Minister for Immigration and Border Protection* [2017] HCA 33 (6 September 2017) the plurality (Keitel CJ, Bell, Gaveller, 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 imposedhttp://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/HCA/2017/33.html?context=1;query=marbury;mask_path=au/cases/cth/HCA - fn27 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] 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.

[vii] As I said in my written opening at the public hearings:

> 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.

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.

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.

[viii] Law enforcement agencies, security agencies and the Department of Home Affairs contended that there are already a number of conditions applicable to the issuing of industry assistance notices that help ensure the responsible use of those notices. A primary argument raised in these submissions is that a distinction needs to be drawn between the compulsory industry notices and warrants or other like instruments. That distinction is said to be between a tool that provides 'content' and one that merely provides 'access' to content. For instance, the Department of Home Affairs submitted that industry assistance notices do not empower agencies to obtain content without an underlying warrant, but are instead merely a mechanism to ensure that whatever content is obtained under a pre-existing warrant accessible and comprehensible to the agency. For that reason, these agencies and the Department contend that it is unnecessary to require any independent or external authorisation of an industry assistance notice distinct from the independent and external authorisation of the warrant to which it relates.

These submissions also contended that there already exist relatively rigorous conditions on the issue of the compulsory industry notices, for instance through the statutory decision-making criteria, notification obligations and limitations on the scope of the power.

The security agencies and the Department of Home Affairs further contended that the executive arm of government routinely issues certain coercive warrants or instruments without any external approval (e.g., warrants issued by the Attorney-General at the request of security agencies). Some contend that this means Australia already has in place a double-lock approval mechanism, because it involves the request made by the Agency Head to be approved by an applicable Minister, potentially with the concurrence of other Ministers.

The security and law enforcement agencies also contended that their exercise of power to request the issue of various warrants and instruments is already subject to various reporting requirements, and to regular periodic review after the fact by the IGIS, the Commonwealth Ombudsman and similar agencies (depending on the agency). In the agencies' submissions, that external review is sufficient to ensure the lawful exercise of those powers.

Australian Government

Independent National Security Legislation Monitor

NEW REVIEW

THE OPERATION OF THE NATIONAL SECURITY INFORMATION (CRIMINAL AND CIVIL PROCEEDINGS) ACT 2004 (CTH) ARISING OUT OF THE MATTER OF ALAN JOHNS (A PSEUDONYM).

An own motion review

The *Independent National Security Legislation Monitor Act* confers an own motion power upon the INSLM to review at any time any of the defined '*counter-terrorism and national security legislation*', which includes the *National Security Information (Criminal and Civil Proceedings) Act 2004 (NSI Act)*. As INSLM, I independently review the operation, effectiveness and implications of national security and counter-terrorism laws; and consider whether such laws contain appropriate protections for individual rights, remain proportionate to terrorism or national security threats, and remain necessary. My 'Royal Commission' like powers as INSLM give me access *as of right* to all relevant material regardless of national security classification. I do not consider complaints.

I recently wrote to the Attorney-General saying:

> *I note with interest your response to Senator Patrick's Question on Notice 957 concerning 'Alan Johns'. In view of the public interest in the matter, and now that the Richardson Review has been completed, I have now decided of my own motion to consider the operation in that matter of the National Security Information (Criminal and Civil Proceedings) Act 2004 and I will make any necessary recommendations arising from that review in my final annual report (parts of which may need to be classified).*

The publicly known facts

Based upon a response by the Attorney-General to Question on notice no. 957 from Senator Rex Patrick, the following matters only have been officially stated or confirmed. They are the public or unclassified facts I assume for the purpose of my unclassified report on this review. There is a great deal of public speculation about the nature of the charges and the evidence supporting them. I am not authorised to disclose anything further than has been made public by the government, and no inferences should be drawn from this notice as to the true facts beyond those set out in it. Interested persons may however be assured that I will obtain, and then examine in private, the charges, evidence, submissions and transcripts of these closed proceedings. All that can be made public will be included in my final unclassified Annual Report to the Attorney-General.

1. ‘Alan Johns’ communicated confidential information contrary to a lawful obligation not to do so. The information was of a kind that could endanger the lives or safety of others. This risk remains.
2. Following an AFP investigation, the CDPP decided a prosecution was appropriate (given the Prosecution Policy of the Commonwealth, it may be assumed that the CDPP therefore considered it was in the public interest to prosecute and there were reasonable prospects of conviction).
3. The relevant offences provide that the Attorney-General’s consent is required before a prosecution can proceed. That consent was given.
4. The prosecution commenced in the ACT Magistrates Court and was ultimately heard in the ACT Supreme Court. The NSI Act was invoked to manage the protection of the national security information in the proceedings.
5. Once the NSI Act is invoked, the Attorney-General may be heard on issues relating to the disclosure and protection of national security information. The Attorney-General was represented by the Australian Government Solicitor in relation to the NSI Act.
6. The court made orders under section 22 of the NSI Act, with the consent of the relevant parties, that is, the Attorney-General and the accused, protecting the national security information. The orders provided for a mechanism for closure of the court in circumstances where highly sensitive national security information would have been disclosed, but did not prevent the defendant or his counsel from accessing the information.
7. Mr Johns was represented by counsel of his choice.
8. Mr Johns pleaded guilty to the offences. There was thus no jury trial which, given the CDPP presented an indictment, would have been by jury: *Constitution* s 80.
9. He was sentenced to a term of imprisonment for the offences. The term of imprisonment was two years and seven months, imposed across an aggregate of five charges. He was released from custody on recognisance to be of good behaviour for three years.
10. Consistent with the Supreme Court orders, Mr Johns may disclose the fact of his conviction and terms of his sentence and that the nature of his offending involved ‘mishandling classified information’. He may not otherwise disclose sensitive information including information that reveals the nature of his offending or the provisions against which he was charged or convicted. The Attorney-General states that ‘any further comment on this specific matter would be inappropriate in light of the court orders and the risks which led to those orders being made.’
11. The NSI Act balances the need to protect national security information with the principle of open justice and gives the court wide powers to make orders it considers appropriate about such matters. The nature of the national security information involved in this proceeding informed the Commonwealth’s position to seek protective orders. The Attorney-General advises that ‘the matter is unique in my experience, and I am not aware of any other similar cases.’

The scope of my inquiry and my request for submissions

The publicly known facts set out above reveal that there has been an apparently unique set of circumstances whereby a person was charged, arraigned, pleaded guilty, sentenced, and has served his sentence with minimal public knowledge of the details of the crime, as a result of consent orders which were not the subject of published judicial reasons. The limited facts

which are now known did not arise because the court orders so provided. Rather, the details of these closed proceedings were apparently revealed in passing in collateral civil proceedings, and as a result of questions in Parliament.

I have commenced this inquiry because of the importance of the principle of open justice including in matters which may relate to counter-terrorism or national security. Further:

1. I concur in the statement by the Attorney-General that 'the matter is unique in my experience, and I am not aware of any other similar cases'. Wholly closed criminal proceedings do indeed appear to be unprecedented in Australia, save possibly during the World Wars.
2. To be clear, this matter was quite different from cases where there are in criminal proceedings:

    a. Temporary non-publication orders to protect the administration of justice, for example by keeping the fact of a conviction, or the nature of evidence given, in open court confidential, so as not to prejudice the fair trial of the accused or a co-accused;
    b. Permanent non-publication and related closed court orders to protect the identities of a person whose identity is protected by common law or statute;
    c. Orders made by a court setting aside a subpoena or refusing access to a document on the grounds of public interest immunity privilege in which case such material is not received into evidence at all.

3. Criminal proceedings, in this case involving the judicial power of the Commonwealth, differ from civil proceedings or a private arbitration not least because of the public interest in the administration of criminal justice. This means that the circumstance that the Attorney-General and the accused agreed on secrecy orders is the beginning of the argument, not the end of it. Very many accused have an interest in their criminal proceedings and sentence *not* being known as it adversely affects their reputation and may affect their treatment by other prisoners.
4. The public interest in open justice is particularly strong in criminal proceedings.
5. I understand that the interests of justice even in criminal matters may require modification of the open justice principle: see, eg *Hogan v Hinch* [2011] HCA 4; *HT v The Queen* [2019] HCA 40. An example of powers in addition to the NSI Act is s 8 of the *Court Suppression And Non-Publication Orders Act 2010 (NSW)* which provides:

> **8 Grounds for making an order**
>
> (1) A court may make a suppression order or non-publication order on one or more of the following grounds:
>
> (a) the order is necessary to prevent prejudice to the proper administration of justice,
>
> (b) the order is necessary to prevent prejudice to the interests of the Commonwealth or a State or Territory in relation to national or international security,
>
> (c) the order is necessary to protect the safety of any person,

(d) the order is necessary to avoid causing undue distress or embarrassment to a party to or witness in criminal proceedings involving an offence of a sexual nature (including sexual touching or a sexual act within the meaning of Division 10 of Part 3 of the *Crimes Act 1900*),

(e) it is otherwise necessary in the public interest for the order to be made and that public interest significantly outweighs the public interest in open justice.

6. In order to ensure that the NSI Act permits suppression orders which are proportionate and only made to the extent necessary, I ask whether the NSI Act should require that, or at least require the court to consider whether:

    a. a contradictor, such as media interests, or a special advocate (such as is now provided for in control order matters) should be heard,
    b. at least some details of the charges and orders should always be publicly known,
    c. reasons should always be given by the presiding judge for the exceptional step of departing from the strong presumption of open criminal justice.

I will consider whether amendments to the NSI Act or indeed any other federal statute or rule should be recommended to avoid a repetition of these apparently unique facts. I will report on this matter in my final Annual Report which I will deliver by the end of my term as INSLM on 30 June 2020.

Dr James Renwick CSC SC
3rd INSLM
March 2020