SUBMISSION TO THE PJCIS REVIEW

Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

14/10/18

A combined submission from:
NSW Council for Civil Liberties
Liberty Victoria
Queensland Council for Civil Liberties
South Australian Council for Civil Liberties
Australian Council for Civil Liberties

Australian Council for Civil Liberties

INTRODUCTION

1. The Joint Council for Civil Liberties[1] (the Joint CCLs) welcome the opportunity to make this submission on the Telecommunications and Other Legislation Amendment (Assistance And Access) Bill 2018 (**the Bill**) to the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**).

2. NSWCCL and QCCL were party to a joint submission from a number of civil society bodies[2] to the Department of Home Affairs on the earlier exposure draft version of this Bill and the NSWCCL also made a separate supplementary submission[3] relating to unsatisfactory aspects of that review process.

3. In those submissions we expressed deep concern with key provisions in the exposure draft Bill and argued it should be rejected by Parliament. We have noted since then that these concerns were very widely shared across many civil society and business and industry groups[4]. We were also critical of the extremely short timeframe allowed for submissions on such a significant and complex proposal and queried the appropriateness of the Department of Home Affairs - in terms of transparency and independence - to conduct such a review.

4. Our unease regarding the review process was intensified when the amended Bill was cleared for Parliamentary consideration eight days after the closing date for submissions and brought into Parliament two days later.[5] This suggests that any consideration of the views presented in the submissions to the Department of Home Affairs must have been, at best, cursory.

5. There has been no public report by the Department of Home Affairs on its analysis of the submissions received nor any description or explanation of the amendments that have been included in the current Bill (Postscript: The Department of Home Affairs made a submission to this PJCIS Review which included its responses to some issues raised in its review process[6]. This

---

[1]NSW Council for Civil Liberties, Liberty Victoria, Queensland Council for Civil Liberties, South Australian Council for Civil Liberties, Australian Council for Civil Liberties.

[2] *Joint Submission by: Australian Privacy Foundation, Digital Rights Watch, Electronic Frontiers Australia, Future Wise, The Queensland Council for Civil Liberties, The New South Wales Council for Civil Liberties, Access Now, Blueprint for Free Speech. 10th September 2018. [Joint Submission PJCIS APF DRW PJCIS* https://www.homeaffairs.gov.au/consultations/Documents/digital-rights-watch.pdf

[3]*NSWCCL Submission to Department of Home Affairs Consultation on Exposure Draft Telecommunications and Other Legislation Amendment (Assistance and Access) Bill. 10th September 2018*

[4] The Department of Home Affairs has recently responded to the many calls for the submissions to be made public – a sample of around 100 submissions was initially published on the department site around about the 8/10/18 and a full list of submissions of those who agreed to publication around the 10/10/18. The CCLs have read a sample of these submissions. There has also been considerable criticism of the Bill in the media.

[5] Submissions closed on 10/9/18. It was reported that the Bill had been cleared by the Coalition on 18/9/18: *Political Alert,* 18/9/18 https://twitter.com/political_alert/status/1041888308278714368 and the amended Bill was tabled in Parliaments by the Minister for Home Affairs on the 20/9/18.

[6] Department of Home Affairs: *Parliamentary Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (submission number 18). (DHA Submission 18)

was too late to enable the Joint CCLs to consider it carefully. Some last minute references have been included in this Joint CCLs submission.

6. At the outset, the Joint CCLs' position is that Australians' safety is of great importance; however, it is imperative that the Government ensures that safety and security measures are necessary, adequate and proportionate. That is to the measures are required to keep Australians safe, that they are able to achieve the intended purpose (which we assume to be the prevention of serious offending) and that the measures to be implemented are proportionate to the reasonable expectations of the Australian community, including that Australians will not be subject to arbitrary interference into their private life.

7. The Bill has the potential to significantly and covertly interfere with Australians' (presently unprotected) human rights and, at the outset, it is the Joint CCLs' submission that the Australian Government ought to introduce enforceable human rights legislation without delay to ensure that Australians are afforded a complete and proper check and balances to any legislation which has the potential to interfere with civil liberties and fundamental human rights.

8. The Joint CCLs do not support the TOLA Bill 2018 in its current form.

MAIN ELEMENTS OF THE BILL

9. The Bill primarily amends the *Telecommunications Act 1997* and, by consequential amendment, also makes amendments to the followings Acts:
   a. *Federal Circuit and Family Court of Australia Act 2018* (to be introduced);
   b. *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018* (to be introduced);
   c. *Administrative Decisions (Judicial Review) Act 1977;*
   d. *Criminal Code Act 1995;*
   e. *Australian Security Intelligence Organisation Act 1979*;
   f. *Surveillance Devices Act 2004;*
   g. *International Criminal Court Act 2002;*
   h. *Customs Act 1901;* and
   i. *Crimes Act 1914*.

Objective

10. In his second reading speech, the Minister for Home Affairs, Peter Dutton justified the Bill on the basis that "*criminal syndicates and terrorists are increasingly misusing and, indeed, exploiting"* encryption. He argued that "*more than 90 per cent of data lawfully intercepted by the AFP is now encrypted in some form*" and the "*lack of access to encrypted communications presents an increasingly significant barrier for national security and law enforcement agencies in investigating serious crimes and national security threats*."

11. The Bill's objective is to provide law enforcement and intelligence/security agencies with "the tools they need to keep Australians safe" in the above context. [7] The central agenda is to provide tools which will allow these agencies speedy access to encrypted data to assist in countering terrorism or criminal activity.

Schedule 1

12. The main proposal in relation to these 'tools' is set out in Schedule 1 and provides powers which will allow the Government to request or require access to encrypted information in particular cases. The intention is to:

> "*enhance cooperation* [of the communication industry] *by introducing a new framework for industry assistance, including new powers to secure assistance from key companies in the communications supply chain both within and outside Australia".*[8]

13. The Bill proposes a graduated approach to ensuring the assistance of 'designated communications providers' in providing access to encrypted data through:

    - voluntary assistance under a 'technical assistance request' (TAR)
    - required assistance under a 'technical assistance notice' (TAN) – as long as the required assistance is "reasonable, proportionate, practicable and technically feasible"
    - required assistance under a 'technical capability notice'(TCN) issued by the Attorney-General where the designated communications provider must do 'acts or things' to ensure the provider is capable of giving assistance – as long as the Attorney-General is satisfied that it is reasonable, proportionate, practicable and technically feasible.[9]

14. Schedule 1 also includes:

    a) A long list of 'designated communications providers' who can be asked/required to provide assistance – this encompasses a very wide range of providers across the communication supply chain.[10]

    b) the contexts in relation to which the assistance can be sought - this has been amended to remove reference to 'protecting the public revenue' [11]

---

[7] Commonwealth, *Parliamentary Debates*, House of Representatives, 20 September 2018, 19-21 (Peter Dutton).

[8] Telecommunications And Other Legislation Amendment (Assistance And Access) Bill 2018): Explanatory Memorandum par 6, p.2 [Exp Mem: The Bill 2018]

[9] [Exp Mem: The Bill 2018] par 8, p3.

[10] Section 317C

[11] Section 317A

c) The assistance (acts or things) they can be asked/required to provide is extensive and for voluntary requests not limited

d) These acts or things can be concealed [12] – the only disclosure requirement is for annual reporting of raw numbers of requests/orders for assistance[13].

Schedule 2

15. Schedule 2 relates to computer access warrants and provides
    - additional power for law enforcement agencies to obtain covert computer access warrants under the *Surveillance Devices Act*, 2004, (similar to existing ASIO powers)
    - new powers for law enforcement agencies and amendments to the ASIO Act designed to address a range of operational challenges associated with the use of existing computer access powers and
    - allows foreign authorities able to request access a computer access warrant to obtain evidence to assist in a foreign investigation.

    These powers are intended to "…strengthen agencies' ability to adapt to a digital environment characterised by encryption by enhancing agencies' collection capabilities such as computer access".[14]

Schedules 3, 4, 5

16. Schedule 3 amends the search warrant framework under the Crimes Act 1914 to:

    - allow law enforcement agencies to execute a warrant in relation to premises or a person without having to be at the premises or in the presence of the person
    - allow for personal computers or devices to be confiscated for a longer period of up to 30 days, for the sake of accessing data
    - significantly increases the penalties for failure to comply with these warrants.

17. Schedule 4 provides for personal searches to be conducted on a person for a computer or data storage device, where there is a reasonable suspicion that those items are evidentiary material.

18. Schedule 5 amends the ASIO Act to:

    - establish immunity from civil liability for people who assist ASIO in good faith and

[12] 317E(j)
[13] 317ZS
[14] Ex Mem The Bill 2018, Par 6 P2

- provide for the Director General of ASIO to ask the Attorney-General to order a person to provide assistance to ASIO (e.g. providing the password to unlock a phone, using technical knowledge to interrogate a database).

SUMMARY OF JOINT CCLs POSITION – A RISK TOO GREAT

19. The Joint CCLs accept that the extent and strength of encryption protections around electronically communicated data is a real problem for the Government and police, security and intelligence agencies wanting access to encrypted data in the context of protecting Australians from the serious threats to public safety. We accept some trade-off of privacy in the interest of public safety is appropriate in such contexts.

20. We have no quarrel with the Government and law enforcement and intelligence and security agencies seeking access to encrypted data in relation to serious criminal and terrorist investigations. Our concerns relate to issues of proportionality, necessity and balance. The exposure draft Bill could not be supported because it spectacularly failed on these criteria.

21. The amendments included in the current Bill do reflect a recognition by the Government of some of the serious concerns with the exposure draft and propose some solutions and additional protections.

22. The Joint CCLs consider that the definition of "designated communications provider" remains excessively broad and the consequential application of the mechanisms available in the Bill are open to abuse, degradation of Australians' human rights and an incompatibility with the freedoms that are enjoyed by all other western-Democratic countries whose citizens are protected by federalised human rights legislation.

23. A number of the amendments are of little substance. For example, the new section 317HAA relating to technical assistance requests requires that the relevant CEO must advise the designated provider that compliance with these requests is voluntary. This provision may remove confusion for some providers, but is not likely to reduce the pressure to comply with a Government request coming from the CEO of one of the law enforcement, intelligence, national security or interception agencies.

24. Some of the amendments do improve the Bill, but overall, they fail to remedy our central concern that the proposed means for gaining access to encrypted data entail an unacceptably high and hugely disproportionate risk of undermining the security of all Australians' encrypted information.

25. We also share the concerns of cybersecurity and other experts that the current proposals pose a credible high risk to the wider security of the nation's financial and other systems which increasingly rely on the critical protection of strong encryption.

26. There are other aspects of the Bill that we oppose – notably the unwarranted secrecy as to the actions taken to give access to encrypted data even when the immediate need for secrecy has passed and the immunity for 'designated communication providers' for the actions they take in response to a request /order to provide this access;

27. The Joint CCLs do not support the current Bill.

28. Notwithstanding the findings of the current welcome, but rushed, PJCIS review, the Bill should be withdrawn and a considerably more extensive and transparent public consultation should be held [15] to address the determinative question: is it technically possible in the real world to implement the Government's proposals in this Bill without risking the very high probability of introducing 'systemic weakness' into the designated encryption systems – with potentially devastating implications for innocent individuals and more broadly for the security of the internet.

29. The CCLs note that the PJCIS has flagged that it intends to hold additional public hearings, apart from the one scheduled for 19 /10/18, in late October and November. The CCLs consider the implications of this Bill are of such significance that the consultation and discussion period should go beyond this into the first quarter of 2019 at least. The Bill should not be rushed prematurely through Parliament in December.

Recommendation 1

The Joint CCLs recommend that the *Telecommunications and Other Legislation Amendment (Assistance And Access) Bill 2018* should not be passed by the Parliament in its current form.

Recommendation 2

The Joint CCLs recommend that the Bill be subject to a far more extensive and transparent review process preferably through a longer PJCIS review extending into much of 2019, to allow considerably more public hearing days and for more opportunities for an exchange of views between Government agencies, independent experts and a wide range of civil society organisations on the controversial elements of the Bill. (see also recommendation 5)

MAIN ISSUES OF CONCERN TO CCLs

A caveat re expertise

30. The Joint CCLs are clearly not cryptographic nor cybersecurity experts. Our longstanding interest in privacy, Government surveillance and related matters has meant that we have developed a reasonably strong knowledge of the internet and encryption systems. We have close relationships with other civil society groups who are expert in these fields and we participate in

[15] The CCLs note that the PJCIS has flagged that it intends to hold additional public in late October and November - apart from the initial one scheduled for 19 /10/18.

civil society discussions with major internet players in Australia. So, we come to this submission as informed non-experts in cyber security.

31. The Joint CCLs' major concerns encompass:

    a) the high risk that the proposed actions to gain access to encrypted information on a case-by-case basis will introduce systemic weakness/vulnerability into encrypted applications;
    b) that these actions and risks will be secret and individuals and others relying on these applications for the security of their data and protection of their privacy will not be informed even when the need for operational secrecy has passed;
    c) that there is inadequate judicial oversight of the decision-making process and limited independent expert oversight of the process and the actions taken by the providers in each particular case;
    d) the extent of immunity available to providers in relation to their actions and to the intelligence agencies in relation to their requests/requirements from providers
    e) and the paucity of public reporting required.

32. In determining our view on the technical feasibility of ensuring that the development of tools to access encrypted information on an exceptional basis can be done without serious risk of causing a systemic weakness or vulnerability in the relevant encryption application, we have noted the strong views of independent experts, both in Australia and overseas, that it cannot, at this time, be done.

33. We share their apprehension that the Government and the relevant agencies do not have the relevant expertise to properly and safely assess the risk of any actions they might request/ require the providers to take and are therefore not able to provide credible assurance that no action will be taken that might lead to any 'systemic weakness or vulnerability'.

34. The Government has clearly noted these strong warnings from many expert voices and has included amendments in the current Bill intended to address these concerns. While some of these amendments do improve aspects of the Bill they do not solve the major problems identified in the first round of submissions.

Introduction of systemic weakness/vulnerability

35. The major concern about the Bill relates to the perceived risk that the effects of providing access to encrypted data cannot be limited to one-off, exceptional cases and that it will, over time, lead to dangerous systemic weaknesses/vulnerabilities in the relevant encryption application.

36. A new provision in the Bill addresses this concern directly by explicitly asserting that a mandatory TAN or a TCN must not have the effect of requiring the implementing or

development of a systemic weakness/ vulnerability nor prevent the rectification of the same in a 'form of electronic protection':

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

(a) requiring a designated communications provider to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection; or

*(b) preventing a designated communications provider from rectifying a systemic weakness, or a systemic vulnerability, in a form of electronic protection. **(317ZG)***

37. These explicit prohibitions are clearly meant to emphatically re-assure those with concerns for the safety of encryption generally, and for their own encrypted data, that there will be no danger of systemic weakness or vulnerabilities arising from the proposed secret, case-by-case encryption breaking tools or actions.

38. This has not been the effect. This provision has been widely described as ineffectual rhetoric. The CCLs have a similar view and are not in any way re-assured by it- although we do accept that it is possible that it was inserted in (misguided) good faith.

39. The prohibition on introducing systemic weakness/vulnerability does not apply to requests for voluntary assistance (TARS). As there is nothing in the current Bill prohibiting agencies from requesting actions or providers volunteering action which might lead to systemic weakness/vulnerability – this is a strange omission.

40. The CCLs consider the new prohibition in 317G, even if largely rhetorical, should also apply to the voluntary TARs.

Recommendation 3

The Joint CCLs recommend that the amended provision prohibiting the implementing or development of a systemic weakness/ vulnerability and the prevention of the rectification of the same in a 'form of electronic protection' should be extended to the voluntary TARs.

Third party assessor

41. It is indisputable that the task of assessing the likely consequences of actions taken in response technical notices or requests is often complex and difficult. One expert academic submission variously states:

"The security implications of a particular proposal are incredibly difficult to understand, even for experts…"

"The tremendous difficulty of understanding the unintended consequences and unforeseen security problems caused by a particular modification make Technical Capability Notices (and their voluntary equivalents) dangerous."[16]

42. It is therefore doubtful that the expertise exists in the relevant Government agencies, or with most affected providers, to assess whether any action taken in response to a Notice (or Request) has the potential to result in systemic weakness/vulnerability beyond the particular instance. To strengthen the assessment process and the credibility of this prohibition, the current Bill has been amended to include a possible third-party to assist in the assessment:

> *(7) If the Attorney-General gives a consultation notice to a designated communications provider, the Attorney-General and the provider may jointly appoint one or more persons to:*
>
> *(a) carry out an assessment of whether the proposed technical capability notice would contravene* section 317ZG; and
>
> *(b) prepare a report of the assessment; and*
>
> *(c) give copies of the report to:*
>
> *(i) the Attorney-General; and*
>
> *(ii) the provider;*
>
> *within the time limit specified in the consultation notice.*
>
> *(8) A person must not be appointed under subsection (7) unless the person has knowledge that would enable the person to assess whether the proposed technical capability notice would contravene section* ***(317ZG.)***

43. The CCLs accept that this is a serious and genuine attempt to build in a stronger capacity to protect against unintended, and unwanted, wider damage to the encryption application. It is an improvement in the Bill. However, commentators have been quick to point out the weaknesses with this proposal.[17]

44. It only applies to TCNS which require the development of a capability to break the encryption in a particular case. It does not apply to TANs or voluntary requests. It may be that a TCN which specifically requires a non-existent capability to be developed is likely to pose the greatest risk of introducing unintended weakness/vulnerability. Nonetheless, it is difficult to see why access to a third-party expert should not be an option in all contexts.

    A technical request for example, could lead to a voluntary agreement to develop a capability which is not currently available to provide access to encrypted data- with unknown safety implications.

45. The assessor - unlike the designated communication providers – is not covered by immunity provisions for any errors made. We do not disagree with this but note that given the technical complexity of the issue and the potential for large scale damage, it may be that there will not be

[16] Chris Culnane and Vanessa Teague Submission to PJCIS inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018. Submission 16, p4 [Culnane and Teague PJCIS Submission 16]

[17] Press references

a ready supply of properly qualified persons, as required by subsection 8, willing to take on these assessments.

46. The decision to appoint such a person or persons is made in secret by the Attorney - General and the designated provider. The Attorney-General may not have access to the expertise to determine when such extra scrutiny is needed and may be influenced by the need to move quickly in a particular situation and therefore be inclined to by-pass an additional process.

47. The designated providers would normally be expected to do all that was possible to prevent a systemic weakness in their service for reputational and commercial reasons. But a provider might consider it to be in their interest to develop a generic tool that can be used for all individual notices they receive - with the belief that they can keep that tool secure and thus not offend the prohibition in 317ZG. History suggests that would be a reckless course of action – but it is not an unlikely one.

48. The most significant problem with this amendment is the likely difficulty of there being insufficient numbers of sufficiently expert persons available to undertake the role. For this reason, we regard the amendment as an improvement in the assessment process. It does not significantly alter the overall problems with the Bill.

Recommendation 4

The Joint CCLs recommend that the third-party assessor proposed in 317ZG(7)(a) be also an available option for the voluntary TARS and the mandatory TANs.

Definition of systemic weakness and systemic vulnerability

49. The Bill does not contain a definition of systemic weakness (or systemic vulnerability) though it is the central concept in assessing the risk associated with the tools used, or developed and used, to achieve the key objective of the draft legislation -i.e. breaking the encryption on a 'case-by-case basis. It is therefore also central to a broader assessment of the proportionality of the action.

50. We note that independent cryptographic, cybersecurity and other relevant experts strongly reject the basic proposition that the development and deployment of a weakness or vulnerability for a one-off case can generally be consistent with a prohibition of creating **systemic** weakness or vulnerability.[18]

    It is clearly in the public interest to take serious note of these independent expert warnings.

51. Our own reading of the Explanatory Memorandum on this issue does not provide reassurance. There is no attempt to provide a robust technical description of how the prohibition re systemic effects can be assured - while also proposing to utilise these weaknesses and vulnerabilities in a

[18] E.g. Culnane and Teague PJCIS Submission 16; CISCO Submission to the PJCIS inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018: Submission 42 p7

particular case. The explanatory comments do not go beyond rhetorical assurances which are tentative, ambiguous and some might say 'contradictory'.

"*While systemic weaknesses cannot be built into services or devices, a technical assistance notice can require the selective deployment of a weaknesses or vulnerability in a particular service, device or item of software on a case-by-case basis. Deployment of this kind is necessary to access protected information of suspect individuals and gather intelligence or evidence in the course of an investigation. This will ensure that the powers achieve legitimate, national security and law enforcement objectives without* ***unduly jeopardising*** *the legitimate privacy and information security interests of innocent parties*."[19]

"New section 317ZG ensures that providers cannot be required to systemically weaken their systems of electronic protection under a technical assistance notice or technical capability notice. The limitation is designed to protect the fundamental security of software and devices. It ensures that the products Australians enjoy and rely on cannot be made vulnerable to interference by malicious actors."[20]

"The mere fact that a capability to selectively assist agencies with access to a target device exists will not ***necessarily*** *mean that a systemic weakness has been built. The nature and scope of any weakness and vulnerability* ***will turn on the circumstances in question and the degree to which malicious actors are able to exploit the changes required****,"*[21]

These explanatory comments are confused, equivocal and contradictory:

- The critical last sentence in the first rhetorical extract above is honest enough to include a significant qualifier: "without **unduly** jeopardising *the legitimate privacy and information security interests of innocent parties".* This is not likely to reassure any innocent parties who have been relying on the security of the encrypted service they have subscribed to.

- The previous statement is inconsistent with the unqualified rhetorical assurance in the second extract: '*The limitation is designed to protect the fundamental security of software and devices. It ensures that the products Australians enjoy and rely on cannot be made vulnerable to interference by malicious actors"*

- The third extract is again more honest in that it asserts only that a one-off capacity "*will not* ***necessarily*** *mean that a systemic weakness has been built*". Again the 'not necessarily" is hardly reassuring for innocent parties relying on the encryption service.

- More disturbingly, it clarifies that "*The nature and scope of any weakness and vulnerability* ***will turn on the circumstances in question and the degree to which malicious actors are able to exploit the changes required."***

[19] Ex Mem The Act 2018 par20 p11 Emphases added by CCLs.
[20] Ibid Par 256, p67 Emphases added by CCLs
[21] Ibid par 258 pp67-8 Emphases added by CCLs

52. If the above reference to the capacity of 'malicious actors' to exploit the one-off tools created is meant as a reassurance to the innocent users, it is not supported by recent history.

53. What is clearly necessary is for the intended meaning of 'systemic weakness' and 'systemic vulnerability' in this context to be spelled out in sufficient detail to establish a robust shared understanding of the measure of unacceptable risk flowing from any action to access encrypted data. When the criteria is more clearly established the problem of understanding the effects of any intervention will remain- but at least there will be some agreement as to what is to avoided.

54. The Government has presented no compelling rebuttal to the strong warnings by independent experts as to the high risk of systemic undermining of encryption protections if these proposals are implemented.

55. The CCLs accept the higher likelihood that the experts are correct when they argue that, at this point in time, it is impossible to ensure that breaking encryption on a one-off basis will not lead to the introduction of a systemic weakness or vulnerability over time. The implications of this are enormous for innocent individuals and more broadly for the many aspects of the nation's well-being which rely on secure and trusted encryption services.

56. The CCLs consider it would be reckless of the Government to proceed with this proposal in its current form. This is especially so with regard to the issuing of TCNs which will require providers to develop new capability for encryption breaking which brings a new risk of systemic weakness. The same risk would apply in allowing providers to volunteer to develop new capability in response to a technical request.

57. If the Bill proceeds, the CCLs urge that the TCNs be withdrawn and a new limitation be placed on Technical Assistance Requests to prohibit them from eliciting a voluntary agreement to develop a new encryption breaking capability.

58. If the Government is determined, against widespread advice, to gain access to encrypted data in one-off cases, it seems clear that more expertise will need to be developed across the main players to ensure robust assessments are able to be made as to the likely implications of proposed tools and actions.

59. Faced with such a major public interest challenge, the CCLs support the suggestion of Professors Culnane and Teague in their submission to this inquiry that a safer and more productive way forward is to foster a far more transparent and open environment for constructive collaboration (and contestation) in the assessment of encryption breaking options and their likely implications involving independent experts as well as the providers and agencies[22]. There would be a raft of security and commercial in confidence secrecy issues to negotiate around, but these should not be prohibitive of such an agenda.

60. Even a small amount of movement in such a direction would be an improvement on the consultation model that apparently underpinned the development of this Bill:

[22] Culnane and Teague PJCIS submission 16

"The Department of Home Affairs has drafted the legislation in close cooperation with agencies, including the Australian Criminal Intelligence Commission (ACIC), Australian Federal Police (AFP) and ASIO. Throughout the drafting process, the Government has consulted with a range of international and domestic technology companies about the proposed reforms."[23]

Civil society organisations and the Australian community are absent.

Recommendation 5

Should the Bill be progressed in Parliament the Joint CCLs recommend that:

a) Technical Capability Notices should be withdrawn because by requiring the development of a new encryption breaking capability (albeit for a particular case) they will introduce a new risk of systemic weakness and vulnerability to the encryption application.

b) A new limitation should be imposed on TARs to prohibit them from eliciting a voluntary agreement to develop a new encryption breaking capability for the reasons above.

Recommendation 6

The Joint CCLs recommend that the Government initiate more transparent and inclusive discussions bringing together industry, government agencies, independent expert organisations and individuals and civil society to further consider the viability of and alternatives to the current proposals set out in schedule 1. These open consultations should be part of and extend beyond the extended formal review process proposed in Recommendation 2

Recommendation 7

The Joint CCLs recommend that an important issue for consideration in the discussions above and the formal PJCIS review process is the need for a precise and useful definition of the terms 'systemic weakness' and 'systemic vulnerability' in the context of the actions proposed by this Bill.

Designated Communication Providers – section 317C

61. Section 317C defines the category of Designated Communication Providers and the range of their eligible activities which can be subject to a technical request or notice. This list is intended to *"include the full range of participants in the global communications supply chain, from carriers to over-the-top messaging providers*".[24] The CCLs understand why providers at all points of the 'communications supply chain' must be covered but, when all 15 groupings of provider categories and sub-categories of functions are combined with the accompanying list of activities of the provider, the scope of those captured is truly startling.

[23] Department of Home Affairs: Assistance and Access Bill 2018: Explanatory Document August 2018 p7

[24] Ex Mem The Bill 2018, par25 p35

62. A partial list of the designated providers includes:

> Carriers or carriage service providers, carriage service intermedia, persons that provide an electronic service, people involved in designing trust infrastructure used in encrypted communications or software utilised in secure messaging applications, people that manufacture, supply, install or operate a facility (infrastructure of a telecommunications network or line – including tower, antenna, tunnel, pit, pole etc), people who make or supply components for infrastructure, people that connect facilities to telecommunications networks in Australia, suppliers and manufacturers of devices such as modems, mobile devices, people who make SIMs, memory units for mobile devices, people who install/maintain customer equipment, people who connect equipment to telecommunications network in Australia (other than end user of the equipment), constitutional corps that manufacture, supply, install or maintain data processing devices.

63. When combined with the activities it appears designated providers could include anyone in any way related to providing an internet service or facilitating same – from the most obvious providers of major applications to a website host. The scope and range of captured individuals, businesses and corporations who could be subject to a technical notice or request seems extraordinarily wide for provisions which should only be activated in the context of serious criminal activity or threat to public safety.

64. The DHA has defended the very wide definition and the inclusion of small players as it:

> *"reflects the flexibility and ease of entrance into the communications market and accounts for circumstances where an individual may establish small-scale services that criminals migrate to because of a perceived lack of cooperation".*[25]

65. The CCLs are not in a position to contest this justification but consider that the appropriateness of the breadth of the definition be thoroughly tested with relevant technical experts in the PJCIS review process.

66. Even if this very wide definition is judged to be appropriate, there are likely flow-on issues relating to the compliance costs and risks in small or start-up businesses being forced or invited to respond to a technical notice or request in this context. It has been suggested that this might have the undesirable effect of stifling innovative start-ups in Australia.[26]

67. The Department of Home Affairs has recognised there may be issues with small businesses and suggests this has been addressed by the amendment requiring an explicit explanation as to the obligations of a notice or request:

---

[25] DHA PJCIS submission No 18: p15

[26] Joint Submission by: Australian Privacy Foundation, Digital Rights Watch, Electronic Frontiers Australia, Future Wise, The Queensland Council for Civil Liberties, The New South Wales Council for Civil Liberties, Access Now, Blueprint for Free Speech. 10th September 2018. [Joint Submission PJCIS APF DRW PJCIS p8 https://www.homeaffairs.gov.au/consultations/Documents/digital-rights-watch.pdf

"..the issuer of a notice or request must now clearly explain the obligations of the relevant DCP. This will support smaller DCPs subject to a notice by either making explicit that compliance is voluntary or clarifying the nature and extent of a notice's requirements."[27]

While clarity is obviously desirable, the CCLs do not think this minor amendment will have any substantive impact on the implications of the requests or notices.

68. The CCLs consider the impact on smaller and start-up businesses is a possible flow-on effect of the extensive range of designated providers which should also be considered by the PJCIS.

Recommendation 8

The Joint CCLs recommend that the PJCIS give careful consideration to:

a) the appropriateness of the very expansive definition of designated communication providers and eligible activities and

b) the likely inhibiting effect on IT innovation flowing from the inclusion of small and start-up businesses as designated communication providers.

Acts or things - Section 317E

69. The extensive list of 'acts or things' that can be required of providers generates much of the concern from experts as to the likelihood of the proposals generating unintended systemic weakness and vulnerability in the accessed application. It also raises questions about the scope goes beyond the objectives of the Bill. Some of the wide range of 'acts or things' listed at section 317E include:
    - Removing one or more forms of electronic protection applied by or on behalf of the provider
    - Providing technical information
    - Installing, maintaining, testing or using software, equipment
    - Assisting access to devices/services/equipment/software
    - Assisting with testing, modifying, developing or maintaining technology or a capability
    - Modifying or facilitating the modification of any characteristics of a service by a designated communications provider
    - Substituting a service by a designated communications provider for another service
    - Concealing these acts.

70. The list is non-exhaustive for voluntary requests. It is also non-exhaustive for TANS and TCPs **if** the provider is already capable of providing the assistance : "*Both TANs and TCNs can request assistance that a provider is already capable of providing*." Otherwise the DHA says the list is

[27] DHA PJCIS submission 18 p16

exhaustive for TCPs[28]- although it can be extended by the Minister by a legislative instrument tabled in Parliament under subsection 317T(5).

71. The CCLs do not see any justification for the list being non-exhaustive for any technical request or notice. All three levels should have exhaustive lists which can only be added to by legislative amendment by Parliament.

72. Given the complexity and the importance of the issue, the CCLs oppose the power for the Minister to add to the list of acts or things by legislative instrument. Any amendments to the list in relation to DCNs (or TARs and TANs) should only be by Parliament amending the Act.

73. Many of the listed 'acts and things' are capable of creating systemic weakness in an encrypted application or system. For example,

    a) '*removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider*' 317E(1)(a) or

    b) 'modifying or facilitating the modification of any characteristics of a service by a designated communications provider' 317E(1)(h)

74. The DHA emphasises that "*a TCN is unable to require that a DCP build a capability to remove a form of electronic protection, like password rate limits or end-to-end encryption*." This confident statement is presumably relying on the questionable effectiveness of the prohibition against the introduction of systemic weakness at section 317ZG. It would however seem able to request access to such a capability if the provider already has it.

75. The DHA's submission argues strongly that the Bill - especially as amended with the proposed prohibitions in 317ZG- does not adopt measures that would permit the introduction of systemic weaknesses that 'malicious actors could exploit. Instead:

    .."it establishes a technologically neutral framework for industry and government to work together towards access solutions with entrenched security protections. The new arrangements put in place by the Bill will allow, where possible, Australian authorities exceptional access to encrypted communications in circumstances negotiated by industry and Government. Importantly, any arrangement that would introduce weaknesses and make innocent, third-party communications vulnerable would be in contravention of the Bill's legal safeguards.[29]

76. The DHA lists four illustrative scenarios which would be regarded as likely to introduce systemic weakness:

    For example, legislation could set out requirements for providers to:

[28] DHA submission No 18, p16. Although this seems inconsistent with Subsection 317T(7) which says that the acts or things that may be specified in a technical capability notice *"include (but are not limited to) listed acts or things".*

[29] Ibid P9

a) *Design their systems in a way that creates a unique law enforcement 'key' to selectively access encrypted data ('key escrow').*

b) *Build devices in a particular way that would store a key on the hardware itself.*

c) *Retain the capability to unlock devices when requested.*

d) *Limit the length of their encryption keys, weakening their complexity and increasing the chance that agencies could 'brute force' access by trying all possible key combinations*.[30]

77. In relation to these scenarios the DHA asserts: *"The Assistance and Access Bill **does not** adopt any of these approaches*."[31]

78. However, the Bill does not specifically exclude these approaches. The prohibition in 317ZG may exclude a requirement for the development of the above acts - depending on the interpretation of 'systemic weakness'. The CCLs have not however identified any provision in the Bill that prohibits using such approaches if the provider already has the relevant capability.

79. The CCLs do not have the technical expertise to discern which of the designated 'acts or things' are potentially systemically dangerous. But it is clear that there are credible different interpretations of this and inconsistencies in the explanations put forward by the DHA and the provisions in the Bill.

80. The DHA's overall justification for the expansive list is operational necessity: '*The items are broadly cast in order to be responsive to operational needs and to reflect the rapidly changing capabilities of the communications industry'*[32]. A similar argument applies to the very wide definition of providers.

81. The assertions about operational need may be accurate, but if so, given the potential harm that could result from mistaken assessments as to likely consequences of one-off actions taken to break encrypted systems, the better argument may be that there are some operational 'needs' which cannot be met safely and where the resulting trade of in loss of security and privacy for innocent Australians is unacceptable.

82. The current list of 'acts and things' requires a considered review – incorporating the perspectives of privacy experts as well as cryptographic and cyber security experts – to ensure that interventions do not disproportionately threaten the security of the relevant system or application or the security of innocent Australian's encrypted information and thereby their privacy.

[30] Ibid
[31] ibid

[32] Ibid

Recommendation 9

The Joint CCLs recommend that:

a) the extensive list of 'acts and things' in section 317E is carefully reviewed with a view to developing a more limited and focussed list of acts that are not likely to undermine the security of the system or the security and privacy of innocent individuals.

b) the list of 'acts and things' be made exhaustive for TARs, TANs and TCNs and

c) proposed subsection 317T(5) giving the Minister power to make additions to the list for DCPs by a legislative instrument be removed from the Bill . Any addition to the list of 'acts and things' for TCPs (or TARs and TANs) should be by amendment of *The Telecommunications Act 1997 (Cth) Act* by Parliament.

Objectives

83. The Bill specifies the objectives for which technical requests and notices can be made.

For TARs they are:

(a) *enforcing the criminal law and laws imposing pecuniary penalties; or*
(b) *assisting the enforcement of the criminal laws in force in a foreign country; or*
(c) *the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.*[33]

For TANs and TCNs they are:

(i) *enforcing the criminal law and laws imposing pecuniary penalties; or*
(ii) *assisting the enforcement of the criminal laws in force in a foreign country; or*
(iii) *safeguarding national security.*[34]

84. In the current Bill these have been amended by the removal of 'protecting the public revenue. This is an appropriate deletion but the objectives remain far too expansive for powers which are so invasive of data security and individual privacy. These powers can only be justified in contexts where there is a serious threat to public safety or serious crime that threatens the public interest.

85. The reference to 'laws imposing pecuniary offences' should be removed - notwithstanding the assurance in the Explanatory Memorandum that it will only be applied when the offence is serious.[35]

[33] Section 317G(5)

[34] Sections 317L(2)(c) and 317T(3)

[35] Ex mem The Bill 2018, Par 97 p44

86. The reference to 'the interests of Australia's foreign relations' and 'national economic well-being' are very broad categories encompassing and obviously inclusive of matters of major and minor significance. The reference to 'national economic well-being should be removed.

87. The all-encompassing reference to *'the interests of Australia's foreign relations'* should be removed or tightened to reference serious threats or offences in relation to *of* Australia's foreign relations.

88. The objective '*enforcing the criminal law'* should be tightened by a limitation to offences of a serious nature which threaten public safety or the public interest.

89. The objective '*assisting the enforcement of the criminal laws in force in a foreign country'* is disturbing in its breadth and potential application. This could apply to laws in other countries which are oppressive and override human rights or apply the death penalty. It appears to open the way for expanded secret surveillance of Australians on behalf of foreign countries including and beyond the Five Eyes allies. It should be removed from the objectives or reformulated so that it prohibits collaboration in relation to oppressive laws or laws which undermine human rights.

Recommendation 10

The Joint CCLs recommend that the objectives specified for TARs, TANs and TCPs be amended by:

a) removing the reference to '*laws imposing pecuniary offences' and 'national economic well-being' and*

b) removing the reference to the '*interests of Australia's foreign relations'* or limiting it to apply to serious threats or offences in relation to Australia's foreign relations and

c) limiting the reference to '*enforcing the criminal law'* to ensure this applies only to offences of a serious nature which threaten public safety or the public interest and

d) removing the broad reference to '*assisting the enforcement of the criminal laws in force in a foreign country. '*

Decision making process and criteria

90. Before issuing or varying a TAN or a TCN the decision maker must be satisfied that:

(a) the requirements imposed by the notice are reasonable and proportionate; and

(b) compliance with the notice is:

(i) practicable; and

(ii) technically feasible.[36]

[36] 317P and 317V

This does not apply before issuing a TAR.

91. This requirement has been strengthened in the current Bill by an additional provision that in considering the 'reasonable and proportionate' criteria the decision maker '*must have regard to the following matters':*

    (a) the interests of national security;
    (b) the interests of law enforcement;
    (c) the legitimate interests of the designated communications provider to whom the notice relates;
    (d) the objectives of the notice;
    (e) the availability of other means to achieve the objectives of the notice;
    (f) the legitimate expectations of the Australian community relating to privacy and cybersecurity;
    (g) such other matters (if any) as the Director-General of Security or the chief officer, as the case requires, considers relevant.[37]

92. The CCLs acknowledge that this is a positive response by the Government to criticism in relation to the decision making process and does strengthen the criteria. It does not, however, apply to TARs – consistent with the non-application of the 'reasonable and proportionate' criteria to TARs. The CCLs consider that both sets of criteria should apply to TARs.

93. The most significant of these newly specified interests that must be taken regard of are those relating to the 'availability of other means to achieve the objectives' and 'the legitimate expectations of the Australian community relating to privacy and cybersecurity'

94. Genuine consideration of available less risky or dangerous means should be an imperative in any context where the law enforcement option under consideration entails high level risks to critical information systems and on the right of innocent persons to the security of their data and privacy. What is missing in this formulation is a requirement to act on an effective option which has less negative effect.

95. Nor is there any incentive for the decision maker to give genuine rather than token regard to options. The secrecy surrounding the issuing of technical requests/notices , the immunities available to the providers and agencies and the tokenistic reporting requirements effectively remove possible incentives.

96. The decision maker should have to be **satisfied** that there was no other less dangerous option to issuing a notice and that the decision was **necessary** in the particular case.

97. The requirement 'to have regard' to the '*the legitimate expectations of the Australian community relating to privacy and cybersecurity*' brings a welcome recognition of the need for some consideration of the possible impact on the wider Australian public in the decision making process. However, it will have no impact.

---

[37] 317RA and 317ZAA

98. Though it is likely that a majority of Australians would support a risky law enforcement act in the context of a serious threat to the public safety - even at some risk to their data security and privacy - there is not likely to be any consensus as to the what their 'legitimate expectations' might be in a less serious and urgent context.

99. If this Bill proceeds it is essential that consideration is given to the protection of the broad public interest and the legitimate interests of innocent consumers whose data security may be undermined resulting in significant adverse effects to their financial or other assets or to their privacy.

Recommendation 11

The Joint CCLs recommend that:

a) the decision making criteria in relation to issuing a TAN or a TCP are also applied to TARs.
b) The requirements in relation to TARs, TANS and TCPs be amended to require the decision-maker to be satisfied of the 'necessity' of giving or varying a request or notice.
c) An additional requirement that regard be given to 'the legitimate interests of innocent persons who are clients of the targeted application/service under a technical request or notice' and whose information and privacy may be at risk.

Recommendation 12

The Joint CCLs recommend that the Bill be amended to provide some appropriate process and provision to allow compensation for innocent consumers whose data security is undermined as a result of actions by providers and/or relevant agencies resulting in significant adverse effects to their financial or other assets or to their privacy.

Oversight secrecy and reporting

100. The CCLs consider that the combined effect of the **lack of judicial oversight** of the proposed activities, the broad secrecy provisions, the heavy penalties for disclosure of information, the minimalist and uninformative reporting requirements to the public or to existing oversight bodies and the broad immunity provisions for providers and agencies is extremely dangerous – and inappropriate in a democracy.

101. The Attorney-General for TCNs or heads of the relevant agencies for TARs and TANS have the power to request or require DCPs to provide designated assistance. The lack of appropriate judicial oversight in this process is disturbing and particularly so in relation to the TCNs. This issue was raised by many of the submissions but continues to be resisted by the DHA as unnecessary:

….ministerial authorisations like the Attorney-General's ability to issue a TCN are an established aspect of the Australian regulatory regime that operate effectively, and appropriately, to discharge and monitor national security and law enforcement powers.[38]

102. The CCLs consider that there should be judicial oversight in relation to all technical assistance requests or notices. Court approved warrants should be required in all instances.

Recommendation 12

The Joint CCLs recommend that there be judicial oversight of requests or notices for technical assistance and that court warrants be required for the issue of TARs, TANs and TCNs.

Secrecy provisions

103. The main secrecy provisions are set out in section 317ZF: *Unauthorised disclosure of information.* The scope of the prohibition is very broad. It essentially criminalises the disclosure of any information about the notices or resulting actions by providers- with the exception of aggregate reporting as to numbers of notices received. There are no exceptions or defences in relation to public interest or the interests of their clients. There is no time limit on the secrecy requirement. There is no requirement for harm to be done by the disclosure. The penalty for unauthorised disclosure is 5 years gaol. [39]

104. This is an excessive secrecy provision in relation to a major extension of surveillance powers by the state.

105. The Explanatory Memorandum asserts:

.. 'there is a high risk that the release of sensitive information contrary to this subsection will cause significant harm to essential public interests, including national security and protection of public safety'.[40]

106. This ignores the counter - balancing high level risks of harm relating to undermining trust in providers and to the security of the internet and encryptions systems that flow from the lack of disclosure - nor the potential for harm to innocent individuals. These are large public interest risks.

107. A degree of secrecy that is necessary to protect intelligence or law enforcement operations is legitimate. But these provisions should be considerably scaled back. It is not acceptable that innocent Australians should not know that encrypted services to which they have subscribed, and which they expect will provide security for their most

[38] DHA PJCIS submission 18 pp31-2
[39] The CCLs have argued against similar excessive secrecy proposals most recently in relation to the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth
[40] Ex Mem the Bill 2018, Par 238, p65

important data, have been interfered with in ways which may have compromised their security.

Recommendation 13

The Joint CCLs recommend

a) The unauthorised disclosure of information offence provisions be amended to include intentional harm to the public interest

b) The unauthorised disclosure of information offence provisions be amended to include a public interest exception or defence

c) The unauthorised disclosure of information offence provisions be amended to include disclosure in accordance with the PID Act as an exception

d) The PJCIS give particular consideration to identifying technical information which can be disclosed by providers to their subscribers and the public without compromising particular intelligence or law enforcement operations.

Reporting provisions

108. Reporting provisions are set out in section 317ZS: Annual reports. The Minister is required only to report on the number of technical assistance requests or notices that were given in any year. Such minimalist reporting provides a poor basis for accountability and leaves the Australians who rely on encrypted services without knowledge as to whether there particular service may have been compromised. This lack of critical information will likely undermine trust and confidence int here systems- with unpredictable consequences.

109. It is clearly important that the Government rethink this and expand the range of information that can be made public to allow a robust and useful reporting regime.

Recommendation 14

The Joint CCLs recommend the reporting provisions in section 317ZS be reviewed with the aim of significantly expanding the information which can be included.

Other matters

110. The Joint CCL also have major concerns relating to the computer access warrants and the search warrant framework amendments proposed in the Bill but given time constraints we have focussed on the central aspect of the industry assistance scheme. We note that these other

areas are covered in many submissions. We endorse recommendations 21-26 and 28-35 of the joint submission from the Australian Privacy Foundation, Digital Rights Watch and others[41]

Conclusion

The Joint CCLs hope this submission is of assistance to the PJCIS. Representatives are available to provide further comment and respond to any queries arising from this submission at the PJCIS public hearings.

This submission was prepared on behalf of the Joint CCLs by Dr Lesley Lynch VP NSWCCL, Angus Murray VP QCCL and Michael Bruill NSWCCL Legal Policy Officer.

Therese Cochrane
Secretary
NSW Council for Civil Liberties
Mob 0402 013 303

Contact in relation to this submission
Dr Lesley Lynch
Mob 0416497508
Email Lesley.lynch@ndeccl.org.au

41