Office of the Victorian
Information Commissioner

t 1300 00 6842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D18/134040

14 September 2018

National Security Policy Branch
Department of Home Affairs
PO BOX 25
Belconnen ACT 2616

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

Thank you for the opportunity to provide comment on the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill* 2018 (**the Bill**). My office, the Office of the Victorian Information Commissioner (**OVIC**) has a unique regulatory focus, with combined oversight over privacy, data security and freedom of information in Victoria, administering both the *Privacy and Data Protection Act 2014* (**PDP Act**) and the *Freedom of Information Act 1982* (Vic). As part of my responsibilities under the PDP Act my office is responsible for setting standards for law enforcement use of systems and data, and auditing such use. As such, the Bill is of particular interest to my office.

As a general observation, while I understand the issues faced by intelligence and law enforcement bodies in the digital age, I am concerned at the risks these reforms pose for the security and privacy of communications as a whole. Members of the community using communications services subject to these reforms have a reasonable expectation that their communications will remain secure and private, and purchase access to certain services for precisely these reasons. There is great utility in the maintenance of secure communications services that employ protections such as end-to-end encryption, which are noted in the Explanatory Document on the Bill.[1] Encryption can also be essential in the protection of individuals' fundamental rights of privacy, freedom of association and freedom of expression, amongst others.

I note that the Explanatory Document refers to certain intentions, or protections, to consider the wider public interests[2] in decisions to issue a technical assistance notice or technical capability notice. While I view these protections as both appropriate and welcome, I suggest that these protections should be reflected in the Bill itself.

My submission will primarily focus on the privacy and data security concerns identified under Schedules 1 and 2 of the Bill.

Inclusion of website in definition of 'service'

1. I question whether it is reasonable and proportionate to include a website in the definition of 'service' under clause 317D(2) of the Bill. The express inclusion of a website under the definition of 'service'

[1] On page 7.
[2] On pages 34 and 38.

will have the effect in practice of requiring designated communications providers to facilitate or provide assistance in accessing an electronic service (including a website). I note the potential for such reforms to have the effect of stifling actions in the public interest, such as whistleblowing, where advocates may have a reasonable expectation that their publications or concerns should remain private and secure. More broadly, my office is concerned about the potential impact the Bill may have on public discourse, as well as the possibility for these reforms to expose innocent persons rather than specific targets.

2. Further, I note that the Bill as currently drafted, could have the effect of undermining protections afforded for individuals in certain circumstances, such as the journalist privilege under Division 1C of the *Evidence Act 1995* (Cth).[3]

Concerns relating to Schedule 2 of the Bill: Computer access warrants

3. The draft Bill covers any and all devices or services likely to connect to the internet or another network. Clause 317C provides that it includes a person if "the person develops, supplies or updates software used, for use, or likely to be used, in connection with: (a) a listed carriage service; or (b) an electronic service that has one or more end users in Australia." Such services could also include so-called 'internet of things' devices including 'smart speakers' and voice-activated systems in vehicles. The interaction of these activities with the *Surveillance Devices Act 2004* (Cth) (**SDA**), and the changes to subsection 6(1) of the SDA (inserted by Schedule 2 of the Bill) that effectively incorporate such services into its scope, represent a substantial increase in scope of the SDA. While I note that computer access warrants are subject to judicial oversight (issued by judges and Administrative Appeals Tribunal members),[4] I am concerned about the increased potential for surveillance by law enforcement these reforms introduce.

4. I note that when the SDA was introduced, it was subject to substantial public debate. The Bill seeks to introduce changes of a similar scale, with the introduction of a new power to access computer systems via a computer access warrant. This unique power can potentially have wide reaching impacts on individual human rights and the security of devices and networks. As such, I am concerned about the introduction of these powers without significant public debate and I would welcome further consideration to the controls in place for law enforcement exercising these powers.

Prohibition on building systemic weakness

5. In principle, I support the inclusion of an express prohibition on the building of systemic weaknesses or vulnerabilities under clause 317ZG of the Bill. However, I am unsure how this prohibition will operate in practice. While I note that it is not the intention of the Bill to undermine "systems that protect the fundamental security of communications,"[5] I am concerned about the potential risk for the capability introduced under the Bill to selectively create weaknesses or vulnerabilities, or to do so unintentionally because the full consequences of a 'one-off' request are not well understood by either the requester or the provider to whom the request is made, or both. There is undoubtedly potential for such weaknesses to result in the undermining of the security of communications as a whole, considering the potential for any created weaknesses to be exploited.

6. In practice, if a designated communications provider builds a weakness (in response to a technical capability notice) for a single use case, for example to enable interception of material from an endpoint such as a smartphone, this would likely be achieved through writing custom software or firmware. This practice, if it were done for a single smartphone, might be determined – in isolation – as not creating a systemic weakness. However, in the development of this non-systemic weakness, code will be developed that might be used to facilitate future requests for other cases involving a

[3] Under ss. 126J and 126K.
[4] Explanatory Document, page 14.
[5] Explanatory Document, page 10.

similar smartphone with minimum disruption and expense. While the initial development may be interpreted as not creating a systemic weakness (as it has a target of one) the ability to configure the capability to facilitate future requests would likely represent systemic vulnerability; such a capability would present a considerable threat to all users of similar smartphones. Until the capability is destroyed after its use under the notice (presumably after receiving a notice of revocation under clause 317Z), its very existence represents a threat to similar endpoints all over the world. To truly avoid the creation of a systemic weakness, the degree to which material developed under a notice is destroyed or re-used would need to be closely monitored by an expert, and appreciated not only in the context of the single request or notice, but in terms of the interactions of multiple requests or notices. Furthermore, designated providers would need to maintain impeccable development hygiene to make a selective request truly 'one-off.'

7. I note that there appears to be no restriction on a technical assistance request (issued under Division 2) having the effect of requesting the creation of a weakness, or removal of one or more forms of electronic protections.[6] Although forms of assistance under a technical assistance request are voluntary, I note the potential for a designated communications provider to agree to provide assistance under a technical assistance request that may unintentionally create a systemic weakness.

Definition of 'systemic weaknesses'

8. The way 'systemic' is defined in the Explanatory Document[7] seems to suggest that there is an underlying assumption that only agencies identified under the Bill will be able to utilise the weaknesses created under technical assistance or capability notices, for express law enforcement purposes under the Bill. However, there is a well documented[8] risk that malicious actors may take advantage of any weaknesses created remains. I suggest that within agencies issuing technical assistance notices and technical capability notices the supporting governance and security arrangements must account for the significant security risks the creation of any weakness poses for communications as a whole.

9. There is also a lack of clarity around how 'systemic' weaknesses will be defined and determined, for the purposes of clause 317ZG in the Bill. In the case of technical capability notices, it is unclear whether this assessment rests with the Attorney General or the designated communications provider, in terms of deciding whether the capabilities built under a technical capability notice would amount to a systemic weakness. For example, I question whether this is an assessment the Attorney General could make in accordance with the decision-making criteria outlined under clause 317V and the consultation process under clause 317W of the Bill.

10. Further consideration needs to be given to the ability of the relevant parties to correctly interpret the meaning of 'systemic weakness.'

'Necessary and proportionate'

11. In relation to the decision-making criteria under Division 3 (technical assistance notices) and Division 4 (technical capability notices) of the Bill, I am concerned that the effectiveness of the safeguards (in the requirement for decision makers to consider whether the issuing of a notice is reasonable and proportionate) will depend on the decision maker's technical understanding of the security risks and wider impact of the notices.

---

[6] Under clause 317E(1)(a), for example.
[7] On page 47.
[8] As pointed out by Dr Vanessa Teague and Dr Chris Culnane of Melbourne University, in their submission, 'Response to consultation on Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, "(a)ny decision about law enforcement access need to take into account the likelihood that criminals will use the same vector." See, page 3.

12. I also note that there is no express requirement for decision makers to consider the necessity of each of the notices. An assessment of whether the notice would be necessary, perhaps by reference to the listed powers and functions under each of the Divisions, would serve as an additional safeguard in decision making.

13. The Explanatory Document notes that the decision-maker "must also consider wider public interests, such as any impact on privacy, cyber security and innocent third parties" when deciding whether or not to issue a notice under either Division 3 or Division 4 of the Bill.[9] Nevertheless, public interest, privacy, cyber security and innocent third parties are not explicitly called out in the decision making criteria in clauses 317P and 317V. These factors are not inherent nor implicit in those clauses that only require decision-makers to consider if notice requirements are "reasonable and proportionate" and that compliance with the notice is "practicable and technically feasible." Given that the scheme has no merits review of the decision to issue Division 3 and Division 4 notices, I believe it is important to explicitly set out these relevant considerations so that decision-makers turn their minds to them. If it is the intention for decision makers to be required to consider the privacy and cyber security impacts of each notice, this should be reflected in the Bill. In the absence of such a requirement, in effect there will be no express obligation for decision makers to consider the wider privacy and security impacts, including the likelihood that any weaknesses built under a technical capability notice will be exploited by malicious actors.

14. I also note that there appears to be no similar express decision-making criteria for decision makers when issuing a voluntary technical assistance request under Division 2 of the Bill. I recommend that requests for voluntary technical assistance should be subject to similar assessments as technical assistance notices and technical capability notices, to ensure privacy and security considerations are adequately considered.

15. Where a request involves a provider of products or services that are used to facilitate trust on a network, such as a Certificate Authority or other PKI provider, the definition of "proportionate" becomes particularly important. Should a weakness in the authority of those products or services become apparent to other parties on the network, the provider will suffer irreparable reputational damage. While the risk of disclosure or discovery may be small, the consequences would be enormous. On the basis of "necessary and proportionate," all such providers would need to be excluded from any and all notices or requests, as there is no proportionate way in which these elements of internet trust can be safely managed. Clause 317C is currently so broad as to include such providers, and the Bill should make it clear that PKI and Certificate Authorities ought not be included in a technical assistance request or notice.

16. The collective understanding of what 'reasonable' security risks are in this context will be continuously evolving. Security itself is a continuously evolving concept – rather than something that can be determined once and then implemented, it is always changing as the software, hardware and techniques in use are updated. Practices and systems that were considered safe only last year may now be considered unwise. An express requirement to consider the wider privacy and security risks associated with the issuing of a notice under Division 3 or 4, would allow decision makers to access current and specific advice on such risks, to avoid the very real possibility of inadvertently creating a systemic weakness for exploitation. I am of the view that there is a role for independent review and assessment of practices undertaken in requests and fulfilment of requests and notices, in order for industry and the public to have any confidence that risks are managed.

[9] Explanatory Document, pages 34 and 38.

Social engineering risk

17. I am concerned about the ability for technical assistance and capability notices to be issued and varied orally.[10] This ability seems to lend itself to social engineering attacks, for example in providing opportunity for people to impersonate law enforcement officers over the phone to access systems. Notwithstanding the limitations on the issuing and variation of notices orally under the Bill (in the requirement that there be an imminent risk of serious harm or substantial damage to property present), and the illegality of impersonating law enforcement, my view is that those limitations do not offer sufficient protection against malicious actors. As such, I recommend that all notices be issued in writing.

Duration of technical capability notices

18. I question why the duration of a technical capability notice is significantly longer than a technical assistance notice, under clause 317TA. If a technical capability notice has a duration of 180 days, there should be a strict timeframe for revocation under clause 317Z. It is not desirable to have open-ended vulnerabilities and in my view the Attorney General should be obligated to monitor the duration, expiry and revocation details of all technical capability notices.

Compliance and enforcement

19. There seems to be a fundamental lack of natural justice and impartiality in the appointment of arbitrators under clause 317ZK, setting out the terms and conditions for technical assistance notices and technical capability requests. I am concerned with the operation of proposed clause 317ZK(6)(b), as it requires the Attorney General to appoint an arbitrator where the parties fail to agree on the appointment of an arbitrator and none of the parties are a carrier or carriage service provider. This lack of impartiality in appointing arbitrators does not seem to lend itself to fair and unbiased arbitration processes.

20. The interaction of clause 317ZK with clause 317ZF is of concern. It will especially disadvantage smaller providers. Secrecy provisions surrounding notices mean that providers will be unable to explain to shareholders why their profit margins have decreased as a result of performing not-for-profit work, or why timelines for delivery of other promised work have been extended. As such, the capability for providers to resource a request or notice without impact to their business should be a component in assessing whether a request or notice is reasonable and proportionate, and this should be reflected in the Bill.

Unauthorised disclosure of information

21. I am concerned about the potential risk in the prohibitions on the disclosure of information about requests or notices issued under Schedule 1, under clause 317ZF. In the event a designated communications provider develops a weakness that becomes exposed to foreign or malicious actors, it appears that the operation of clause 317ZF, as currently drafted, would mean that a provider – or another party that discovers the exposure – would be unable to inform the information security community of a vulnerability. On the face of it, this is clearly counter to the interests of effective cyber security risk management. This secrecy provision itself introduces a form of systemic weakness.

[10] Under clauses 317H(1), 317JA(5), 317M(1) and 317Q(3). As well as technical assistance requests, under clauses 317H(1) and 317JA(5).

Transparency and governance

22. There is a lack of clarity both under the Bill and in the Explanatory Document[11] what "in the interests of law enforcement," under clause 317T(6)(a) of the Bill should be interpreted to mean. I question whether the scope of clause 317T(6)(a) should be limited by reference to a certain threshold, such as is the case under s 6 of the SDA, defining a relevant offence as one that is punishable by a maximum term of three years imprisonment or more.[12]

23. I am concerned that the annual reporting requirements under clause 317ZS of the Bill may be inadequate to ensure proper transparency and accountability to the public. The annual reporting requirements in the Bill only require the Minister to report on the number of technical assistance notices and technical capability notices issued each year. I suggest that annual reporting requirements under the Bill also include the number of technical assistance requests issued in the year and an explanation of the purposes for which the notices were required (by reference to the express functions and purposes under Divisions 2, 3 and 4 of the Bill).

24. I question whether there is sufficient parliamentary scrutiny over the Minister's power to broaden the scope of 'listed help' under clause 317T(5) of the Bill. I note that the Explanatory Document explains that the Minister's power should be "limited in the legislation and subject to ongoing Parliamentary scrutiny,"[13] which I welcome. However, I note that the effectiveness of ongoing Parliamentary scrutiny will depend on the extent to which the impacts of the proposed expansion of 'listed help' are properly understood. Given the limitations on disclosure of use of the requests or notices, and the extremely limited reporting required under 317ZS, it is unclear how Parliament could develop an informed view.

25. Upon reading clause 317ZH(1)[14] it appears that it is the intention of the Bill to make it clear that any technical assistance or capability notice will have no effect to the extent that it would require a designated communications provider to do an act or thing for which a warrant or authorisation would be required, under the Acts listed in clauses 317ZH(1)(a) – (e). However, there appears to be a lack of judicial oversight over the issuing of notices themselves under Divisions 3 and 4 of the Bill, leaving the assessment as to the reasonableness and proportionality of notices to administrative decision makers. On this point, I recommend decision makers be required to consider whether there is already a warrant in place, in assessing whether a notice under Division 3 or Division 4 is reasonable or proportionate.

26. As a general observation, I am concerned about the potential for these reforms to considerably broaden the surveillance powers of law enforcement, without adequate oversight from a body with the expertise and resources to monitor the aggregate impact of the reforms.

27. I note that the courts retain their inherent powers of judicial review under the section 75(v) of the Constitution of a decision made by a senior decision maker or the Attorney General to issue a notice.[15] However, the Bill excludes judicial review under the *Administrative Decisions (Judicial Review) Act 1977* (**ADJR Act**) by including decisions made under the new Part 15 of the *Telecommunications Act 1997* (inserted by Schedule 1 of the Bill) as a class of decision that is not subject to the ADJR Act (under paragraph (daaaa) of Schedule 1 of the ADJR Act). While both of these avenues of judicial review have similar grounds of review, the ADJR Act is more accessible for litigants, particularly smaller providers. Consequently, I suggests that ADJR review not be excluded under the Bill.

---

[11] On page 37.
[12] Explanatory Document, page 14.
[13] On page 37.
[14] And page 48 of the Explanatory Document.
[15] Explanatory Document, page 11.

28. The Explanatory Document also notes that decisions to issue technical assistance and capability notices will not be subject to merits review.[16] While I appreciate that some decisions of a law enforcement nature (as identified by the Administrative Review Council)[17] have been identified as being unsuitable for merits review, I see a significant distinction between the powers under this Bill and decisions made for other law enforcement purposes. As such, I urge the Department of Home Affairs to reconsider the need for a mechanism of merits review, that accounts for the unique nature and broad scope of the powers of senior decision makers under the Bill.

29. In the absence of merits review, I urge that the decision-making criteria in clauses 317P and 317V provide detailed guidance to decision-makers and specify the relevant considerations and irrelevant considerations that are set out in the Explanatory Document. These considerations include the public interest, privacy impacts, cyber security impacts, innocent third-party impacts, interests of the agency, interests of the provider, other means to meet objectives, benefits to the investigation, business impact on the provider and whether the provider is the most appropriate person to assist the agency.

30. The limitation on the avenues for review of decisions made under the Bill, the potential security threats these reforms pose, and the limitations on disclosure and reporting, highlight the need for the powers under Schedule 1 of the Bill to be subject to independent oversight. I suggest establishing an independent oversight body, with the appropriate technical expertise to assess whether each notice is necessary and proportionate in the circumstances. I note that the UK's *Investigatory Powers Act 2016* provides for the independent review of any decision made to issue a technical capability notice under that Act by a Judicial Commissioner.[18] I would suggest a similar level of oversight, at a minimum, for all decisions to issue a technical assistance or capability notice.

31. An independent oversight body could also perform the essential function of reviewing and reporting on the cumulative impacts on the security of communications as a whole, posed by the reforms. Such a body would need the skills and resources to stay abreast of continuing developments in devices, software, and networks to inform these assessments. Independent oversight, appropriately resourced, could increase public confidence that the aggregate purposes to which the notices were being put were balanced with appropriate civil liberties and human rights considerations.

I thank you again for the opportunity to comment on an exposure draft of the Bill and will watch the progression of the Bill with interest.

I have no objection to this letter being published by the Department of Home Affairs without further reference to me. I also propose to publish a copy of this letter on the OVIC website but would be happy to adjust the timing of this to allow DHA to collate and publish submissions proactively.

If you have any questions regarding any of the above, please don't hesitate to contact Emily Arians, Senior Policy Analyst at emily.arians@ovic.vic.gov.au.

Yours sincerely

Sven Bluemmel
Information Commissioner

[16] Explanatory Document, page 41.
[17] In the publication, 'What decisions should be subject to merits review?' (1999) 13, as cited on page 41 of the Explanatory Document.
[18] See s 254 of the IPA