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

12 October 2018

Our ref: D18/134138

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

Dear Committee Secretary,

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 our 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, this Bill is of particular interest to my office.

My submission primarily focuses on the privacy and data security concerns identified under Schedules 1 and 2 of the Bill. The remaining concerns I have with the Bill can be summarised as follows:

- I am not convinced that the prohibition under s 317ZG will operate effectively in practice to prevent the creation of systemic weaknesses or vulnerabilities in the system.
- I question whether there are appropriate decision-making criteria in place to ensure that the issuing of technical assistance and technical capability notices does not result in any unnecessary or disproportionate impact on the privacy and security of communications in every case.
- I am concerned about the potential for these reforms to broaden the totality of surveillance powers of law enforcement without adequate oversight from an independent body with the expertise and resources to monitor the aggregate impact of the reforms.

General comments

As a general observation, while we understand the issues faced by intelligence and law enforcement bodies in the digital age, my office is concerned with the impact 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, as noted in the Explanatory Document, released by the Department of Home Affairs during the consultation on the Exposure

Draft of 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.

The Explanatory Document referred to considerations of wider public interests[2] in decisions to issue a technical assistance notice or technical capability notice. I note relevant amendments to the Bill as introduced have been made, to expressly require decision makers to consider "the availability of any other means to achieve the objectives of the notice"[3] and "the legitimate expectations of the Australian community relating to privacy and cybersecurity".[4] These are welcome amendments.

The basis for most of the controls proposed in the Bill and the Explanatory Memorandum rest on a collective understanding of what 'reasonable' means in the context of security risks. 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 vulnerable.

The amendments in the Bill since the Exposure Draft are welcome but are still insufficient, in my view, to prevent significant risk to the security of Australia's information and individual privacy. The Bill as currently drafted contains provisions that create systemic risk. Absent stronger controls and oversight, the benefits provided to law enforcement and security agencies appear to be considerably outweighed by the risks posed to the cybersecurity of the nation.

Inclusion of website in definition of 'service'

1. My office questions whether it is reasonable and proportionate to include a website in the definition of 'service' under s 317D(2) of the Bill. The express inclusion of a website under the definition of 'service' will have the effect in practice of requiring designated communications providers to facilitate or provide assistance in accessing an electronic service (including a website). My office notes 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 to individuals in certain circumstances, such as the journalist privilege under Division 1C of the *Evidence Act 1995* (Cth).[5]

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. Section 317C (Item 6) includes a person that "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),[6] I am

[1] On page 7.
[2] On pages 34 and 38.
[3] Under new ss 317RA(e) and 317ZAA(e).
[4] Under new ss 317RA(f) and 317ZAA(f).
[5] Under ss 126J and 126K.
[6] Explanatory Document, page 14.

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, my office supports the inclusion of an express prohibition on the building of systemic weaknesses or vulnerabilities under s 317ZG of the Bill. However, I am not convinced that this prohibition will operate effectively in practice. While I note that it is not the intention of the Bill to undermine "systems that protect the fundamental security of communications,"[7] 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 was 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 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 s 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.' For this reason, I am concerned that creation of these 'one-off' vulnerabilities could fall foul of new sections 317RA(f) and 317ZAA(f), as contrary to the legitimate expectations of the Australian community relating to privacy and cyber security, thus limiting the effectiveness of the powers granted by the Bill.

7. The wording of s 317ZG(3) seems to imply that a selective weakness does not create a systemic weakness, suggesting there is a belief that selective weaknesses can be adequately secured. International experience suggests such an approach is not well-founded.

[7] Explanatory Document, page 10.

8. 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.[8] 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'

9. The way 'systemic' is defined in the Explanatory Document[9] 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[10] risk that malicious actors may take advantage of any weaknesses created. My office urges that agencies issuing technical assistance notices and technical capability notices ensure that the supporting governance and security arrangements account for the significant security risks the creation of any weakness poses for communications as a whole.

10. In the Exposure Draft of the Bill, there was a lack of clarity around how 'systemic' weaknesses would be defined and determined, for the purposes of s 317ZG. In the case of technical capability notices, it was 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. I welcome the amendments inserted into the Bill as introduced, to outline a specific process for the appointment of a technical expert, for the purposes of assessing whether a technical capability notice would contravene s 317ZG, under sections 317W(7) – (10). These amendments provide some clarity as to who will be making the assessment (during consultation) as to whether a proposed technical capability notice would create a systemic weakness. However as mentioned in above, this assessment is difficult to make on a case-by-case basis. A full understanding of the interactions of all the components of the security ecosystem will be necessary to understand systemic weakness, and the secrecy provisions of the Bill may limit the ability of the technical experts to have a complete understanding of systemic risk.

11. I would also suggest that the requirement under s 317W(7), to appoint a technical expert, for the purposes of assessing whether a technical capability notice would contravene s 317ZG, be mandatory rather than at the discretion of the Attorney-General and designated communications provider.

'Necessary and proportionate'

12. 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.

13. I also note that there is no express requirement for decision makers to consider the necessity of each of the notices. However, assuming that the requirement under the Bill as introduced for decision makers to consider "the availability of other means to achieve the objectives of the notice"[11] has been inserted to require decision makers to turn their mind to the necessity of each of the notices before

---

[8] In accordance with s 317E(1)(a), for example.

[9] On page 47.

[10] As pointed out by Dr Vanessa Teague and Dr Chris Culnane of Melbourne University, in their submission on the Exposure Draft of the Bill, '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.

[11] Under new ss 317RA(e) and 317ZAA(e).

issuing, I welcome this amendment. An assessment of whether the notice is necessary, would serve as an additional safeguard in decision making.

14. 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.[12] On this point, the insertion of sections 317RA and 317ZAA are welcome. However, there remains a lack of clarity as to whether the impact on innocent third parties will be an assessment the decision maker will be required to make in accordance with these new provisions. Given that the scheme has no merits review available for a decision to issue a notice under Division 3 or Division 4, I believe it is important to explicitly set out these relevant considerations in the Bill, to provide an 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.

15. 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. My office recommends 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.

16. 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' (for the purposes of sections 317P and 317V) 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 appears to be no proportionate way in which these elements of internet trust can be safely managed. Section 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.

17. To complement the express requirement for decision makers to consider the "legitimate expectations of the Australian community relating to privacy and cyber security"[13] when issuing a notice under Division 3 or 4, decision makers should further be required to consider any current and specific advice received on such risk (for example, under s 317W in relation to technical capability notices). Such a requirement could help to avoid the very real possibility of inadvertently creating a systemic weakness for exploitation. My office is 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.

Social engineering risk

18. I am concerned about the ability for technical assistance requests and notices, as well as technical capability notices to be issued and varied orally under the Bill. 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.

[12] Explanatory Document, pages 34 and 38.
[13] Under ss 317RA(f) and 317ZAA(f).

Duration of technical capability notices

19. I question why the duration of a technical capability notice is significantly longer than a technical assistance notice, under s 317TA of the Bill. If a technical capability notice has a duration of 180 days, there should be a strict timeframe for revocation under s 317Z. It is undesirable 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

20. There seems to be a fundamental lack of natural justice and impartiality in the appointment of arbitrators under s 317ZK, setting out the terms and conditions for technical assistance notices and technical capability requests. I am concerned specifically with the operation of s 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.

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 s 317ZF of the Bill. In the event a designated communications provider develops a weakness that becomes exposed to foreign or malicious actors, it appears that the operation of s 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.

22. The interaction of s 317ZK with s 317ZF, setting out instances where the disclosure of information is unauthorised under the Bill, is of concern. It will especially disadvantage smaller providers. Secrecy provisions surrounding notices mean that providers will be unable to explain (to shareholders and others) why profit margins may have been impacted as a result of performing what may be substantial work to comply with a notice or request, or why timelines for delivery of other promised work have been extended. As such, the capability for providers to resource a request or notice should be a component in assessing whether a request or notice is reasonable and proportionate, and this should be reflected in the Bill. It is currently unclear whether this is the type of assessment expected to be made under the new requirement for decision makers to consider the "legitimate interests of the designated communications provider to whom the notice relates."[14]

Transparency and governance

23. There is a lack of clarity both under the Bill and in the Explanatory Document[15] what "in the interests of law enforcement," under s 317T(6)(a) means. I question whether the scope of s 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 imprisonment for a term of three years or more.[16] I note that the Explanatory Memorandum[17] for the Bill states that, "it is expected that the Minister will consult with industry before tabling an instrument" with respect to determinations made under s 317T(5).

---

[14] Under ss 317RA(c) and 317ZAA(c)

[15] On page 37.

[16] Explanatory Document, page 14.

[17] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 53.

24. My office questions whether there is sufficient Parliamentary scrutiny over the Minister's power to broaden the scope of 'listed help' under s 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,"[18] which is welcome. However, 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 limited reporting required under s 317ZS, it is unclear how Parliament could develop an informed view.

25. My office expresses concern that the annual reporting requirements under s 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. My office welcomes the amendments to the Bill that require the Minister to also report on the number of technical assistance requests issued in the year.[19] However, I am of the view that the annual reporting requirement under the Bill should also include 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.

26. Upon reading s 317ZH(1)[20] 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 sections 317ZH(1)(a) – (g). 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. 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.

27. My office notes that the courts retain their inherent powers of judicial review, under s 75(v) of the Constitution, of a decision made by a senior decision maker or the Attorney General to issue a notice.[21] 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, my office suggests that ADJR review not be excluded under the Bill.

28. The Explanatory Memorandum notes that decisions to issue a technical assistance or technical capability notice will not be subject to merits review.[22] I appreciate that some decisions of a law enforcement nature (as identified in the Administrative Review Council)[23] have been identified as being unsuitable for merits review and note that the Explanatory Memorandum states that decisions to issue a technical capability notice, "where complex or political consideration exist" should rest with the executive arm of government.[24] However, I see a significant distinction between the powers under this Bill and decisions made for other law enforcement purposes. As such, I suggest the Committee consider 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. I also stress the need for senior decision

[18] On page 37.
[19] Under the new s 317ZS(1)(a).
[20] As well as page 48 of the Explanatory Document.
[21] Explanatory Document, page 11.
[22] On page 60.
[23] In the publication, 'What decisions should be subject to merits review?' (1999) 13, as cited on page 41 of the Explanatory Document.
[24] On page 60.

makers to be subject to an appropriate level of oversight by an independent body, outlined below in Points 30 and 31.

29. In the absence of merits review, the insertion of ss 317RA and 317ZAA are welcome. As a further safeguard, decision makers should have access to detailed guidance, setting out the relevant and irrelevant considerations for the purposes of ss 317P and 317V (read with ss 317RA and 317ZAA, respectively). 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. My office suggests 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.[25] 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 the Bill. It represents a dramatic expansion of the powers of law enforcement and security agencies, and the degree to which the Government is able to balance this expansion with the rights of individuals is of great interest to my office.

I have no objection to this letter being published by the Committee 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 the Committee 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

[25] See s 254 of the Investigatory Powers Act (UK).