Submission to the Department of Home Affairs on the Exposure Draft of the

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

September 2018

The Office of the Information Commissioner (OIC) is an independent statutory authority. The statutory functions of the OIC under the *Information Privacy Act 2009* (Qld) (IP Act) include commenting on the administration of privacy in the Queensland public sector environment. This submission does not represent the views or opinions of the Queensland Government.

Overview

1. The OIC welcomes the opportunity to comment on the Department of Home Affair's Exposure Draft of the Telecommunications and Other Legislation (Assistance and Access) Bill 2018 (the Assistance and Access Bill).

2. The OIC acknowledges the challenges faced by law enforcement agencies in keeping pace with emerging technologies and new means of enabling criminal activity, and recognises the discussion in the Explanatory Document outlining limits, safeguards and oversight of the use of the industry assistance measures. However, the OIC contends that given the privacy incursions that could flow from the use of Technical Assistance Requests (TARs), Technical Assistance Notices (TANs) and Technical Capability Notices (TCNs), the legislative measures proposed in this regime could go further to ensure that they –

    a. are necessary and proportionate

    b. do not jeopardise data security, and

    c. entrench adequate oversight, transparency and accountability measures.

3. The powers that would be created by the Assistance and Access Bill are particularly privacy invasive and contribute to the continual and gradual erosion of the privacy rights of individuals. Therefore, further consideration should be given to whether the proposed amendments strike an appropriate balance between privacy and other rights, including the community's right to safety and security. This is especially the case given other proposals at the Federal level that will impact privacy and human rights, many of which are yet to be settled, for example the Identity-matching Services Bill.

4. The OIC respectfully recommends that, prior to its introduction into Parliament, the Bill be reassessed for necessity, proportionality and general data security implications, and that the following practical improvements are incorporated into the Bill to strengthen oversight, transparency and accountability –

    a. sections 317P(a) and 317V(a) be expanded to stipulate in the legislation the matters that should be considered in assessing whether a notice is reasonable and proportionate, and that these requirements also be applied to TARs (see paragraphs 7 and 8)

    b. meaningful annual reporting requirements covering: errors; the number and type of all TARs, TANs and TCNs; and purpose, nature, source of authority and outcomes of TARs, TANs and TCNs (see paragraph 16)

    c. the creation of an independent judicial oversight mechanism that oversees the issuing of TARs, TANs, TCNs, and reviews and reports on their outcomes (see paragraph 17)

d. that an independent review of the legislation is undertaken within 2 years of commencement (see paragraph 18), and

e. that the nature and extent of interference with a person's privacy be expressly considered during the process of issuing a TAR, as well as for issuing a TAN or TCN (see paragraph 19).

Necessity and proportionality

5. The right to privacy is broadly recognised as a fundamental human right and entrenched in numerous treaties to which Australia is a signatory, including Article 12 of the UN Declaration of Human Rights[1] and Article 17 of the International Covenant on Civil and Political Rights[2]. While the right to privacy is not absolute and must be balanced with other rights, including public safety, 'any instance of interference must be subject to a careful and critical assessment of its necessity, legitimacy and proportionality'[3].

6. However, as drafted, the Bill provides broad powers that supplement existing law enforcement powers, such as the ability to covertly hack devices at endpoints when information is not encrypted[4]. The powers envisaged by the Bill would put the security and reliability of society's communications as a whole at risk 'to make law enforcement's job somewhat easier'[5]. If such a significant policy trade-off is to be made, it should be made after informed public debate and rigorous assessment of the potential risks. Regrettably, the compressed timeframe for the consideration of this Bill limits such analysis. Further, given potential privacy incursions, these powers should be drafted as narrowly as possible, and limited to specific areas of identified need, rather than providing broad powers, and the factors to be considered in exercising the power should be stipulated in the legislation.

7. In this regard, the OIC recommends that sections **317P(a) and 317V(a) of the Bill be re-drafted to include the broader range of factors to be considered in determining whether a notice is 'reasonable and proportionate' as outlined in the Explanatory Document**, i.e. whether other means are available to achieve the objective, the likely benefits to an investigation, likely business impact on the provider, and wider public interests, such as any impact on privacy, cyber security and innocent third parties[6].

8. It is also appropriate that these considerations be required for the issuing of a TAR, which, if complied with by a communications provider, has comparable potential for privacy incursions.

---

[1] United Nations, 'Universal Declaration of Human Rights', viewed at http://www.un.org/en/universal-declaration-human-rights/index.html, accessed on 6 September 2018.
[2] United Nations Human Rights, 'International Covenant on Civil and Political Rights', viewed at https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx, accessed on 6 September 2018.
[3] United Nations Human Rights, Office of the High Commissioner, 'The Right to Privacy in the Digital Age', viewed at https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx, accessed on 6 September 2018.
[4] Mann, M, 'The devil is in the detail of government bill to enable access to communications data', viewed at https://theconversation.com/the-devil-is-in-the-detail-of-government-bill-to-enable-access-to-communications-data-96909, accessed on 16 August 2018.
[5] MIT Press, 'Keys Under Doormats Security Report', viewed at https://mitpress.mit.edu/blog/keys-under-doormats-security-report, accessed on 6 September 2018.
[6] Department of Home Affairs, Assistance and Access Bill 2018, Explanatory Document, August 2018, pp 9, 10.

Security

9. It is apparent from the Explanatory Document that the Department of Home Affairs recognises the need to provide limitations, safeguards and privacy protections in the exercising of these powers[7]. However, the fundamental ability of law enforcement to exercise such powers remains controversial. '[C]reating…services to enable communications interception capabilities for law enforcement has persistently been criticised by cryptography and security experts as dangerous for decades'[8]. MIT's paper, *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*[9], is a useful resource that raises some critical issues to be considered. In summary, it contends that proposals like these are –

> …unworkable in practice, raise enormous legal and ethical questions, and would undo progress on security at a time when Internet vulnerabilities are causing extreme economic harm.
>
> As computer scientists with extensive security and systems experience, we believe that law enforcement has failed to account for the risks inherent in exceptional access systems. Based on our considerable expertise in real-world applications, we know that such risks lurk in the technical details…Our strong recommendation is that anyone proposing regulations should first present concrete technical requirements, which industry, academics and the public can analyse for technical weaknesses and hidden costs.[10]

10. This sentiment is echoed in current IT and cybersecurity commentary, which concurs that this 'is not a solution to catching criminals but it is weakening the defences of every single device that receives encrypted messages, therefore making it easier for criminals who want to steal data'[11]. Despite the ban on 'backdoors', commentators assert that it's unclear how tech companies will be able to fully comply with the proposed laws without backdoors, inherently creating the risk that this vulnerability will be open 'for other entities capable of exploiting the access as well'.[12] It is not clear how powers aimed at weakening encrypted systems for law enforcement will not weaken encrypted systems for everyone[13].

11. Other questions regarding security implications that warrant further consideration are: whether good operators are likely to relocate their operations to avoid the uncertainty created by such a regime; which, if any, technical experts will be engaged to act as advisors on the question of whether the help sought via a TAN or TCN constitutes or risks 'systemic' weakness; and how will law enforcement agencies protect tools provided via a TAN or TCN from the type of leak, theft or misuse experienced by the US National Security Agency at the hands of the 'Shadow Brokers'[14]?

---

[7] Ibid, p9.
[8] Saarinen, J, 'Five-Eyes nations to force encryption backdoors', viewed at https://www.itnews.com.au/news/five-eyes-nations-to-force-encryption-backdoors-511865, accessed on 6 September 2018.
[9] Abelson, H et al, 'Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications', Computer Science and Artificial Intelligence Laboratory Technical Report, Massachusetts Institute of Technology, viewed at https://www.csail.mit.edu/research/keys-under-doormats.
[10] Ibid, p1.
[11] Crozier, R, 'Govt finally reveals how it plans to target encryption', viewed at https://www.itnews.com.au/news/govt-finally-reveals-how-it-plans-to-target-encryption-500156, accessed on 6 September 2018.
[12] Domanski, H, 'Encrypted communications targeted by new Australian anti-crime law', viewed at https://www.techradar.com/au/news/encrypted-communications-targeted-by-new-australian-anti-crime-laws, accessed on 6 September 2018.
[13] Domanski, H, 'Math be damned: Australian PM demands encrypted chat apps be opened up for law enforcement', viewed at https://www.techradar.com/au/news/laws-of-mathematics-be-damned-australian-pm-demands-encrypted-chat-apps-be-opened-up-for-law-enforcement, accessed on 6 September 2018.
[14] See https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html.

Oversight, transparency and accountability

12. Any powers that encroach on privacy should be subject to independent oversight and review, be transparent, and have clear and ongoing accountability measures in place.

13. The regime appears to be largely based on the UK's *Investigatory Powers Act 2016*, which itself has been subject to credible criticism and a successful legal challenge requiring redrafted legislation to be drawn up by November[15]. This is despite the UK Act providing protections not replicated in the Australian Bill, including extensive judicial oversight by the Investigatory Powers Commissioner (which is in addition to the Investigatory Powers Tribunal), and a specific requirement that public authorities using the powers have regard to privacy[16].

14. Part 8 of the UK Act – Oversight arrangements – provides extensive measures for overseeing (s229) and reporting on (s234) the regime, including reporting on the number and type of uses of powers, information about the result of those uses including impact, and the operation of safeguards. It also specifically requires error reporting (s231) and that 'the Investigatory Powers Commissioner must, in particular, keep under review the operation of safeguards to protect privacy' [s229(5)].

15. In contrast, the Australian Bill does not establish any judicial oversight of the issuing of TARs, TANs, or TCNs, and annual reporting requirements are limited only to the numbers of TANs and a specific subset of TCNs[17] to be reported upon annually under Chapter 4 of the *Telecommunications (Interception and Access) Act 1997*.

16. OIC recommends that **annual reporting requirements** include –

    a. Reporting on the number and type of all TARs, TANs and TCNs (including TCNs that

    b. Reporting on the purpose, nature, source of authority, and outcome of all TARs, TANs and TCNs

    c. Reporting on errors, in a manner similar to section 231 of the UK *Investigatory Powers Act 2016*.

17. The issuing of TARs, TANs and TCNs should be overseen by an **independent judicial oversight mechanism**, which also reviews all instances of government access to personal data under warrant and reports on the virtues or shortcomings of that access against enforcement outcomes and privacy principles.[18] Other options may include appointing a Public Interest Monitor or engaging the Independent National Security Legislation Monitor to (as is consistent with its existing functions) review the operation, effectiveness and implications of these measures and consider

---

[15] Cobain, I, 'UK has six months to rewrite snooper's charter, high court rules', viewed at https://www.theguardian.com/technology/2018/apr/27/snoopers-charter-investigatory-powers-act-rewrite-high-court-rules, accessed on 6 September 2018.

[16] Section 2 – General duties in relation to privacy, Investigatory Powers Act 2016 (UK), viewed at http://www.legislation.gov.uk/ukpga/2016/25/section/2/enacted.

[17] Section 317ZS(1)(b)(ii) indicates that only the number of TCNs 'directed towards ensuring that designated communications providers *are capable of giving help to interception agencies*' must be reported upon. However the Explanatory Document, at page 36, indicates that for 'administrative efficiency, a technical capability notice may also operate as a quasi-technical assistance notice. A technical capability notice can require a provider to do a thing it is already capable of doing'. Therefore, based on the wording of 317ZS, it seems likely that a TCN acting as a quasi-technical assistance notice, would not fall within 317ZS(1)(b)(ii).

[18] Austin, G, 'New data access bill shows we need to get serious about privacy with independent oversight of the law', viewed at https://theconversation.com/new-data-access-bill-shows-we-need-to-get-serious-about-privacy-with-independent-oversight-of-the-law-101378, accessed on 16 August 2018.

whether the laws contain appropriate protections for individual rights, remain proportionate, and remain necessary.

18. OIC also notes the absence of review arrangements for the operation of the legislative amendments as a whole, and recommends that the Bill include a requirement for an **independent legislative review** of the regime to commence within two years of its operation.

19. It is also of concern that TARs are not subject to any consideration of the nature and extent of interference with a person's privacy, factors to which a judge or Administrative Appeals Tribunal member must have regard in issuing the underlying warrant necessary for the issuing of a TAN or TCN (as highlighted on page 10 of the Explanatory Document). Consideration of the **nature and extent of interference with a person's privacy should be a necessary precursor to the issuing of a TAR**.

20. The OIC appreciates the Department of Home Affairs' consideration of this submission and is available to provide further information or assistance as required.