25 October 2019

Dr James Renwick CSC, SC
Independent National Security Legislation Monitor
By email: inslm@inslm.gov.au

Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

Dear Dr Renwick,

About us

We work with the Allens Hub for Technology, Law and Innovation ('the Allens Hub') — an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law, the Allens Hub aims to add depth to research on the diverse interactions among technology, law, and society. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society and the broader community. More information about the Allens Hub can be found at http://www.allenshub.unsw.edu.au/. Our submissions reflect our views as researchers and are not an institutional position.

Focus of submission: Transparency and Accountability

The attached article sets out research on the importance of transparency and accountability of law and systems in the national security and law enforcement context.[1] This compares Australian and UK approaches, albeit in the context of untargeted rather than targeted data collection and analysis. However, many of the points made there apply equally in this context. In particular,[2]

- Decisions around the boundaries of national security and law enforcement agencies' power to collect, access, analyse and act upon data should be democratically based. This broad context is essential for public trust. It requires meaningful democratic debate, which requires a degree of transparency and openness. In particular, the public should have sufficient information regarding the exercise of powers and the managerial, political and independent oversight of the exercise of those powers to hold government accountable for its actions. This is also consistent with Australia's commitments internationally, including under the Open Government Partnership.

[1] Lyria Bennett Moses and Louis De Koker, 'Open Secrets: Balancing Operational Secrecy and Transparency in the Collection and Use of Data by National Security and Law Enforcement Agencies' (2017) 41 *Melbourne University Law Review* 561.

[2] References and arguments are in Bennett Moses and De Koker, above n 1

- Transparency is not simply a question of publishing legal rules, but ensuring that those rules are clear, coherent, simple and comprehensible.[3] Subject to the following point, the justification for the existence of powers should also be explained publicly.
- There is a need to balance the legitimate need for secrecy with the importance of transparency, bearing in mind that cultures of secrecy and incentives for secrecy in the national security community can extend beyond strategic need. Oversight agencies (such as IGIS and ombudsmen) play an important role in system-wide accountability but are not a substitute for maximising public transparency within necessary constraints. Transparency is thus layered – the general public will not have the same information as the agency or an oversight agency.

The article went on to discuss the relative complexity and non-transparency of the Australian legal framework and the relative lack of public justification for particular powers, comparing the broader public debate in the UK, facilitated in part through a series of reports that culminated in the *Investigatory Powers Act*. This debate has led to UK to move from debating "privacy or security" to solving the challenge of "privacy and security".

Impact on INSLM questions

The INSLM's review will consider whether the Act achieves an appropriate balance, whether the Act contains sufficient safeguards for protecting the rights of individuals and remains proportionate and necessary. This is not merely a question of the rights of individuals, but rather the capacity of the public to engage with the exercise that the INSLM has been tasked with. We therefore encourage the INSLM to engage with an important background question – whether the rules are sufficiently clear; whether their justification has been sufficiently explained and is sufficiently understood; and whether ongoing reporting is enough to ensure that the public can engage meaningfully with these questions. This is not simply a question of the rights of individuals, but rather the capacity of the public to engage with the exercise that the INSLM has been tasked with and the democratic legitimacy (or democratic licence) of the framework.

Known unknowns

The Department of Home Affairs, in its submission dated September 2019, concedes that the legislation is complex and that there have been diverse interpretations and understandings of its effect. In our view, this is not a reason to critique the interpreters, but rather an opportunity to draft legislation where intent is clear and its impact has been subject to sufficient public-facing analysis. On the contrary, the potential impact of this legislation seems to be subject to extensive disagreement, despite the possibility of testing the claims made by different stakeholders empirically.[4] Examples include:

- The extent to which interception capabilities to access the content of communications remains important in investigations, particularly given developments in accessing data at rest and the collection and retention of metadata.[5]
- The extent to which encryption will become ubiquitous.[6]

---

[3] Torbjorn Larsson, 'How Open Can a Government Be? The Swedish Experience' in Veerle Deckmyn and Ian Thomson (eds), Openness and Transparency in the European Union (European Institute of Public Administration, 1998) 39, 40-2.

[4] Mayank Varia, 'A Roadmap for Exceptional Access Research', *Lawfare* (5 December 2018).

[5] Compare Harold Abelson et al, Computer Science and Artificial Intelligence Laboratory Technical Report, *Keys Under Doormats: Mandating insecurity by requiring governmental access to all data and communications* (6 July 2015) ("On the contrary, law enforcement has much better and more effective surveillance capabilities now than it did then.") with James B. Comey, Federal Bureau of Investigation Director, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?," speech delivered to Brookings Institution, October 2014 ("We call it 'Going Dark,' and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority.")

[6] Compare Berkmann Center for Internet & Society, *Don't Panic: Making Progress on the "Going Dark" Debate* (1 February 2016) ("End-to-end encryption and other technological architectures for obscuring user data are unlikely to be adopted ubiquitously by companies, because the majority of businesses that provide communications services rely on access to user data for revenue streams and product

- The extent to which secure backdoors can be built[7] and, if they can, the degree of damage to the broader network security and encryption protocols caused by aces requirements such as the TOLA amendments.[8]
- The extent to which autocratic regimes and bad actors can leverage the mandate and technological changes associated with Australia's policy (or the US or UK policy).[9]
- Impact on Australian industry – loss of international competitiveness and costs of compliance.[10]

Need for clear rules

The wide range of interpretations for crucial terms in the legislation such as "systemic vulnerability" and "systemic weakness" suggest that clearer definitions are required. While legislation should avoid unnecessary technological specificity, it is necessary that both industry and the public, as well as overseas stakeholders, understand the outer limits of the powers granted and the extent to which cyber risks might be generated. If the Act aims to avoid imposing new cyber risks on non-targeted individuals, then this should be explicit in the definitions. For example, Minister Dutton, in a letter to Facebook, suggested that "Companies should not deliberately design their systems to preclude any form of access to content."[11] Is this an example of a matter that could be subject to a TCN under the Act?

The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) amendments operate across a range of existing laws which are already complex. Revisions to both the *Telecommunications (Interception and Access) Act 1979* (Cth) and the *Telecommunications Act 1997* (Cth) have resulted in duplication, confusion, conflict and issues with interpretation. The *Blunn Review* in 2005;[12] the Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice Report 108* in 2008,[13] the *Inquiry into Potential Reforms of Australia's National Security*

---

functionality, including user data recovery should a password be forgotten.") with Eric Manpearl, 'Preventing Going Dark: A Sober Analysis and Reasonable Solution to Preserve Security in the Encryption Debate' (2017) 28:1 *University of Florida Journal of Law and Public Policy* 65, 79 ("Even if end-to-end encryption does not become widespread, it may still pose a significant threat if enough sophisticated malicious actors utilize products that adopt end-to-end encryption.")

[7] Compare Harold Abelson et al, Computer Science and Artificial Intelligence Laboratory Technical Report, *Keys Under Doormats: Mandating insecurity by requiring governmental access to all data and communications* (6 July 2015) ("Communications technologies designed to comply with government requirements for backdoors for legal access have turned out to be insecure.") with Eric Manpearl, 'Preventing Going Dark: A Sober Analysis and Reasonable Solution to Preserve Security in the Encryption Debate' (2017) 28:1 *University of Florida Journal of Law and Public Policy* 65, 99 ("Cryptographic envelopes, split key encryption, and possibly even biometric encryption, depending on how widespread end-to-end encryption is adopted, all present potential solutions for achieving this technological mandate in a secure manner.")

[8] Compare the terms of s 317ZG with concerns raised in many submissions that the definitions and interpretations of "systemic weakness" and "systemic vulnerability" are too narrow. See also Harold Abelson et al, Computer Science and Artificial Intelligence Laboratory Technical Report, *Keys Under Doormats: Mandating insecurity by requiring governmental access to all data and communications* (6 July 2015) ("We have found that the damage that could be caused by law enforcement exceptional access requirements would be even greater today than it would have been 20 years ago.") and Access Now, *The Role of Encryption in Australia: A Memorandum* (January 2018). Confusion around the impact of the Act was not helped by statements to the effect that the laws of mathematics must give way to national law.

[9] See eg Berkmann Center for Internet & Society, *Don't Panic: Making Progress on the "Going Dark" Debate* (1 February 2016) ("if the U.S. government were to mandate architectural changes, surveillance would be made easier for both the U.S. government and foreign governments, including autocratic regimes known to crack down on political dissidents.")

[10] On the one hand are arguments about international perceptions of the Australian law, on the other are observations that many companies' business strategies are inconsistent with high levels of consumer privacy.

[11] Letter to Mark Zuckerberg from Rt Hon Priti Patel MP, William P Barr, Keven K. McAleenan and Hon Peter Dutton MP (4 October 2019).

[12] Anthony Blunn AO, Attorney Generals Department, *Report of The Review of The Regulation of Access to Communications*, August 2005, Recommendations, 10; Recommendation (i) 'comprehensive and over-riding legislation dealing with access to telecommunications data for security and law enforcement purposes be established' amongst other recommendation for review.

[13] Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice Report 108 (2008) Recommendation 71-2.

Legislation (2013) at Recommendation 18;[14] the Chair's Minority Additional Comments from the *Comprehensive Revision of the Telecommunications (Interception and Access) Act 1979 (2015)*[15] and various submissions to inquiries held in 2010, 2013 and 2015 have called for the Act/s to be reviewed, revised and/or rewritten. The *TOLA* amendments add to this complexity. To ensure clarity, which we believe is essential for public transparency, the *Telecommunications (Interception and Access) Act 1979*, the *Telecommunications Act 1997* and the *Surveillance Devices Act 2004* should be redrafted into a comprehensive and consistent statutory regime. This would also provide an opportunity for greater public consultation around the proportionality of intercepts, assistance requests, computer access warrants, surveillance warrants and metadata access and retention.

Need for public justification

While agencies cannot disclose matters for which operational secrecy is required, the *Report of the Bulk Powers Review*[16] in the UK highlights how public disclosure of the justification for powers can assist public debate around the necessity for and proportionality of powers granted. Ideally, justification for the new powers will go beyond noting the need for law to keep up with technology, providing information on:

- quantitative and qualitative information on how the powers have been used and what they have achieved;
- the costs and benefits of the TOLA amendments in light of further analysis of the "known unknowns" set out above;
- risks and benefits associated with the scope of legislation, in particular its extension to foreign offences;
- how costs will be fairly allocated, for example where an ultimately innocent individual suffers financial loss as a result of compromised security due to the implementation of a request or notice; and
- choices concerning the level of review and oversight provided for in the legislation (including comparisons to arrangements in comparable jurisdictions).

Ideally, public justification would go beyond explanation and include engagement and debate.

[14] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into Potential Reforms of Australia's National Security Legislation* (2013) Recommendation 18.

[15] Legal and Constitutional Affairs References Committee, Parliament of Australia, *Comprehensive revision of the Telecommunications (Interception and Access) Act 1979* (2015) Minority Report (Senator Ludlam).

[16] David Anderson QC, *Report of the Bulk Powers Review* (Cmd 9326, 2016).

More comprehensive reporting

Reporting under the Act should be sufficient for government, industry and the general public to get a sense of the costs and benefits of the Act. For this, s 317ZS is manifestly insufficient. Reporting should include qualitative as well as quantitative information about issued requests and notices, including systematic data about the benefits of the program (in terms of types of offences, discovery of plots, conviction of offenders, etc).[17] Provisions that prevent disclosure, such as s 317ZF, should have a time limit or lapse at the close of the relevant investigation. Disclosures in annual reports should include data-based *evaluative statements* of the Act in terms of whether and why it is viewed as meeting its objectives, what has been gained and what, if anything, has been lost, in particular in terms of cyber security and trust in Australian networks and companies. Such reporting, if conducted regularly with a fixed deadline each year, would facilitate a broader, more evidence-based, conversation around many of the concerns raised in submissions without immediately undermining or weakening the exercise of powers under the Act by the relevant authority.

Lyria Bennett Moses, Director, Allens Hub for Technology, Law and Innovation, UNSW Law

Genna Churches, PhD Candidate and Member of the Allens Hub for Technology, Law and Innovation, UNSW Law

Nicholas Parker, Research Assistant, Allens Hub for Technology, Law and Innovation, UNSW Law

[17] For an example, see https://www.uscourts.gov/statistics-reports/wiretap-report-2018.