Electronic Frontiers
AUSTRALIA

:

W www.efa.org.au
E email@efa.org.au
@efa_oz

6 March 2020

Dr James Renwick CSC SC
Office of the Independent National Security
Legislation Monitor (INSLM)
Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600

By Email: INSLM@inslm.com.au

Dear Dr Renwick CSC SC,

RE: Review of the Telecommunications and other Legislation Amendment (Assistance & Access) Act 2018

1. We refer to the abovementioned review, to the public hearing conducted on 20 February 2020 ("**the Hearing**") and to your invitation to provide a supplementary submission to the abovementioned review.

2. At the outset, we repeat our gratitude for your ongoing interest and careful consideration into the TOLA and we provide this further submission in supplement to previous submissions and to the evidence provided at the Hearing.

3. We have provided succinct responses to questions arising at the Hearing under discrete headings below for ease of reference.

Is the TOLA a form of mass surveillance?

4. At the Hearing, the writer was queried as to EFA being the only organization that held concerns regarding the TOLA's potential application as a tool for mass surveillance. EFA respectfully maintains its position in this regard and it is relevant to note that the joint submissions provided to the INSLM were works of joint authorship with the authors' qualifications set out, in relation to the October 2018 Submission at pages six (6) and seven (7). Those authors qualifications included academic and practicing lawyers, cyber security architects, information systems specialists and criminologists.

5. In that submission, the inclusion of s. 31 of the *Telecommunications (Interception and Access) Act 1979* ("**TIA**") was compared to the clandestine operation by the Communications Security Establishment (Canada) ("**CSE**") in 2014 where a "test" conducted by the CSE effectively constituted indiscriminate mass surveillance of Canadian and non-Canadian citizens in airports[1].

6. A similar situation would be possible under the TOLA amendments to the *Telecommunications (Interception and Access) Act 1979* via Part 2.4 of that Act. Such a situation arises where the head or acting head of a security authority (being broadly defined as an authority of the Commonwealth that has functions primarily relating to security, collection of foreign intelligence, the defence of Australia or the conduct of the Commonwealth's international affairs)[2] may request of the Attorney General authorisation to develop or test interception of communications passing over a telecommunications system.

7. You would appreciate that the issue of mass surveillance is that, as demonstrated by the Snowden whistleblowing, such arrangements are secret and conducted in a manner that is not transparent. This requires blind trust in government to use (now and in the future) surveillance techniques in a manner that is responsible and proportionate.

8. In direct further assistance to the limiting factors that you (correctly) raised during the Hearing, our concern is that these factors are not sufficient as they leave the door open for mass surveillance.

9. Firstly, if we take the example of s. 317P (in relation to TANs), we accept that the concept of "reasonable and proportionate" is imported into the decision making criteria. However, the truly relevant section is s. 317RA which provides a list of matters which much be considered when determining if a TAN is reasonable and proportionate. It is important to note that:

    a. Australia does not have an enforceable federal human rights framework.

    b. The majority of these considerations are focused towards the interest of law enforcement (see: 317RA(a),(b),(d),(e)(ea), (eb) and (g) with the only counterweighing considerations being the legitimate interests of the designated communication provider to whom the notice relates (317RA(c)) and the legitimate interest of the Australian community relating to privacy *and* cybersecurity (317RA(f). Respectfully, for something to be reasonable and proportionate there ought to be a higher and greater focus on Australians' human rights and the preservation of Australians' fundamental human rights[3].

---

[1] This document is sourced from https://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881 and the writer does not otherwise submit to its provenance.
[2] Section 5(1) of the TIA.
[3] We respectfully draw attention to the stark contrast in the approach being adopted in the European Union with Advocate General Campos Sánchez-Bordona's recent opinion on matters before the Court of Justice of the European Union that engage human rights issues against national security interests. In his opinion, the means and methods of combatting terrorism must be compatible with the rule of law and human rights. See: Advocate General's Opinions in Case C-623/17 Privacy International, Joined Cases C-511/18

c. The concepts of privacy and cybersecurity should not be conflated.

10. Secondly, if we take the example of s. 317ZH which provides that a TAR, TAN or TCN "has no effect to the extent (if any) to which it would request or require a designated communications provider to do an act or thing for which the agency, or an officer of the agency, would be required to have or obtain a warrant or authorisation". There are two clear issues with this limitation:

    a. this requires a designated communications provider to be aware of the general limitation and willing to resist the agency's request. This engages the following issues:

        i. whether the designated communications provider has proper legal assistance;
        ii. whether the designated communications provider has the financial resources to resist the agency's request;
        iii. whether the designated communications provider's risk assessment is such that the resistance of the TAR, TAN or TCN overrides the potential (severe) penalty for non-compliance; and
        iv. whether designated communications provider is technically able to achieve compliance with a TAR, TAN or TCN without knowingly or unknowingly operating in a manner which would have properly required a warrant.

    b. the limitation must be construed with reference to the effect of ss. 317ZH(4) and (5) that limit the limitation. By way of example, in relation to a TAR, the limitation at s. 317ZH(1) does not prevent a TAR issuing that would require a warrant if, pursuant to s. 317G(2)(b)(v) or (vi), the assistance requested was by the Director-General of Security – ASIO made the request in relation to a matter that facilitates the objective of a law. The scope of this provision enlivens a vast array of legislative objectives many of which are generally tasked towards the ambiguous concept of the safety of Australia. Effectively, in our submission, the limitation serves little purpose as it is overridden by ss. 317ZH(4) and (5).

11. To be clear, our submission is not that the TOLA is a regime of mass surveillance of Australian citizens – our submission is that the scope of the amendments by the TOLA means that such a regime *could* be deployed in future and we submit that the appropriate check and balance against such a system requires introducing a federal enforceable human rights framework and judicial oversight over the use of surveillance in Australia (and we return to this concept below).

12. We trust that the above is of assistance.

La Quadrature du Net and Others and C-512/18 *French Data Network and Others*, and Case C-520/18 *Ordre des barreaux francophones et germanophone and Others* (Press Release No. 4/20, 15 January 2020).

13. Please do not hesitate to contact the writer should you require any further information or documentation.

Yours sincerely,

Angus Murray
Chair of the Policy Committee
Electronic Frontiers Australia