Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

4 March 2015

Mrs Jane Prentice MP
Chair
House of Representatives Standing Committee on Infrastructure and Communications
ic.reps@aph.gov.au

Dear Mrs Prentice

Re: Inquiry into the use of s.313 of the Telecommunications Act

While giving evidence to the Committee today, I was asked two questions which I was unable to answer on the spot. I provide the following information and would be pleased if you would accept it as a Supplementary Submission.

(1) Prior APF Submissions in Relation to TA s.313

The scores of APF Submissions on telecommunications matters are indexed here:
https://www.privacy.org.au/Papers/indexPolicies.html#TelecommsDNC

The term "s.313" occurs just once, and a copy of the relevant text is in the attachment. This relates solely to the scope for s.313 to be used as an uncontrolled means of 'requesting' content from ISPs. The absence of any deeper consideration bears out my statement that the effect of s.313 was invisible to the Parliament, the public, and APF until the ASIC incident.

(2) ALRC Comments in Report 108 (2008)

A search for the string <313> in the three volumes of the Report finds no relevant text:
http://www.alrc.gov.au/publications/report-108
That is also consistent with the real nature of the provision having been always 'under the radar'.

In case any ambiguities arise, the notes that I was speaking from while giving verbal evidence are at:
http://www.rogerclarke.com/DV/TA313.html. APF would be pleased to provide further clarifications if that would assist.

Yours sincerely

Roger Clarke
Immediate Past Chair, Australian Privacy Foundation
(02) 6288 6916 Roger.Clarke@privacy.org.au

Exposure Draft Telecommunications (Interception and Access) Bill 2007

Submission to the Attorney-General's Department
February 2007

[top of p.3]

Access to content and substance

While we welcome the clarification in proposed TIAA section @172 that proposed TIAA Part 4-1, Divisions 3 to 5 do not allow disclose of the 'content and substance' of communications, **we remain very concerned that the 'loophole' of the existing TA s.280 appears to have been confirmed in proposed amendments to TA s.313**. This section would expressly mandate carriers and CSPs to provide assistance to government agencies that included disclosure of information in accordance with TA s.280 (proposed ss. 313(7)(e)). Without amendment of TA s.280, **this would potentially mandate the disclosure of content and substance, as an alternative to the more controlled access regime in the TIAA**. Like the EFA, we refer the committee to its previous recommendation, and support the amendment to s.280 proposed by EFA.

We are very disappointed that such a fundamental revision of the relevant provisions has missed the opportunity to more clearly define what is meant by key terms such as 'telecommunications data' and 'content or substance'. This creates unacceptable ambiguity and uncertainty about the reach of the various powers and protections. It also leaves open the possibility that very sensitive information such as mobile phone location data, email message headers and various internet logs would not be considered 'substance or content' or stored 'communications', and would therefore be subject not to the TIAA warrant controls but to the much weaker protection applying to 'authorisations' under the proposed TIAA Part 4-1 (and to the unconstrained discretion to make voluntary disclosures (see next paragraph). We submit that a much clearer legislative distinction between 'traffic data' and 'substance and content' is required.