Supplementary Remarks — The Hon Tony Smith MP

Having only joined the Committee in February of this year, I was a participating Member for only the final public hearing in March, and consequently was not part of the extensive deliberations with over 50 witnesses at 10 days of public hearings in 2009, when the vast bulk of the evidence was taken.

As such the report's recommendations are very much a product of the considered views of Members formed during those months of hearings and deliberations of which I was not part.

Nonetheless, from my limited involvement on the Inquiry, I believe that, overall, the report is an important contribution to the debate with many sensible and practical recommendations for consideration. I do, however, have a different view on some aspects of the report, which I have outlined below.

In this short period of time, it has become very clear to me that participating Members, led by the Chair and Deputy Chair, worked very hard over many months distilling and weighing the issues. They have been ably assisted by Jerome Brown, Committee Secretary, Jane Hearn, Inquiry Secretary, and the other staff from the Committee Secretariat.

Recommendation 14

Recommendation 14 states:

> **That the Australian Communications and Media Authority take the lead role and work with the Internet Industry Association to immediately elaborate a detailed e-security code of practice to be registered under the *Telecommunications Act 1997* (Cth).**
>
> **That the code of practice include:**

- **an obligation that the Internet Service Provider provides basic security advice when an account is set up to assist the end user to protect themselves from hacking and malware infections;**
- **a mandatory obligation to inform end users when their IP address has been identified as linked to an infected machine(s);**
- **a clear policy on graduated access restrictions and, if necessary, disconnection until the infected machine is remediated;**
- **the provision of basic advice and referral for technical assistance for remediation; and**
- **a requirement that acceptable use policies include contractual obligations that require a subscriber to:**
  - ⇒ **install anti-virus software and firewalls before the Internet connection is activated;**
  - ⇒ **endeavour to keep e-security software protections up to date; and**
  - ⇒ **take reasonable steps to remediate their computer(s) when notified of suspected malware compromise.**

The substance of the recommendation and the first four stipulated items for inclusion within a proposed Code are worthy.

However, I believe the last suggested inclusion relating to subscriber contractual obligations is problematic.

Every fair minded person agrees that it is critical to take steps to ensure all internet subscribers understand the importance of, and their responsibility to secure and maintain security of, their own computer systems.

It is clear that while many Australians do take steps to ensure the security of their systems by installing and diligently maintaining security software, large numbers do not, many of whom are unaware of the dangers and potential costs to themselves and the wider community.

Continued education and awareness building at a wide range of levels is the first priority to ramping up knowledge, understanding and action.

However, to dramatically and quickly institute a requirement that ISPs contractually require the subscriber to install anti-virus software and firewalls before connecting to the internet, whilst well meaning, opens up a plethora of new liability issues for subscribers.

Such a move could only be considered in the longer term following careful consideration of the implications to subscribers in terms of their liability, and only

after comprehensive communication over a significant period of time about the implications of such a fundamental change.

Because the fundamental intent of Recommendation 14 is to register an e-security code with 'speed' ("*That the Australian Communications and Media Authority take the lead role and work with the Internet Industry Association to* ***immediately*** *elaborate a detailed e-security code...*"[1]), I do not believe that this aspect of the recommendation could be implemented without creating major uncertainty and dislocation.

Recommendation 26

In my view, the approach with this recommendation is in some conflict with the approach taken in Recommendation 25, which is for the Productivity Commission to carry out a broader in depth investigation to provide more comprehensive analysis to support future policy development in this area.

It makes sense for the Productivity Commission to consider all of the issues in depth, particularly since any changes resulting from Recommendation 26 could have an impact on the broader market, and recommend on the full and appropriate suite of measures that might be considered.

Recommendations 28–30

Recommendations 28–30 are worthy.

However, I note the Committee's view that the current general exemptions to the *Privacy Act* relating to small business should be removed.

Whilst the expressed view does not translate into a recommendation, I point out that the general small business exemption has been in place as an acknowledgment of the costs that would be entailed by small business if they were brought under the Act.

1 Emphasis added.

I believe the focus should be on the adoption of codes of practice in areas where there is a clear necessity, which is precisely what Recommendation 29 envisages with respect to the Australian Internet industry, including smaller ISPs, rather than adopt a blanket approach that would place a burden on all small businesses.

Hon Tony Smith MP