DISSENTING REPORT BY AUSTRALIAN GREENS

1.1 Unfortunately the Committee was unable to hold a hearing into this Bill which makes yet another set of amendments to the Telecommunications Interception Act, in this case to allow interception, copying, recording and disclosure of electronic communications in the name of protecting computer networks from malicious access and building confidence in the online world. It also allows specified government organisations – law enforcement, national security, defence and international relations - to intercept communications and undertake disciplinary actions ensure that computer networks are appropriately used.

1.2 While much improved through consultation on an August exposure draft, during the Inquiry into this Bill the Privacy Commissioner, Electronic Frontiers Australia and the Australian Law Reform Commission recommended minor amendments to a) clarify definitions of what constitutes "network protection duties" and "disciplinary actions" b) tighten requirements to destroy copies of intercepted communications.

1.3 The Australian Greens concur that these amendments are necessary to clarify the Bill and strengthen its safeguards and are not satisfied that the Attorney General's Department adequately addressed these suggestions when dismissing them.

1.4 The Attorney General claims that network protection activities vary for each network and therefore cannot be defined, however, given that this is the pretext for this suite of amendments it is not inappropriate that parameters should be set and the scope and nature of activities more clearly defined. The Privacy Commissioner asked, "what measures are covered by 'the operation, protection or maintenance of the network' and when is an interception 'reasonably necessary?'

1.5 The Attorney states that imposing an obligation to destroy copies of lawfully intercepted information is unenforceable. As the Australian Law Reform Commission submitted, arising from the Commission's thorough inquiry into privacy issues, there is, "no reason why copies of information obtained from a stored communication warrant must be destroyed but copies of information obtained from an interception warrant are not… The covert nature of interception and access to communications requires the safeguard that the intercepted or accessed information is destroyed as soon as it is no longer required."

1.6 Given these issues were thoughtfully raised, and could easily be addressed through minor amendments, the Australian Greens do not share the Committee's view that the Bill should be passed without amendment.

Senator Scott Ludlam