9 October 2009

Committee Secretary
Senate Legal and Constitutional Committee
Parliament House
Canberra ACT 2600
Australia

By email: legcon.sen@aph.gov.au

Dear Sir/Madam

Telecommunications (Interception and Access) Amendment Bill 2009
Confidential Submission

I am writing in response to the invitation for submissions concerning the *Telecommunications (Interception and Access) Amendment Bill 2009* (the **Bill**) and the *Telecommunications (Interception and Access) Act 1979* (the **TIA Act**).

I am a lawyer practising in the area of information technology. In that role I have been called to advise on the TIA Act and new developments several times. However, I am making this submission in a private capacity and my views in this letter are entirely my own.

I write from the perspective of a lawyer advising a typical corporate entity or government agency, rather than a Commonwealth agency, security authority or eligible authority of a State.

My general impression of the Bill is that it will provide a welcome but limited degree of assurance for organisations managing electronic communications and computer networks on a day to day basis.

My concerns do not so much relate to the policy and privacy issues surrounding the interception of incoming emails by the administrators of corporate networks. Rather, they concern the extent to which the Bill will leave the prohibition of interception under the TIA Act:

- uncertain in scope; and
- inconsistent with the standard practices and realities of corporate network management.

I note the comment by Senator Ellison in relation to the *Telecommunications (Interception) Amendment Act 2006* (Senate Official Hansard, No. 3, 29 March 2006, p 125) referring to a need for a 'solution to the conflict between the general

prohibition against interception and the need to allow appropriate access for network administrators to conduct their activities lawfully'.

The Explanatory Memorandum to the Bill states that:

> 'The Bill ensures that all legitimate activities in relation to protecting computer networks, whether it is the infrastructure or the information stored or transmitted by them, which are undertaken by network administrators in either the government or non-government sectors, do not inadvertently constitute an offence under the TIA Act.'

I am not convinced that the Bill fulfils the need identified by Senator Ellison or the function stated in the Explanatory Memorandum. There are activities that network administrators and other users of computer networks continue to engage in regardless of the TIA Act that will still potentially be unlawful despite the proposed amendments. Some of these are everyday activities that almost all network administrators would do and users would accept without thinking there is any possibility of contravening the TIA Act.

Amendment of the TIA Act is urgently required, but I am concerned that passing of the Bill in its present form will represent a lost opportunity to introduce the necessary degree of clarity.

My concerns, as expanded on in this letter, include the following:

1. The legality of standard practices for dealing with nuisance spam emails remains unclear.

2. Standard practices concerning employee changes and absences appear to be unlawful, including for circumstances such as:

   (a) leave;

   (b) termination of employment (resignation, dismissal or retirement); and

   (c) change in address.

3. Common commercial practices involving redirection of emails for other purposes appear to be unlawful.

4. The legality of typical email quarantining practices is unclear under the definition of 'accessible'.

I regularly find myself in a position where I am told by network administrators that they engage in certain practices in relation to email, that the practices are standard throughout the industry, and that they are demanded by management. They are appalled to be told that the practices are illegal or that the legislation is insufficiently clear for me to provide any assurance that they are not exposed to considerable personal liability and penalties. This extends to scanning of incoming email for inappropriate content. On the other hand, I regularly encounter email users who

believe that network administrators do, and are entitled to carry out, scanning practices that are also illegal or dubious under the legislation. At the very least, there seems to be a considerable disconnect between the law and the beliefs of administrators and users of computer networks. If conduct is to be unlawful, then surely this should be made clear in the legislation and an effort should be made to ensure that the general community is aware that it does not accord with their beliefs, particularly where lack of compliance may be pervasive and the consequences are potentially drastic.

1. The legality of standard practices for dealing with nuisance spam emails remains unclear

The proposed amendments will arguably permit some 'responsible persons' to intercept *all* emails entering a computer network prior to arriving at the mail server, even if only by way of implementing automatic scanning processes that create and test a temporary copy of the emails ('scanning'). This type of conduct may be 'reasonably necessary' to perform network protection duties. The Explanatory Memorandum provides more information concerning the meaning of 'protection', indicating that it includes not only the network infrastructure but also the protection of data stored and transmitted on the network:

> 'Such data may include sensitive government and business data held on the network, as well as any personal and financial data which individuals have supplied, for example in the course of their employment or in requesting or purchasing services' (Explanatory Memorandum, page 4)

Emails that are intercepted and identified as threatening the network – such as emails containing active content or with attachments indicating a security risk; or sent in such quantities as to threaten the operation, protection or maintenance of a computer network; or phishing attempts – may be dealt with as permitted by the proposed legislative provisions. Presumably, this would include using the information to stop further attacks by blocking sender email addresses, or deleting emails (there being no obligation to allow delivery).

However, emails that do not fall within the protection exemption may include emails identified as having nuisance value, rather than having implications for the operation, protection or maintenance of the network. This category includes emails typically referred to as spam, constituting unsolicited commercial or pornographic content. While such emails do not constitute a threat to the network, it is still regarded as undesirable to permit those emails to simply pass through to the intended recipient.

It is therefore common practice for network administrators to run applications that identify nuisance spam emails by automatically scanning, then blocking the emails – a use of the information that may arguably not be reasonably necessary to protect the network. Administrators may also use the information to quarantine suspect emails, by creating a copy on a server that is not immediately accessible to the intended recipient. The same application sends the intended recipient a message inviting the intended recipient to choose to receive or delete the email. The quarantining process is implemented because in some cases, these applications 'catch' legitimate emails.

I am concerned that the legality of screening and filtering nuisance emails, and quarantining suspected nuisance emails – that is not sufficiently serious to fall within the threat/inappropriate use classification – is not sufficiently clear under the proposed legislative provisions.

If it is intended that the legislation not permit this type of activity, then it would certainly be inconsistent with the practices of thousands of network administrators and operators of commercial spam filters. If it is intended to allow this type of activity, then the Bill requires amendment as the scope of network protection duties is insufficiently clear.

2. Standard practices concerning employee changes and absences appear to be unlawful

Many organisations provide individual employees with a personal email account, with a personal address, eg. *employeename@employername.com.au*. Employees receive work related emails at these addresses, but may also receive personal emails. Changes in the employee's circumstances may mean that the employee no longer has access to the email account, but third parties will continue to send work related emails to the address. It may be essential for the operation of the employer's business that those emails be read by current employees. Employers and employees typically make arrangements to allow this to happen. It is possible that some of these arrangements may contravene the TIA Act.

Some scenarios follow:

(a) **Leave**: An employee (A) goes on leave and provides a co-worker (B) with access to the employee's email account to deal with work-related emails during A's absence. While A is on leave, is an incoming email arriving at the mail server still regarded as 'accessible' to A, so that B can lawfully access the email? If, as seems possible, the answer is 'yes', could leave be of such duration as to lead to different conclusion, eg. maternity or long service leave?

(b) **Termination of employment (resignation, dismissal or retirement)**: An employee (A) resigns from an organisation. A agrees that (or standard work procedures of which A is aware provide that) a co-worker (B) may access A's email account for one month after A's resignation. It seems unlikely that emails arriving at the mail server for A's email account can still be regarded as 'accessible' by A. It is arguable that by opening a new email addressed to A, B will contravene the TIA Act. It is also arguable that if the employer even allows a copy of an email addressed to A to be created on its network, it may contravene the TIA Act. If so, all emails addressed to A would need to be blocked from the employer's network.

(c) **Change in address**: An employee (A) moves to another part of an organisation (eg. a different government department) and A's email address changes. Emails sent to A's old email address are not forwarded to A's new email address. Instead, as with the scenario in (b) above, A agrees that (or

standard work procedures provide that) a co-worker (B) may access A's email account for one month after A's transfer. Again, it seems unlikely that emails arriving at the mail server for A's email account can still be regarded as 'accessible'. The same implications arise as set out in paragraph (b).

These are common situations in which it is not clear whether contravention of the TIA Act may take place, even where employees provide consent or agree to employment terms permitting other employees to access their emails in their absence. Such access can be essential to the ongoing operation of a business. It is not always possible, in a practical or technical sense, to block emails sent to that address and send an automated response without a copy of the email being made somewhere, however briefly. An automated response may also be inadequate to ensure business continuity.

Dealing with these emails may be important for the *operation of the organisation* that relies on the network, but whether or not they are necessary for the *operation of the network* is not clear.

3. Common commercial practices involving redirection of emails for other purposes appear to be unlawful

There are circumstances in which a person (A) may wish to invite another person (B) to send an email to an address provided by A, where the address appears to be A's personal address, but is in fact controlled by a third party (C) with A's consent. B then sends an email to the address provided by A; A is therefore the intended recipient. Instead, the email goes to C's mail server, *which is not directly accessible by A*. C might, for example, forward the email to A, or use it in accordance with A's instructions.

The scenario as stated in the abstract sounds complex, but may not be uncommon. For example, the following was recently reported in *The Australian*:

> 'A PERTH reader recently received a letter from BT Financial Group about his superannuation, complete with this kind invitation at the end from BT Financial Group chief executive Rob Coombe: "Don't forget we're here to help. Call us on 132 135, or if you prefer, you can email me directly me at (Coombe's personal email address) - I'd love to hear from you."
>
> Reader X took up the offer, flagging his email before he hit Send. An electronic receipt for Reader X's email duly turned up and revealed his missive, complete with all his contact details and super account number, had been delivered into the server of marketing company Campaign Master (slogan: "We've mastered email marketing"). Reader X was, to say the very least, surprised. But faster than you can say "phishing expedition", BT's head of superannuation informed Reader X that BT has a standard agreement for a third party to intercept emails, had been doing so for years and nobody had noticed. Well, put that way, that's OK then.'
>
> ('Privacy? What's that?', *The Australian*, 23 July 2009, http://www.theaustralian.news.com.au/story/0,25197,25821377-25090,00.html)

There are insufficient facts to allow a full analysis of this situation under the TIA Act. However, this type of scenario certainly raises issues under the legislation which will not be resolved by the proposed amendments.

It might be argued that because A has agreed to C receiving and accessing the email and dealing with it in accordance with A's instructions, the email is 'under the control of' A as the intended recipient when received by C (as required by s 5H(1) of the TIA Act in order for an email to be accessible to the intended recipient). However, on that reasoning, an employee could also effectively consent to his or her employer receiving and accessing an email without the knowledge of the sender, and this does not appear to be the case under the TIA Act in its present form.

4. The legality of typical email quarantining practices is unclear under the definition of 'accessible'

The general prohibition on interception has been interpreted as meaning that, in the absence of statutory exceptions, a copy of an email can only be made once it has reached the email server and is therefore available to the intended recipient.

This is one interpretation of the current legislation as it applies to emails, but it does not seem to me that it is the only one. The meaning given to the term 'accessible' by s 5H of the TIA Act is not exhaustive, and the arrangements from network to network may differ:

> '(1) For the purposes of this Act, a communication is accessible to its intended recipient if it:
>
> (a) has been received by the telecommunications service provided to the intended recipient; or
> (b) is under the control of the intended recipient; or
> (c) has been delivered to the telecommunications service provided to the intended recipient.
>
> (2) Subsection (1) does not limit the circumstances in which a communication may be taken to be accessible to its intended recipient for the purposes of this Act.'

Some screening practices involve automated systems screening emails for content or spam and quarantining the email, while simultaneously notifying the intended recipient and providing him or her with an opportunity to release the email. In doing so, it could be argued that the intended recipient is afforded a degree of control over the email. It is not clear whether such practices are permissible under the legislation.

The definition of 'accessible' is generally unsatisfactory. For example, it potentially permits a network administrator to operate scanning systems and practices that check an email for any purpose after it has arrived at the intended recipient's email server, remove it prior to the intended recipient having an opportunity to access the email –

possibly in a matter of seconds – and use the information gained from the email for any purpose. The legislation does not make the legal status of such practices clear.

I regret that I have not had more time to prepare these submissions but thank you for the opportunity to comment on the proposed amendments.

Yours sincerely

[Name withheld on request]