Australian Government

Office of the Privacy Commissioner

Telecommunications (Interception and Access) Amendment Bill 2009 - Network Protection

Submission to the Senate Standing Committee on Legal and Constitutional Affairs

October 2009

Key Recommendations

1) The Office of the Privacy Commissioner (the Office) recognises the need for an appropriate balance between the public interest in computer network owners and operators being able to undertake legitimate activities aimed at detecting and responding to security risks and maintaining individual privacy.

2) The Office has a number of suggestions aimed at enhancing aspects of the *Telecommunications (Interception and Access) Amendment Bill 2009*. These are as follows:

   i. The Bill could provide additional guidance on the operation of the provisions to assist organisations to train authorised persons in respect of what action is lawfully permitted to be undertaken under the scheme.

   ii. Any exceptions permitting secondary uses or disclosures should be well defined. These exceptions should align with community expectations and be based on clearly articulated public policy reasons.

   iii. Section 63C could be strengthened to prohibit secondary uses or disclosures by: (a) persons engaged in network protection duties, (b) the responsible person and (c) their employer.

   iv. The Bill should clarify that 'disciplinary action' in clause 15, regarding misuse of the computer network, applies to activities that pose a risk to network security only.

   v. Information Privacy Principles 10 and 11 (regulating use and disclosure of personal information) in the *Privacy Act 1988* should continue to apply to the Australian Federal Police under clause 15 (s.63D(4)) of the Bill.

   vi. Consideration could be given to including in the Bill a provision to allow individuals access to intercepted communications, that relate to them, to be modelled on National Privacy Principle 6.1 in the Privacy Act.

   vii. The Office suggests that all intercepted records of a communication, whether the original or a copy, obtained for the purpose of network security should be destroyed when no longer needed for that purpose.

Office of the Privacy Commissioner

1) The Office of the Privacy Commissioner (the Office) is an independent statutory body whose purpose is to promote and protect privacy in Australia. The Office, established under the Privacy Act, has responsibilities for the protection of individuals' personal information that is handled by Australian and ACT Government agencies, and personal information held by all large private sector organisations, private health service providers and some small businesses.

2) The Office also has responsibilities under the Privacy Act in relation to credit reporting, and personal tax file numbers used by individuals and organisations. In addition, the Office has regulatory functions under other Acts, such as the *Telecommunications Act 1997* and the *Crimes Act 1914*.

Preliminary

3) The Office welcomes the opportunity to comment on the *Telecommunications (Interception and Access) Amendment Bill 2009* (the Bill).[1] This submission draws on comment that the Office made to the Attorney-General's Department on the earlier exposure draft of the Bill[2] and on previous submissions in relation to the *Telecommunications (Interception and Access) Act 1979* (the TIA Act).[3]

4) A primary objective of the TIA Act is to protect the privacy of individuals who use the Australian telecommunications system. It does so by making it an offence to intercept communications passing over the network. A secondary objective is to specify the circumstances in which it is lawful for interceptions to take place.

5) The Office notes there needs to be an appropriate balance between the public interest of computer network owners and operators being able to undertake legitimate activities aimed at detecting and responding to security risks and the public interest in protecting the personal information of individuals.

6) Research that the Office conducted in 2007 asked questions about privacy in the workplace. Among the issues surveyed, 43% of respondents considered that employers should be able to read employees' emails, *only if they suspect wrongdoing*. A further 30% believed that employers have no right to undertake these activities under any circumstance. [4]

---

[1] For information about the inquiry and the Bill: www.aph.gov.au/senate/committee/legcon_ctte/telecommunications/index.htm

[2] Exposure Draft of the Telecommunications (Interception and Access) Amendment Bill 2009 - Network Protection; Submission to the Attorney-General's Department (August 2009) http://128.121.81.229/materials/types/download/9386/6924

[3] See for example the Office's submission on Telecommunications (Interception and Access) Amendment Bill 2008; Submission to the Senate Legal and Constitutional Affairs Committee (April 2008), pp.5-6 at http://128.121.81.229/materials/types/submissions/view/6761

[4] Office of the Privacy Commissioner Survey results: *2007 Community attitudes towards privacy in Australia,* p. 53, Available on the Office's website www.privacy.gov.au/materials/types/download/8820/6616

7) The Explanatory Memorandum[5] (EM) to the Bill notes that activities undertaken for network protection purposes are critical to the efficient operation of network infrastructure and also to the protection of data stored and transmitted on the network. The EM states that some network protection activities that take place at the threshold of a computer network such as copying or recording of communications for quarantining, analysing, or filtering may constitute a technical breach of the TIA Act.

8) The Bill proposes that network protection measures be made lawful subject to certain conditions. 'Network protection duties' are defined in the Bill as relating to:

- the operation, protection or maintenance of the network; or
- if the network is operated by, or on behalf of, a designated Commonwealth agency[6], security authority or eligible authority of a state – ensuring that the network is 'appropriately used' by employees, office holders or contractors of the agency or authority. 'Appropriately used' is defined separately.

Exception to prohibition on interception

9) Clause 11 (s.7(2)(aaa)) proposes that the interception of a communication by a person is permitted if:

- the person is authorised in writing by the responsible person for a computer network to engage in network protection duties in relation to the network; and
- it is reasonably necessary for the person to intercept the communication in order to perform those duties effectively.

10) The Office suggests that the legislation could provide additional guidance on the operation of the provisions to assist organisations to train authorised persons about what actions are lawfully permitted to be undertaken under the scheme (including clause 11). For example, what measures are covered by 'the operation, protection or maintenance of the network' and when is an interception 'reasonably necessary'.

Dealing in information

11) An effective privacy regime regulates the use or disclosure of personal information collected for a specific purpose. The Office suggests that any exceptions permitting secondary uses or disclosures should be well

[5] Explanatory Memorandum available at http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r4196_ems_1cb5f906-2a2e-47de-a547-aee58b3d25da/upload_pdf/334184.pdf;fileType=application%2Fpdf

[6] 'Commonwealth agency' is limited to the Australian Federal Police (AFP), the Australian Commission for Law Enforcement Integrity (ACLEI) and the Australian Crime Commission (ACC)

defined. These exceptions should align with community expectations and be based on clearly articulated public policy reasons.

12) Clause 15 of the Bill establishes a framework for the use and disclosure of intercepted communications by authorised persons. Under this clause, a person engaged in computer network protection duties may, in performing those duties, use or disclose lawfully intercepted communications whether originating internally or externally. The lawfully intercepted communication may be disclosed to a 'responsible person' for the network or to another person if it is reasonably necessary to enable that latter person to perform network protection duties in relation to the network.

13) The responsible person for a network may communicate lawfully intercepted information to a designated agency if that person suspects, on reasonable grounds, that the information may be relevant in determining whether a prescribed offence has been committed.[7]

14) Except for a designated Commonwealth agency, a security authority or eligible authority of a state, there appears to be no restrictions on any secondary uses or disclosures of the intercepted information placed on: (a) a person engaged in network protection duties, or (b) on the responsible person, or (c) on their employer. The Office suggests that s.63C could be strengthened to prohibit secondary uses or disclosures by such persons and their employer.

15) In addition, if the network is operated by, or on behalf of, a designated Commonwealth agency, security authority or eligible authority of a state, clause 15 (s.63D)) permits the use and disclosure of lawfully intercepted communications by a person engaged in network protection duties for 'disciplinary action', in relation to a communication originating internally.

16) 'Disciplinary action' in relation to the misuse of the computer network is not defined in the Bill, however, Clause 9 (s.6AAA) states that an appropriate use of the computer network (within a designated Commonwealth agency, security authority or eligible authority of a state) will depend on:

- whether the user has accepted the terms of the network owner or operator's IT use policy in writing
- whether the conditions of that policy are reasonable, and
- whether the user complies with them.

17) The Office notes that IT policies often include conditions that are not related to computer network protection, although these conditions may be reasonable in the circumstances. For example, an IT policy may regulate individuals' use of the computer network for non-work related purposes, such as internet banking.

18) Under the proposal, it appears that it could be lawful for the network owner or operator to use and disclose an intercepted communication for disciplinary action even though that use of the network does not pose a network security risk. For this reason, it appears that the amendments may

[7] A prescribed offence is generally an offence punishable by a term of imprisonment for a maximum period of at least 3 years.

be potentially broader than needed to achieve the stated objectives of the proposal. Therefore, the Office suggests that the Bill should clarify that 'disciplinary action' in clause 15, regarding misuse of the computer network, applies to activities that pose a risk to network security only.

19) Clause 15 (63D(4)) applies to a designated Commonwealth agency, a security authority or eligible authority of a state. The clause prohibits the use and disclosure of intercepted communications for disciplinary purposes in relation to users of the network, if it were to contravene another law of the Commonwealth, state or territory.[8]

20) As the Office understands it, clause 15 is intended to preserve the operation of any workplace surveillance legislation provisions in federal, state or territory law. However, it is unclear if the Information Privacy Principles 10 and 11 (regulating use and disclosure of personal information) in the Privacy Act are intended to continue to apply to the AFP (as a designated Commonwealth agency[9]). The AFP is ordinarily subject to the IPPs in the Privacy Act and the Office suggests that this coverage continue to apply.

Access to intercepted communications

21) Access to one's own personal information is an essential component of an effective privacy framework. NPP 6.1 in the Privacy Act permits an individual to access information held about them by an organisation unless an exception applies. However, the small business operator exemption in s. 6D[10] of the Privacy Act and the employee records exemption in s. 7B(3)[11] of that Act may prevent affected individuals from accessing their intercepted communications under NPP 6.1, depending on the size and type of entity in which their information is held.

22) The Office submits that consideration be given to including in the Bill an access provision modelled on NPP 6.1. This provision should allow an affected person to access intercepted information relating to them. This could assist in achieving an appropriate balance between the competing public interest in maintaining computer network protection and individual privacy.

Destruction of records

23) The Bill amends the current requirements in s.79 TIA Act.[12] That section requires an interception agency to destroy a 'restricted record' if the chief officer of the agency is satisfied that the restricted record is not likely to be

[8] A similar provision in clause 20 is intended to apply to further uses and disclosures.
[9] The ACLEI and the ACC are not subject to the IPPs in the Privacy Act
[10] See Information Sheet 12 'Coverage of and Exemptions from the Private Sector Provisions', pp.1-2, 4-5 at www.privacy.gov.au/materials/types/download/8709/6544
[11] See Information Sheet 12 'Coverage of and Exemptions from the Private Sector Provisions', pp.3-4 at www.privacy.gov.au/materials/types/download/8709/6544
[12] Clause 14 (s.35(1A)) also amends the requirements that a state law must meet before the Minister can declare an eligible state authority to be an interception agency. These requirements relate to the security and destruction of a restricted record which are excepted

required for a permitted purpose. A restricted record is the record that has been intercepted and does not include a copy of that record.

24) Clause 21 to the Bill states that the requirements of s.79 do not apply to a communication that was intercepted for computer network protection by an interception agency. The EM states that this obligation would pose an onerous administrative burden on such agencies as the responsibility is placed on the chief officer of the agency rather than on an authorised officer (such as a 'responsible officer').

25) Accordingly, a new provision (s.79A) is introduced relating to the destruction of a restricted record as soon as practicable if it is not likely to be required for specified purposes. The provision applies generally to computer network protection (including interception agencies) and the obligation to destroy the restricted record is placed on the 'responsible officer'.

26) The Office suggests that all intercepted records of a communication, whether the original or a copy, obtained for the purpose of network protection should be destroyed when no longer needed for that purpose.

Review of TIA Act

27) The Office recommends that the operation of these amendments should be independently reviewed in five years from commencement.