Australian Government
Attorney-General's Department

Information and
Security Law Division

04/1990

19 March 2004

Senator Marise Payne
Chair
Senate Legal and Constitutional
Legislation Committee
Parliament House
CANBERRA ACT 2600

By E-mail legcon.sen@aph.gov.au

Dear Senator Payne

Telecommunications (Interception) Amendment Bill 2004

I refer to the Committee's inquiry in relation to the above Bill, to which the Attorney-General's Department lodged a written submission on 12 March 2004.

We have now had an opportunity to review the other written submissions lodged with the Committee. In light of the matters raised in those submissions, we have set out in the attached pages a number of additional comments that may assist the Committee in its deliberations. .

I trust that the attached information is of assistance to the Committee.

Yours sincerely

Keith C Holland
Assistant Secretary
Security Law Branch

Telephone: 6250 5430
Facsimile: 6250 5985
E-mail: keith.holland@ag.gov.au

Telecommunications (Interception) Amendment Bill 2004

Comments on Submissions to the Senate Legal and Constitutional Legislation Committee

Submission of Electronic Frontiers Australia

The submission lodged by Electronic Frontiers Australia indicates that it supports the amendments contained in the Bill, subject to confirmation that its understanding of the effect of the amendments, as outlined in the submission, is correct. Having reviewed the submission, we note that paragraph 4.2 contains an accurate summary of the policy rationale for and effect of the amendments.

Electronic Frontiers Australia is correct in its understanding, outlined at paragraph 4.3.1 of the written submission, that a telecommunications interception warrant will be required to access communications made using a voice over internet protocol (VoIP) service. While such services are expressly excluded from the definition of delayed access message service in proposed subsection 6(5), they remain subject to the protection conferred by the general prohibition against interception of telecommunications already provided in the Act.

In paragraph 4.3.2 of its written submission, Electronic Frontiers Australia indicates that there are two possible interpretations of the provisions of proposed paragraph 6(7)(a). The provision is intended, as set out in the Explanatory Memorandum, to make clear that access to a communication by the intended recipient does not amount to an interception for the purposes of the Act. A contrary interpretation would, as noted by Electronic Frontiers Australia, be inconsistent with both the intention of the amendments as outlined in the Explanatory Memorandum, and the underlying objects of the Act.

Electronic Frontiers Australia have recommended that additional amendments be included to expressly exclude from the definition of interception the act of copying communications data for backing-up or disaster recovery purposes. This issue is discussed at paragraphs 4.4.1-4.4.3 of the written submission. We consider that the inclusion of such a provision is unnecessary because the Act is directed at protecting the privacy of users of the Australian telecommunications system. It is not intended that the Act frustrate legitimate business use of telecommunications technology or IT systems in general. Automated backup for the purposes of business continuity does not impinge upon the Act's object of protecting the privacy of communications.

Submission of Privacy Victoria

The submission lodged by Privacy Victoria makes six recommendations in relation to the provisions of the Bill.

Firstly, Privacy Victoria recommends that the Bill expressly extend the general prohibition against interception to communications that are stored temporarily or at an intermediate stage in transmission. The existing prohibition against the interception of communications passing over a telecommunications system in subsection 7(1) of the Act makes it unnecessary for the amendments to be structured in this way. The Act already clearly extends general protection to all communications while in their passage over a telecommunications system. The amendments set out

clear provisions that clarify the circumstances in which certain communications have ceased their passage over the telecommunications system for the purposes of the Act. The amendments ensure that the general prohibition against interception will continue to apply to communication that have merely paused in their passage over the telecommunications system.

Secondly, Privacy Victoria recommends that the Bill further clarify the definition of delayed access message service. We consider that the definition in proposed subsection 6(5) is clear and unambiguous in application. The concern expressed by Privacy Victoria in relation to voice over internet protocol (VoIP) services is unfounded. As noted above, the Act already extends general protection to all communications passing over a telecommunications system. The exclusion of VoIP services from specific provisions addressing how that general protection applies to delayed access message services ensures that VoIP services are treated in the same way as, and receive the same level of protection already afforded to, standard voice telephony.

Thirdly, Privacy Victoria recommends that the Bill impose a general requirement for access to stored communications to be authorised under telecommunications interception warrants, and then set out exceptions to that general requirement. The privacy interests of users of the Australian telecommunications system are protected by the existing general prohibition against interception in subsection 7(1) of the Act. As noted above, the amendments simply make clear when those protections apply by making clear when specified communications cease their passage over the telecommunications system.

Fourthly, Privacy Victoria recommends that the Bill expressly limit to law enforcement agencies the power to access communications that are no longer passing over a telecommunications system. It is not necessary to include a provision of this kind because the amendments do not allow unregulated access to communications that are no longer passing over a telecommunications system. Where a telecommunications interception warrant is not required in order to access a particular communication, because that communication has ceased its passage over the telecommunications system, the person seeking access may nevertheless only access the communication in accordance with some other form of lawful authority, such as a search warrant.

Fifthly, Privacy Victoria recommends that the Bill provide for the intended recipient of a communication to be notified where access to the communication is sought with their apparent authority but without actual knowledge. It is not necessary for the amendments to include such a requirement - clear and unambiguous authority will be required in order to attract the operation of the provision. By conferring such authority the recipient will by necessary implication be aware of the communications that the authorised person may have access to.

Finally, Privacy Victoria recommends that the Bill provide for the parties to a stored communication to be notified of requests to access the communication, subject to judicial discretion to waive notification in certain circumstances. This recommendation is founded on the misconception that the amendments will allow unregulated access to communications that are not, or are no longer, passing over a telecommunications system. As noted above, even if a telecommunications interception warrant is not required in order to access a particular communication, the person seeking access may proceed only under appropriate lawful authority, such as a search warrant.

Submission of the Australian Federal Police

The Australian Federal Police notes in its submission concern that the amendments in the Bill will inhibit its ability to protect its IT systems from malicious or inappropriate content. We consider the AFP's concerns in this regard to be unfounded. At paragraph 32 of its submission, the AFP acknowledges that automatic reading of a communications by a computer, as performed by virus-detection or content filtering software, does not currently constitute an interception for the purposes of the Act. Amending the definition of interception to include reading and viewing a communication is not intended to change this. Rather, in line with the underlying objective of the Act to protect the privacy of telecommunications users, reading refers to the human act of reading, and apprehending the meaning of, written words, rather than electronic or mechanical scanning of data.

The AFP have also expressed concern that the amendments in the Bill conflict with section 3L of the *Crimes Act 1914*, which empowers the holder of a search warrant to operate computer equipment at the warrant premises to gain access to data stored remotely. The Department does not share the AFP's concerns in this regard, to the extent that the provisions in the *Crimes Act* do not override the specific protections conferred upon communications by the interception legislation.