Australian Privacy Foundation

post: GPO Box 1196
Sydney NSW 2001
phone: +61 2 9231 4949
facsimile: +61 2 9262 3553
email: mail@privacy.org.au
web: www.privacy.org.au

27 June 2004

Phillip Bailey
Acting Secretary
Senate Legal and Constitutional Committee
Parliament House
CANBERRA ACT 2600

Dear Mr Bailey

Telecommunications (Interception) Amendment (Stored Communications) Bill 2004

I attach a submission to the Committee's Inquiry into the above Bill.

The submission builds on concerns we have raised on the previous occasions that the government has attempted to make this radical change in interception policy, most recently in our submission to the Committee on the TI Amendment Bill 2004 dated 11 March.

We also copied to the Committee our letter to the Attorney-General dated 1 June 2004 concerning the current Bill when it was introduced.

Yours sincerely

Nigel Waters

Board Member and Policy Co-ordinator, APF

Australian Privacy Foundation

post: GPO Box 1196
Sydney NSW 2001
phone: +61 2 9231 4949
facsimile: +61 2 9262 3553
email: mail@privacy.org.au
web: www.privacy.org.au

Senate Legal and Constitutional Committee

Inquiry into the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004

Submission

Unacceptable intrusion into communications privacy through Telecommunications (Interception) Act changes

We are writing to express our serious concern about the proposed changes to the Telecommunications (Interception) Act 1979 concerning delayed access stored communications. In our view these changes would allow an unacceptable level of relatively unsupervised intrusion into the communications privacy of all Australians.

While other changes to the Interception Act regime over the last few years have been of serious concern they have not been as radical as those now proposed. This Bill would fundamentally overturn an essential principle – that the content of communications *before they are received* should only be accessible to authorities under the strict supervision of the Interception warrant regime.

Communications privacy is an essential foundation for a free and democratic society. Unless all Australians – including politicians and jouurnalists - can communicate on a presumption of confidentiality, there would be a devastatingly 'chilling' effect on free expression, on accountability, and on legitimate political discussion and organisation. That is in addition to the unacceptable potential for relatively unsupervised intrusion into individuals' private affairs.

The current position, which must be defended, is that individuals can communicate for the most part privately, secure in the knowledge that it is only in the most exceptional circumstances, where there is

reasonable suspicion of serious wrongdoing, established to the satisfaction of an independent quasi-judicial authority, that the content of a communication can be intercepted.

We make the point that the changes would not allow access to any *more* information than can be obtained under warrants – so any government suggestions that failure to pass the amendments would obstruct law enforcement should be rejected. These changes are all about dismantling important safeguards and accountability mechanisms, and as such can and should be resisted without having to concede that privacy comes at the price of law enforcement capability.

The Telecommunications (Interception) Amendment (Stored Communications) Bill 2004 effectively resuscitates changes that were proposed in 2002, and were comprehensively rejected, not least by your Committee. Subsequent provisions in the February 2004 Bill, while not perfect, at least attempted to confirm protection for delayed access messages, but were withdrawn following disagreements over interpretation between different government advisers. We are alarmed that the position represented in the February Bill has been abandoned so quickly, without any reasoned explanation.

Our position remains that the interception regime, with its strict safeguards involving high thresholds (investigation of major offences), warrants and relatively transparent reporting, must continue to apply to 'stored & forwarded' communications such as E-mails, SMS, pager messages and voice messagebanks, after they have been downloaded via a telecommunications line, at least until they have been opened and/or read by the intended recipient.

Under the proposed amendments, 'stored communications' resulting from a delayed access service would be accessible to law enforcement agencies through the much weaker provisions of the Telecommunications Act.

Assurances by the government that this access would still be subject to equivalent safeguards such as search warrants are misleading – the vast majority of 'stored communications' that law enforcement agencies would be interested in would be only be 'protected information' to the extent provided by Part 13 of the Telecommunications Act – access would at best require a certificate from a senior police officer, and in most cases simply a request to a telecommunications business from police (see section 282). The content of such 'stored communications', which could be every bit as sensitive as a voice phone call, would have no more protection than less sensitive, content free traffic data about the parties to, timing of and duration of a call.

We draw the committee's attention to the statistical evidence of relative use of the two means of access. While the number of interception warrants authorised per year is still in the hundreds[1], the number of disclosures to law enforcement agencies under Part 13 of the Telecommunications Act runs to at least 500,000[2].

The Telecommunications Act is itself ambiguous about the treatment of emails and other delayed access messages – certificates under s.282 (3),(4) and (5) cannot be used in relation to 'contents or

[1] Annual Reports on the operation of the Telecommunications (Interception) Act.

[2] Despite the record keeping and monitoring provisions (ss.304-309 of the TA 1997), there is wholly inadequate public reporting of the volume of disclosures, particularly in light of the Privacy Commissioner's finding in 2001-02 of significant failures to meet the record keeping requirements (Operation of the Privacy Act Annual Report 2001-02, p.81). We understand that the Privacy Commissioner has been unable to perform his monitoring role under s.309 of the TA for the last two years due to lack of resources. The 500,000 figure came to light in Parliamentary proceedings some years ago and there is no reason to think it has decreased.

substance of communications' but it has never been certain whether this prevents their use for some stored messages, or whether it would be unlawful for telecom businesses to give access to stored messages 'voluntarily' under s.282(1) or (2).

What is clear is that allowing access to the content of unread stored communications under the Telecommunications Act rather than the TI Act would result in a much wider range of government agencies being able to intercept and read them. The list of agencies authorised under the TI Act to seek warrants, while extensive, is at least limited to major law enforcement agencies and 'watchdogs'. Under the TA, a wide range of other agencies, including the ATO, Centrelink, Customs and Immigration, would gain direct access. While these agencies may sometimes be involved in major crime investigations, we believe that they should continue to have to collaborate with a police agency that has Interception Act warrant powers if they require access to content of stored communications.

More and more of the routine communications of Australians are through the convenient 'store & forward' technologies. We are all entitled to the same protection and safeguards as apply to 'old fashioned' voice communications.

There is no rational distinction between 'real time' and 'store & forward' communications that would justify the law enforcement agencies being allowed to reap a technological dividend, at the expense of the privacy of all Australians.

It is important to maintain the technological neutrality of existing protections requiring a warrant for interception by not discriminating against caching and other incidental transient storage techniques. We understand that other submissions will point to some major concerns about the perhaps unintended effects of the amendments. For instance, they may result in it no longer being an illegal interception for a person to download someone else's email, or dial into their voice mail box, without their knowledge or permission, or for telecommunications carriers and Internet Service Providers to intercept customers communications.

In bringing forward these amendments, the government has consistently failed to produce any signficant empirical evidence, or even well founded estimates, of the scale of the alleged 'problem'. Given the magnitude of the changes, it is reasonable to expect at least some evidence of significant investigations that have been handicapped by the requirement to obtain a warrant. Mere assertions that the changes are necessary should not be enough.

We note that the government has promised a further review of the Interception Act. We would welcome such a review, provided it was independent and had sufficiently wide terms of reference. The suggestion by the Attorney-General in his Second Reading speech that it would be carried out by his Department does not meet these criteria. Surely if there is to be a review in the near future, it is premature to rush into making significant changes to the regime in the meantime.

We urge the Committee to reject this (literally) unwarranted incursion into the legitimate and essential privacy of communications which underpin a free society.

For further contact about this submission, please contact

Nigel Waters
Board Member and Policy Co-ordinator, APF