Australian Privacy Foundation

post: GPO Box 1196
Sydney NSW 2001
email: mail@privacy.org.au
web: www.privacy.org.au

Computer Network Protection – Exposure Draft amendments to the Telecommunications (Interception and Access) Act 1979

Submission to the Commonwealth Attorney-General's Department

August 2009

The Australian Privacy Foundation

The Australian Privacy Foundation is the main non-governmental organisation dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians. Since 1987, the Foundation has led the defence of the right of individuals to control their personal information and to be free of excessive intrusions. The Foundation uses the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed. For further information about the Foundation and the Charter, see www.privacy.org.au

Introduction

As the Committee will be aware, the APF has taken a particular interest in the telecommunications interception legislation and has participated actively in debates about successive amendments over the last twenty years.

Unfortunately, other commitments on the time of our all-volunteer Board, together with the very short consultation period, mean that that we have not been able to analyse these proposed changes with our usual thoroughness. We are very disappointed that so little time has been allowed for consideration, given that the 'problem' - of network protection activity and its compliance with the interception law - has been identified for a long time.

We have however seen enough in the Discussion Paper and draft Bill to make us seriously alarmed, and this alarm is reinforced by our understanding of the concerns of other interested parties – particularly Electronic Frontiers Australia, who have a good understanding of the technical aspects of the issue.

Scheme fails to meet its own objectives

We welcome the acknowledgement in the Discussion paper that the current temporary exception for government agencies is too broad for general application, and that network protection needs of organizations should be balanced with the clear privacy protection objective of the Act. However, we submit that the proposed scheme does not deliver this result, for several reasons which we set out below.

We acknowledge that some 'network protection' activity is consistent with and supportive of the security principle in Privacy laws, and that an *appropriate* level of monitoring of network activity is often a relevant means of complying with those principles, and can help to protect individuals' privacy, guard against identity crime etc. However, the emphasis must be on the

word ‘appropriate’ and we submit that the proposed scheme does not strike the right balance.

Restriction to data and not speech is of limited comfort

We acknowledge that the proposed ‘network protection’ exception will not allow organizations to access real time speech (s.7(2)(a)) or to use speech reconstituted from voice over internet protocol (VOIP) communications for network protection purposes (s.63C(4)). While this limits the privacy intrusion potential of the exception, it leaves the growing proportion of total communications that are in ‘store and forward’ technologies such as emails, SMS and instant messaging open to the use of the exception. We also fail to see why there is not a straightforward prohibition on reconstituting VOIP speech, rather than the indirect prohibition on its use.

Scope and Application of the amendments are unclear

The concept of ‘responsible person’ in the draft Bill is defined as a ‘network operator’ (s.5(1)) but the application of the provisions in practice is uncertain. It is not clear to us whether the proposed ‘network protection’ exception applies only to an organisation’s own internal private network, or more broadly to external networks operated by telecommunications carriers and carriage service providers, including Internet Service Providers (ISPs). While the two illustrative scenarios in the Discussion Paper are of the former, we suspect the latter, in which case the adverse privacy implications of the proposals are much worse – privacy intrusions will be potentially much more widespread and pervasive. The exception would apply not just to communications of persons employed by and transacting directly with a network operator but also to communications between third parties where the network operator is merely an intermediary. Individuals would face the prospect of their communications being accessed not only by an ‘end user’ organisation but also by one or more intermediary service providers. We submit that the government needs to explain more clearly whether the exception applies to third party ‘intermediary’ network operators.

It would also appear that network operators would be able to access communications of individuals with whom they have no direct relationship, and therefore could not be covered by an ‘Acceptable Use Policy’ (AUP). This would include third party individuals making unsolicited contact with a network operator by email, SMS etc. Given that the entire scheme is based on parameters to be set by AUPs, this would appear to leave a gaping hole even in the imperfect protection offered. Unless network operators are able to access communications involving such third parties, it is difficult to see how they could effectively monitor communications of employees or customers with whom they do have an AUP, as it would be impossible for them to confine the access to ‘one side’ of communications with third party correspondents.

Amendments are a ‘blank cheque’

We believe that the proposed amendments would in effect give network operators a blank cheque to write ‘Acceptable Use Policies’ (AUPs) which are completely self-serving. They could allow network operators to intercept the content of communications for almost any purpose they chose – far removed from any objective criteria of security requirements or suspected criminality.

Because the terms ‘appropriately used’ (in proposed s.6AAA and in the definition of ‘network protection duties in s.5(1)) and ‘disciplinary purposes’ in proposed s.63C(3) are undefined, network operators are given a very broad discretion to write whatever ‘purposes’ they like into their AUPs, and to intercept communications for almost any purpose. We cannot see that the requirement for AUP conditions to be ‘reasonable’ (s.6AAA(b)), and for access to be ‘reasonably necessary’ in (s.7(2)(aaa)(ii)) as providing significant safeguards – left to the

discretion of the network operator and only challengeable in retrospect, these provisions are unlikely to deter organizations from drafting very wide and self-serving AUPs.

The Discusssion Paper admits (p.11) that the amendments are expressly designed to give network operators maximum flexibility to define 'appropriate use' and 'appropriate action' to suit their own circumstances, and implies that almost anything that an operator can get a user to sign up to will be acceptable. This flies in the face of the common reality of lengthy 'small print' terms and conditions, often in a 'click through' format and rarely read by users. We submit that placing the onus on consumers to protect themselves by reading and challenging conditions is wholly unrealistic and also directly contrary to the government's policy objectives in its separate proposed 'unfair contract terms' legislation. We seek an explanation from the government as to how that proposed consumer protection legislation would apply to AUPs for the purposes of the network protection exception in the TIA Act.

Routine monitoring rather than targeted investigations

Another objectionable feature of the proposed amendments is that they make no distinction between reactive investigation of suspected misuse (which can be justified) and pro-active or even routine and continuous monitoring of all communications, to detect *possible* misuse. This amounts to mass surveillance – both of employees and of other persons communicating with the or through the network operator.

Lack of proportionality

Even where a particular specific purpose can be seen as justifying some monitoring, it is completely unclear as to why the amendments need to give network operators the ability to intercept and examine the detailed 'contents and substance' of communications. In most cases, it should only be necessary for network operators to monitor 'traffic' – types and volumes of communications, in order to detect possible violations of legitimate AUPs. In some cases, this might lead on to more detailed investigations that would require examination of content, but this should often be done by the appropriate authorities such as the police, brought into an investigation at the point where criminality is suspected.

Another disproportionate aspect of the proposed amendments is the apparent lack of any limit on *which* employees would be able to exercise the right to intercept and examine the content of communications. To the extent that network protection activity is to be allowed, it should be strictly limited to small numbers of specifically designated employees, subject to strict confidentiality standards, audit trails and other safeguards against misuse.

Potential for inappropriate use by law enforcement agencies

The proposed 'network exception' exception creates the potential for 'short cuts' by law enforcement agencies, which would normally require a TIA Act warrant to access 'stored communications'. They could seek to avoid the administrative burden of this safeguard by working with network operators to get them to access communications under this exception and then disclose the information to them, as they would be permitted to do under proposed s.63D. This would be an unacceptable and inappropriate outcome which needs to be clearly prohibited in any amendments.

Relationship to workplace privacy regulation unclear

We submit that in relation to network operators monitoring of their own employees' communications, the government has not adequately addressed the relationship of the proposed amendments to workplace privacy laws. This is of particular concern given the recommendation of the ALRC, in its 2008 Report 108 *For Your Information,* that the exemption for 'employee records' from the *Privacy Act 1988* be removed, and that the Standing Committee

of Attorney's General has an ongoing project to develop uniform workplace privacy laws – which are already in place in NSW. Even if network protection activities are subject to privacy principles, the common 'required or authorized by or under law' exception to Use and Disclosure principles would mean that privacy law would provide no additional constraint on the purposes for which accessed information could be used. The government needs to explain this relationship in light of conflicting policy objectives.

For further contact on this submission please contact
Nigel Waters, Board Member
E-mail: Board5@privacy.org.au

Please note that postal correspondence takes some time due to re-direction – our preferred mode of communication is by email, which should be answered without undue delay.