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

Telecommunications (Interception and Access) Amendment Bill 2007

Submission to the Senate Legal and Constitutional Affairs Committee

July 2007

CONTENTS

The Australian Privacy Foundation

The Australian Privacy Foundation (APF) is the leading non-governmental organisation dedicated to protecting the privacy rights of Australians. We aim to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians.

Since 1987 the Australian Privacy Foundation has led the defence of the rights of individuals to control their personal information and to be free of excessive intrusions. We use the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed.

For further information about the Foundation, see www.privacy.org.au

Introduction

We welcome the opportunity to make a submission on this important legislation. The Foundation has made submissions on most of the privacy related amendments to telecommunications legislation over the last decade, and notes that the history has been one of progressive weakening of controls and increasing powers of access – in our view disproportionately to any increased threat or risk.

The Committee may be aware that the Foundation made an extensive submission in February 2007 to the Attorney-General's Department (AGD) on the Exposure Draft Bill. We are very disappointed to see that few of our concerns have been addressed. This submission therefore covers much the same ground, and contains many of the same criticisms, as our earlier submission. However, we also note that the new Bill raises further concerns, which are also highlighted below.

We believe that the government is misleading the community by asserting that there are no major privacy implications arising out of the proposed legislation. The Minister claims in his second reading speech that "It is important to stress that this proposal does not represent new powers for security and law enforcement agencies. Rather it creates new, more systematic and appropriate controls over the existing access framework." The first sentence is simply not true, and is even contradicted by the Explanatory Memorandum (EM) which acknowledges, for instance, that the new 'prospective' information access powers have 'higher' privacy implications and impact (pp 7 & 9).

The Bill clearly increases the access powers of enforcement agencies and reduces the level of privacy protection.

Given the complexity of the Bill, and our reliance entirely on volunteers, we are grateful to Electronic Frontiers Australia for sharing with us their analysis of the Bill, and make reference to their submission where appropriate. It is very disappointing that no independent analysis of the Bill in the form of a Bills Digest from the Parliamentary Library is available as at the date that submissions to the Committee are required.

General Comments

In this submission, we refer to the *Telecommunications Interception and Access Act 1979* as the TIAA, and the *Telecommunications Act 1997* as the TA.

We note at the outset that the Bill contains some provisions that are contrary to recommendations of the Blunn Report, and contrary to the recommendations of this Committee in its report on the Telecommunications (Interception) Amendment Bill 2006.

While there is a superficial attraction in bringing the 'assistance to enforcement agency' provisions together in one Act, there are also serious disadvantages.

Firstly, removal of the exceptions for ASIO and enforcement agencies from the TA leaves Part 13 as incomplete and potentially misleading in terms of the privacy protection it offers. The replacement wording – mere references to Divisions 3 to 5 of Part 4-1 of the TIAA – will mean nothing to readers of the relevant TA sections. We submit that as far as possible the practical effect of legislation should be apparent from a 'plain reading' of provisions. The proposed changes will have the effect of reducing the transparency of the protection/access regime. Only experts who follow the trail to the TIAA will understand the overall effect. On the face of the TA,

it will appear that there are no exceptions for law enforcement or national security. We submit that it should be possible to leave in the TA Part 13 the express references to ASIO and enforcement agencies, for transparency, even if the details of their access is dealt with in the TIAA.

Secondly, the removal of the provisions relating to access by ASIO and enforcement agencies from the TA to the TIAA blurs the significant distinction that has existed until now between interception legislation, which applies stricter controls to access to more sensitive information, and the 'standard' telecommunications legislation, which controls access to other information including customer details and traffic data. By amending the TIAA to cover access by enforcement agencies to all personal information held by carriers and CSPs, we believe there is a risk that, over time, the distinction will be further blurred and the careful balance which has been established between the public interests in privacy protection on the one hand and enforcement interests on the other will be upset. We appreciate that a more optimistic view would reverse this argument in the belief that the higher standards applying to interception will 'rub-off' on the other access provisions. However, experience suggests that this would be naïve and any influence is likely to be in the other direction over time.

Thirdly, to the extent that the unsatisfactory overlap between the *Privacy Act 1988* and Part 13 of the TA is being addressed by the ALRC in its current Review of Privacy, we believe it is premature to transfer these provisions. The ALRC canvassed the issues in its October 2006 Issues Paper 31, and will be issuing a Discussion Paper in September 2007 which will contain draft proposals in relation to Telecommunications privacy, and the ALRC's final report is due by mid 2008. We can see no evidence of any urgent need for amendments which would justify not waiting for the ALRC's recommendations.

Fourthly, locating the provisions relating to access by enforcement agencies in the TIAA rather than the TA will make it more difficult to rationalise the overlap between these provisions and the Privacy Act. We believe that it is important to keep the 'default' access regime for customer details and traffic data as far as possible consistent with the obligations on other private sector businesses. We reject any presumption that individuals are entitled to less protection of information about their telecommunications transactions than about other transactions. The fact that telecommunications data is undoubtedly of great potential value to enforcement agencies does not in itself justify a more permissive access regime – we would argue the reverse – it demands tighter controls, not only over 'substance and content' but also over 'traffic data' – see below for our concerns about the unclear boundaries of these concepts.

Specific Comments

This section of our submission identifies and briefly comments on the most serious problems which APF has identified with the Bill.

Access to content and substance

While we welcome the clarification in proposed TIAA section 172 that proposed TIAA Part 4-1, Divisions 3 to 5 do not allow disclose of the 'content and substance' of communications, we remain very concerned that the 'loophole' of the existing TA s.280 appears to have been confirmed in proposed amendments to TA s.313. This section would expressly mandate carriers and CSPs to provide assistance to government agencies that included disclosure of information in accordance with TA s.280 (proposed s.313(7)(e)). Without amendment of TA s.280, this would potentially mandate the disclosure of content and substance, as an alternative to the more controlled access regime in the TIAA. Like the EFA, we refer the committee to its previous recommendation, and support the amendment to s.280 proposed by EFA.

We are very disappointed that such a fundamental revision of the relevant provisions has missed the opportunity to more clearly define what is meant by key terms such as 'telecommunications data' and 'content or substance'. This creates unacceptable ambiguity and uncertainty about the 'reach' of the various powers and protections. It also leaves open the possibility that very sensitive information such as mobile phone location data, email message headers and various internet logs would not be considered 'substance or content' or stored 'communications', and would therefore be subject not to the TIAA warrant controls but to the much weaker protection applying to 'authorisations' under the proposed TIAA Part 4-1 (see below). We submit that a much clearer legislative distinction between 'traffic data' and 'substance and content' is required. For example, while we welcome the statement in the EM that subject lines of emails are not 'telecommunications data', this needs to be confirmed in the legislation itself.

Access to other telecommunications data

The express provision for voluntary disclosure in proposed TIAA sections 174, 177 and 181 is a direct equivalent to the existing TA subsections 282(1) & (2), and also which effect restates exception (h) in NPP 2.1 of the Privacy Act, which applies to most large private sector businesses. We note that Blunn identified inconsistency between the two 'parts' of s.282 and recommended clarification of both objectives and processes (Blunn 1.7.5 & 1.7.6).

We welcome the addition of sub-sections to the voluntary disclosure provisions (s.174(2) and s.177(3)) stating that they do not apply to info that has been requested by an agency. This addresses concerns that we raised on the Exposure draft that these provisions could be abused by enforcement agencies putting pressure on carriers and CSPs to disclose information without the formalities that attach to 'authorisations' under the other provisions of Parts 4-1. But this change does not deal with all of the issues of consistency and clarity in relation to sections 174 & 177.

Historical vs Prospective information

The Bill establishes a new distinction between historical information (being information held at the time of an authorisation) and prospective data (being information that comes into existence during the life of an authorisation). There is no current provision in the TA for access to 'prospective' information, and this is a major new power.

ASIO and Criminal law-enforcement agencies directly (and civil penalty-enforcement or revenue protection agencies, indirectly via a Criminal l-e agency) will be able to gain access to prospective data by means of a certification process. While this process has more safeguards that the authorisation process for existing information, it is still far too loose a control over what amounts to a continuing surveillance authority. Prospective information could include, for instance, real time mobile phone location information – and this has been confirmed by amendments to the TA Part 13 in the *Communications Legislation Amendment (Content Services) Act 2007* (passed in June 2007)
(TA s.275A)

Mobile phone location information would normally be subject to the provisions of the *Surveillance Devices Act 2004*, which require a warrant for access. This Bill appears to have the effect of substituting the much weaker 'certification' regime of the TIAA for the warrant regime for a significant category of 'tracking device' (and perhaps also some 'data surveillance devices'). We submit that the government should be required to justify this significant weakening of the protection offered by the *Surveillance Devices Act*.

The EM gives contradictory indications (pp 6 & 8) as to whether information about 'websites visited' would be accessible under the weaker 'authorisation' provisions of Part 4-1 or would be regarded as 'content and substance'. Given the extreme sensitivity of web browsing information (it has rightly been described as revealing a user's thought processes) and the consequences for other rights and freedoms, it is essential that the application of the amendments to this information is more clearly articulated.

We refer to the detailed submissions of EFA on the 'prospective information' provisions, and share their concerns.

Purposes of access

The Exposure draft Bill provided for three categories of enforcement agency with limits on the purposes for which each type of agency could access telecommunications information. This Bill replaces this useful distinction with omnibus provisions applicable to all types of 'enforcement agencies', such that officers of one type could authorise access for the purposes of another type of agency.

Furthermore, there appear to be fewer controls (than in the Exposure draft) on the secondary use of information initially obtained for an authorised purpose.

Common issues concerning the process of authorising access to data

The new provisions appear to weaken the requirement for a conforming certificate, requiring instead only a written request stating that the authorising officer is 'satisfied'. Provision is made for the issue by the Communications Access Co-ordinator of further requirements in a legislative instrument (s.183), but this is too

important a safeguard to be left to discretion of an official who will not have any guaranteed independence (by default, it will be the Secretary of the Attorney General's Department).

The existing ACMA determination which specifies requirements for certificates will lapse under the new regime. We note that Blunn recommended no change in the requirement for a conforming certificate (Blunn 1.7.2) We therefore submit that the issue of further requirements for the form and conditions of 'authorisations' be made mandatory, and by one of the independent authorities (either the Privacy Commissioner or ACMA, retaining the requirement for consultation with the other).

The Bill appears to remove the requirement both for formal certification (of the need for access) and for documentary evidence of 'authorisation' to be provided to carriage service providers.

We fear that the new definition of 'authorised officer' will have the effect of reducing the level of seniority of those able to issue notification of 'authorisations'. Under the existing TA, authorisations under s.282 can only be given by 'senior officers'. Proposed TIAA s.5AB appears to allow agency heads to delegate to officers of any rank or seniority. Furthermore, it appears to be the intention that notifications may sent by "a relevant staff member" which means any staff member of any agency.

The Exposure draft Bill provided for a higher level of authorisation for access to prospective information, with a role for 'Certifying officers'. This concept has been dropped from the Bill, leaving authorisation for prospective information at the same level of 'authorised officers' as applies to access to historical information.

In relation to ASIO access authorisations are by 'eligible officers' and we seek confirmation that there is no change in the level of seniority required.

Overall, the weakening of the safeguards surrounding authorisation for access not only reduces accountability, but also create a serious risk of security breaches – of inadvertent and unlawful disclosure by carriage service providers in response to emails that are not in fact sent by a person authorised to do so.

Agencies allowed access

Addition of more agencies is a typical form of 'function creep'. EFA has noted that the definitions of a civil penalty-enforcement agency and a public revenue agency have changed, but that it is not clear if this will have the effect of giving a wider range of agencies access to telecommunications data. We urge the Committee to seek clarification of this, and if that is the effect, to seek specific justification.

We question the justification for Crimtrac to be included in the definition of criminal law enforcement body in proposed TIAA ss.5(1). The common public understanding is that Crimtrac is a 'service' agency providing databases for a number of enforcement agencies – it is not clear what if any 'investigatory' functions it performs which could justify the need for it to have access powers under the TIAA. Clearly Crimtrac databases will include telecommunications data, but all of this should arrive via other user agencies.

Secondary offences

We note that proposed TIAA s182 is significantly weaker than s.298 of the TA which it replaces. We endorse EFA's detailed comments on these provisions.

Application of the Act to Commonwealth agencies and Security authorities

We note the proposed amendment to TIAA s.5F(2) and s.5G and understand that this is to extend the protection for 'internal network monitoring' from the AFP, to other agencies with interception powers. We submit that it is most unhelpful to use the familiar term 'Commonwealth agencies' in a context that only applies to a very narrow sub-set. It gives the impression on a 'plain reading' that the protection applies to *all* Commonwealth agencies. This is an example of a disturbing trend in legislation to use terms to mean something other than what a lay reader would understand.

Interception capability etc

The proposed TIAA Chapter 5 appears to replicate and replace the current provisions in Part 15 of the TA. We have not analysed the new Chapter in detail for any differences, and reserve our opinion on any changes.

We share EFA's concerns about the imprecision of the term 'security authorities' in relation to the development and testing of interception capabilities (Part 2-4) and internal network monitoring (ss.5F(2) and 5G), particularly the replacement of the familiar term 'national security' with 'security' alone in the definition of 'security authority' in s.5(1).

Reporting

Agencies issuing authorisations will be required to report aggregate details annually to the Minister (s.186). We welcome the requirement for the Minister to table annual disclosure reports including each agency's figures in Parliament, but note that the agency reports, and consequently the Minister's report do not include details of secondary disclosures. Given that the secondary disclosure/use provisions of the Bill are significantly more permissive than the existing provisions of the TA, we submit that the reporting requirement should include secondary use and disclosures, and should require separate reporting of 'historical' and 'prospective' information access. This level of detail should in our view be included in the Minister's public annual report to Parliament, but at the very least should be made available to independent authorities such as ACMA, the Privacy Commissioner or the Ombudsman.

For the same reason, we submit that the annual reports by carriers, CSPs etc to ACMA under s.308, and any report by the Privacy Commissioner to the Minister on his/her monitoring under s.309, should be required to be made public. ACMA has chosen to publish some valuable figures (Appendix 6.1 of the Communications Report 2005-2006) and the Office of the Privacy Commissioner has inconsistently made some reference to the monitoring function in some Annual Reports. We submit that it is not satisfactory to rely on the discretion of these agencies.

Conclusions

This Bill does far more than just bring together existing provisions from the TA and the TIAA. It significantly changes the nature, and balance between, the powers and protections relating to access to telecommunications personal information. In so doing it ignores key recommendations of the Blunn Review, and of the Senate Committee in previous reports.

While the Bill has some positive features, there are many negatives, and it should not proceed in its current form. We strongly submit that the Bill be withdrawn pending further development of a consistent and considered policy, and further consultations, taking into account the recommendations of the ALRC in its final report of its current Privacy Review, due next year.

If the Bill does proceed, the Australian Privacy Foundation supports the specific amendments proposed by EFA, together with the other changes suggested in this submission.