Australian Privacy Foundation

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

Exposure Draft *Telecommunications*

(Interception and Access) Bill 2007

Submission to the Attorney-General's Department

February 2007

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 draft legislation. However, we note that due to an apparent oversight, we were not informed of the very limited consultation period at the same time as other stakeholders (on 2 February) and only became aware of it on 10 February. We welcome the week's extension granted for a submission but note that even so we are placed at a disadvantage relative to other interested parties.

The Department is well aware of our interest, and that of other NGOs including EFA, in this area of policy, and we have been significant participants in Telecommunications Interception policy development - including in the Blunn Review, to which this legislation is, at least partly, a response.

Expecting considered responses to draft legislation in only two weeks stands in stark contrast to the thorough reviews and inquiries which we have come to expect in the highly sensitive area of telecommunications interception. Analysis of the draft Bill is also hindered by the absence of any explanatory material such as a draft Explanatory Memorandum. Given that the Bill brings together provisions from two existing Acts, the only way to detect and assess the significance of any changes is in effect a line-by-line comparison. We do not believe that each interested party should have to do this – it is very time-consuming and easy to miss differences. We submit that the government has a responsibility to identify and explain proposes changes when seeking community input.

The Department's approach to consultation may have been affected by the view that "We do not anticipate any major privacy implications arising out of the proposed legislation." (email to us 12 February). With respect, that is for others to judge, and as you will see from our submission we disagree and believe there are some major implications. While the intention of the drafters may have been to strengthen the protection of telecommunications data, we believe that the Bill may have the reverse effect of increasing the access powers of enforcement agencies and in practice reducing the level of protection.

We note that the Telecommunications interception and surveillance page of the Department's website, and even the 'review' page within it (see http://www.ag.gov.au/www/agd/agd.nsf/Page/Telecommunications_interception_and_surveillance) do not mention the draft legislation. This seems a serious oversight – any interested party monitoring your

website specifically for developments in interception policy would be unaware of the draft legislation and consultation. The Bill can be found under 'Publications' but no-one would know to look there unless prompted.

General Comments

Given the extremely limited time available, and our reliance entirely on volunteers, we are grateful to Electronic Frontiers Australia for sharing with us their analysis of the draft Bill, and make reference to their submission where appropriate.

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

While there are some advantages 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 <u>all</u> 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. 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. 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 ss. 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 (and to the unconstrained discretion to make voluntary disclosures (see next paragraph). We submit that a much clearer legislative distinction between 'traffic data' and 'substance and content' is required.

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 and also 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 submit that this residual discretion can too easily 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 Part 4-1. The Bill should make it very clear that voluntary disclosure provisions are designed to allow occasional and exceptional disclosures. If this is primarily in circumstances where carriers and CSPs themselves become aware of unlawful conduct, then a version of NPP 2.1(f) might be more appropriate. Enforcement agencies pro-actively seeking information to assist in investigations should use the 'authorisation' provisions and should not be permitted to suggest voluntary disclosure as an alternative. Doing so should arguably be made an offence as it is contrary to the clear intention of the legislation.

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. Such information would normally be subject to the provisions of the *Surveillance Devices Act 2004*, which require a warrant for access. We fear that this Bill will 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 clearly explain the effect of this Bill on the coverage of the *Surveillance Devices Act*.

We refer to the comments of EFA on the prospective information provisions. We note EFA's concern that the technical feasibility and practicality of these provisions appear not to have been given sufficient attention. We also share EFA's concern that these provisions raise similar issues as were raised by the

stored communication warrant regime, and our initial view is that access to prospective information, if it can be justified, should be subject to at least the same safeguards as 'stored communications'.

Common issues concerning authorisations for 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, 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).

We fear that the new definition of 'authorised officer' will have the effect of reducing the level of seniority of those able to issue '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. Certifying officers, for the purposes of access to prospective information, still have to be 'senior' officers as defined in TIAA s.5(1), and we submit that there is no justification for a lesser standard to apply to access to existing 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.

Agencies issuing authorisations will be required to report aggregate details annnually to the Communications Access Co-ordinator (proposed TIAA section @189). While we welcome this additional accountability measure, which should also deter misuse, its effectiveness is severely limited by t lack of independence of the Co-ordinator, about which we have already commented above. Also, there appears to be no requirement for these reports to be made public or even made available to independent authorities such as ACMA, the Privacy Commissioner or the Ombudsman. We submit that it is essential for accountability that these reports be made public.

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.

The proposed replacement TA section 305, and new section 306A, use the term 'number-database operator' which does not appear to be defined anywhere, although it appears in existing s.308. The meaning of this term should be clarified.

Agencies allowed access

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?

Without a line by line comparison it is difficult to know if any other agencies have been added. We seek an assurance that they have not, or if there are any other changes, a justification that we can assess.

Secondary offences

We note that s184(1) does not appear to apply to information disclosed to ASIO (under Division 3), although the 'exception' for such disclosures in proposed section @184(2) implies otherwise. This should be clarified.

Section 184(2) also appears to widen the permitted secondary uses by criminal law-enforcement agencies, including allowing the use of 'prospective information' without the 3-year imprisonment threshold that applies to its original collection.

Application of the Act to Commonwealth agencies and Security authorities

We note the proposed amendment to 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 term 'Commonwealth agencies' but then define this as only 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 had time to analyse the new Chapter for any differences, and reserve our opinion on any changes.

We have not had time to analyse the new TIAA Part 2-4 relating to the development and testing of interception capabilities, but support the comments made by EFA.

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.

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