Australian Privacy Foundation

Privacy Amendment (Enhancing Privacy Protection) Bill 2012

Supplementary Submission to the House of Representatives Standing Committee on Social Policy and Legal Affairs

August 2012

email: mail@privacy.org.au

website : www.privacy.org.au

Please note that APF does not have a single postal address – we prefer communication by e-mail. If a postal address is required please contact the signatory.

Publication of submissions

We note that we have no objection to the publication of this submission in full. To further the public interest in transparency of public policy processes, APF strongly supports the position that all submissions to public inquiries and reviews should be publicly available, except to the extent that a submitter has reasonable grounds for confidentiality for all, or preferably only a limited part of, a submission.

Supplementary submission

We re-iterate our overall conclusion that the Bill has major weaknesses and would if enacted diminish privacy protection in some important respects. The Bill should preferably be withdrawn for more work, or substantially amended, in the ways we have suggested in our main submission.

We note that as well as generally inquiring into the Bill, the Committee was specifically requested to consider four specific issues:

REASONS FOR REFERRAL/PRINCIPAL ISSUES FOR CONSIDERATION: Consideration of: (a) the adequacy of the proposed Australian Privacy Principles; (b) the efficacy of the proposed measures relating to credit reporting; (c) whether defences to contraventions should extend to inadvertent disclosures where systems incorporate appropriate protections; and (d) whether provisions relating to use of depersonalised data are appropriate

Our specific response to these issues is as follows:

(a) the adequacy of the proposed Australian Privacy Principles;

We do not consider the proposed APPs to be an adequate replacement for the current IPPs and NPPs – see the Section 2 of our main submission for our detailed criticism

(b) the efficacy of the proposed measures relating to credit reporting;

We have some major outstanding concerns about the new credit reporting regime, including its unnecessary and unhelpful complexity – see Section 3 of our main submission.

(c) whether defences to contraventions should extend to inadvertent disclosures where systems incorporate appropriate protections;

The APF opposes any new defence, and considers that the issue should be dealt with, as it currently is, by means of the 'security' and 'use and disclosure' principles. The way the APPs (and the existing IPPs and NPPs) address this issue is through these principles. The security principles require agencies and organisations (entities in the revised scheme) to "take such steps as are reasonable in the circumstances to protect the information ...." (APP11 – IPP 4 & NPP 4 have the same effect). It follows that the **security** principle will not be breached by *any* type of disclosure (whether inadvertent or not) where reasonable steps were taken.

However, the **use and disclosure principle** is a separate obligation, and it is quite possible for a disclosure to contravene this principle notwithstanding that there is no breach of the security principle. An example would be where an employee makes an unauthorised disclosure whilst acting in good faith in the course of their duties – this might result from inadequate training or specification of their duties in relation to personal information. In such a circumstance, the entity should accept liability for a breach of the use and disclosure principle. This would contrast with either a malicious disclosure by an employee (knowingly unauthorised) or an external 'hacking' incident, where the entity should not be held liable under the use and disclosure principle – the disclosure would not in either of these cases be 'by the entity'.

We believe that the construction of the proposed amendments would not change this situation. We submit that the Committee should seek assurances from the government that it is neither the intention, nor the effect, of the amendments to remove the possibility of an entity contravening the use and disclosure principle without it having also contravened the security principle.

(d) whether provisions relating to use of depersonalised data are appropriate

There are several parts of the Act that address the issue of de-personalisation or de-identification.

The 'retention and disposal' part of the security principle (APP11.2) requires entities, in specified circumstances, to 'take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified'. (The Credit reporting regime has similar requirements (Clauses 21V and 21S)). Similarly, various exceptions in the APPs reference the concept of de-identification as a safeguard (Clause 16B(2)(b), APP 4.3 and APP 6.4(b)).

A new definition of 'de-identified' would be inserted by the Bill:

> ***de-identified***: personal information is ***de-identified*** if the information is no longer about an identifiable individual or an 7 individual who is reasonably identifiable.

This attempts to deal with the longstanding, but increasingly contentious issue of whether, and if so when and how, de-identification of information that related to individuals can ever be 100% guaranteed. Technological advances continually challenge the assurances given that particular de-identification techniques cannot be 'reverse engineered' and create new opportunities for relating ostensibly de-identified data back to individuals (with varying degrees of reliability).

Re-identification technologies and options are increasing at a massive rate and costs and barriers falling away in many areas, with at least the following three trends:

> (i) growth of online behavioural targeting, for both commercial and governmental purposes;
>
> (ii) increased data logging and retention (including in response to legal requirements, with a major extension being canvassed in the government's current proposals for national security legislation), and
>
> (iii) increased cooperation of technology vendors in building in capabilities to lower the cost and complexity of surveilling known targets, without discussing or even raising it with affected end users.

Policy makers need to look forward to the future when this re-identification functionality is pervasive, often as a backdoor feature of many infrastructure or operation tools, or greatly facilitated by those tools. Government's analysis of this challenge has lagged behind, assuming that practicalities and cost continue to create a severe barrier, which is no longer the case in many areas.

A wide range of interests, including law enforcement, national security, IT security, the psychographic marketing industry and global litigants are seeking access to re-identification functionality, and this will often be in direct conflict with expectations of privacy, confidentiality, and personal information security. These interests must not be allowed to exclude themselves from effective privacy regulation by arguing a spurious case that a 'de-identification' or 'de-personalisation' permanently removes any need for regulation.

In some scenarios, reasonable steps to de-identify personal information would be sufficient to guard against most 'risks'. The fact that re-identification might be theoretically possible, given enough effort, has in the past been considered insufficient grounds to try to regulate de-identified data. The Privacy Foundation considers that while this remains true in many circumstances, special consideration may need to be given to some types of personal information in some applications, and that express safeguards are needed to address successful re-identification of previously de-identified information.

We note that the best privacy protection is achieved by not collecting personal information in the first place, and in this respect we draw attention to our comments in

Section 2 of our main submission on the weakness in the revised 'anonymity' principle (APP 2).

A related issue is the definition of 'personal information' in the first place. We have commented on the weakness of the current and proposed definitions and need for future re-consideration, in our man submission (page 9).

De-identified credit reporting information

In the proposed new credit reporting regime (Part IIIA) there is a specific provision dealing with de-identified credit reporting information (clause 20M) which includes provision for the Information Commissioner to make rules for the research use of such information. The EM explains this as being necessary to allow for such research use, since the way the amended Act would otherwise work would be to prohibit such use. This seems a clumsy way of achieving this desirable and generally uncontentious outcome – we question why it has not been possible to draft Schedule 2 (the new Part IIIA) in such as way as to not limit the use of permanently and irrevocably de-identified credit information in the first place. As we have noted above, the Act should of course generically address the risk of 're-identification', particularly in light of increased technological capabilities.

For further information please contact:

Graham Greenleaf [redacted] or

Nigel Waters [redacted]

Board Members
Australian Privacy Foundation

APF Web site: http://www.privacy.org.au

Please note that APF's preferred mode of communication is by email, which should be answered without undue delay. APF does not have an organisational postal address. If postal communication is necessary, please contact the person named above to arrange for a postal address.