Australian Privacy Foundation

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

Personal Property Securities Bill 2008 Consultation Draft

Submission to the Commonwealth Attorney-General's Department

August 2008

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.

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.

General comments

The proposed new Personal Property Securities (PPS) regime appears to have been developed from a wholly business-centred perspective – it seems to be all about oiling the wheels of commerce. There is presumably an underlying assumption that whatever is good for business efficiency is automatically and necessarily in the interests of consumers, but we strongly dispute this.

The bias was illustrated by the agenda for the briefing seminars held in May – the one in Sydney we attended had eight separate external speakers all addressing business or commercial law aspects of the proposals. There was no speaker from a consumer perspective and no-one to even acknowledge that there may be important consumer interests that diverge from those of the business and legal communities.

The Commentary on the draft Bill does not clearly explain the 'reach' of the proposals, particularly in terms of the monetary threshold – para 2.11 (re Clause 83) talk of an interest value threshold of $5,000 but it is not clear if this translates into an asset value threshold or if this means that interest/asset values below this threshold would not be included in the Register. The Bill provides for registration of *all* security interests in personal property (10.3) and Clause 21 defining security interest does not contain any value threshold. This is not only unclear but also inconsistent.

In the absence of any figures on how many individuals are likely to have details included in the new Register, we have had to assume that it will be very large with a substantial proportion of all consumers included.

Failure to address privacy issues

The Commentary fails to address most of the concerns raised by the APF in its February 2007 submission on the Discussion Paper. Privacy is acknowledged as an issue but is supposedly taken care of by a proposal to make unauthorised access to the PPS Register an 'interference with privacy' under the Privacy Act, with the normal Privacy Act right of complaint (2.39). This supposed safeguard is undermined by the fact that the vast majority of small businesses and individuals who might access the

register are **exempt** from the Privacy Act.

The inadequate consideration of privacy issues highlights the need for a full Privacy Impact Assessment (PIA) as recommended by the Privacy Commissioner for privacy significant projects. While a PIA should have been conducted at a much earlier stage in the PPS project, it is not too late and is essential for properly informed debate about the draft legislation.

Privacy concerns need to be addressed in the design of the scheme, and in particular in the nature and role of the PPS Register. The proposed PPS Register has distinct similarities to the credit reference databases that are heavily regulated, for good reasons most recently outlined by the ALRC in the course of its review of Privacy law (the ALRC's final report is due for release on 11 August). The PPS Register will potentially be used either in place of or as a complement to credit reference checks, giving rise to many of the same issues, and yet little consideration has been given to the need for similar controls.

Specific privacy issues

The decision to make the basic search parameter the debtor or grantor[1] name is the fundamental flaw from which most of the other privacy detriments flow. There is no reasoned justification for why debtor name has to be the primary search key. APF asked in its previous submission why the primary key could not be an asset identifier, such as Vehicle or Boat Registration Number, Product serial nunber etc. Where there is a registrable charge against a serial numbered asset, we asked why it should not be sufficient for searchers to know that a charge was registered against the asset, with no need to know the identity of the grantor/debtor, at least in a first stage of inquiry. These questions have not been answered. No figures are given as to the estimated number of assets likely to be registered which do not have a serial number which could be used as the basis of the register – only with such an estimate would the size of any residual problem be known.

It is not clear what details of grantors will be held (10.15 and the table in Clause 195 do not specify – will this be done by Regulation?). It seems to be implicit in the design that the details will include names and date of birth of individuals. This in itself represents a major security risk as these two items of information held together in a widely available public register is an open invitation to identity crime – other registers which contain this information such as Birth Registries and Electoral enrolment databases have tighter access controls. Have the government agencies charged with combatting identity crime been consulted about this risk?

The suggestion that a grantor can '... include a person named as such in a registration regardless of whether they have granted an interest ...' (10.16) is incomprehensible. Does this mean one person can nominate another for inclusion in the register without consent of the second party? Does it mean that a grantor can arbitrarily name someone for inclusion who has nothing to do with the property involved?

The Bill provides for secured parties to be 'wholly responsible' for the accuracy of all details contained in their registrations (10.21), but it is not clear how this will relate to the responsibility that the Registrar will have under the Information Privacy Principles of the Privacy Act (the extent to which the information would be in a 'generally available publication' and therefore exempt from some IPPs is not explained – a major omission in the Commentary).

The Commentary also suggests that the Register system could perform validity checks against other databases (10.21). This has major privacy implications, and serious practical issues in relation to data matching. Again, there is no acknowledgement of these issues, including the risks of 'function creep' arising from comparison of the Register information with other databases, or of the applicability of the Privacy Commissioner's Data-matching Guidelines.

The Bill provides for what is described as a 'unique number' (10.22 and Clause 195) but given that the number can be devised by the secured party, it is difficult to see how it could be unique and there is no

1 Debtor and grantor are defined separately but it is unclear if they are effectively synonymous

discussion of the need for standards in relation to numbering of registrations, which could have significant privacy implications.

The provision for mandatory registration of serial numbers where they exist (10.32) is welcome, but is negated by allowing search by grantor name as well even where a serial number could meet the objective.

The apparent exclusion of grantor addresses from the Register content has the positive effect of reducing the attraction and value of the Register to third parties, but paradoxically compounds the data quality issues. It is also unclear how the proposed requirement for grantors to be given notice of 'register events' (10.103) will be achieved unless there is an address or other contact details on the Register.

Reliance on names and date of birth alone, when grantor name search is fundamental to the scheme design, is fundamentally flawed. Experience of other public registers and the credit reporting databases shows that name and date of birth alone are not sufficient to achieve required levels of accurate matching. It was necessary for the Privacy Commissioner to make Determinations under Part IIIA of the Privacy Act to allow credit reporting agencies to collect and hold drivers licence numbers to assist in matching, even where they already held addresses as an additional data field. Name and date of birth alone will simply not work. There is a naïve reference to 'technological solutions' in 10.112 which asserts that an exact match search routine with a correction table for frequently used substitutes are somehow going to deal with the enormous complexity of data matching.

There seems to be some inconsistency in the proposals with regard to name 'standards' – para 10.20 envisages Regulations prescribing some standards for source documents, but para 10.62 foreshadows advice to [searchers] to ask grantors for 'other names' by which they are known (which at least acknowledges the practical reality that many individuals legitimately have multiple 'identities') .

It seems clear that the very serious and complex issues of identity verification and matching, with enormous privacy implications, have not been adequately addressed – the Commentary seems to suggest that these are simply matters of detail which can be addressed later, when in fact they are fundamental matters which need to be resolved before the effect on personal privacy (and security) can be properly assessed.

It is not clear what the implications are of providing for registration *before* parties have entered a security agreement (2.32) - surely this invites abuse? What safeguards are there against premature registration (or the threat of it) being used against people? The analogous controls over consumer credit reporting in the Privacy Act have very strict criteria for listing of 'defaults' and 'serious credit infringements', and yet the threat of default listing is a major continuing problem.

It is not clear why a default period of registration of 7 years is proposed (2.33) – why should an entry only remain for as long as the interest is held? - this seems to be suggested later in the Commentary (10.25 and 10.70)

The Bill provides rights for persons with an interest in collateral to seek amendment of registered details (10.72 on) but while it is asserted that unresolved disputes could be taken up through either an administrative or a judicial process (10.74), the administrative process outlined in 10.77 and on does not appear to be available to grantors – leaving aggrieved grantors with only the expensive and inaccessible option of litigation (10.85 on). It is not clear how these amendment rights would interact with existing correction rights for individuals under the Privacy Act.

The provision that consumer grantors would not be able to waive the requirement to be sent a verification statement (10.104) is a welcome safeguard but seems to be undermined by the fact that failure to send a verification statement to a grantor would not alter the effectiveness of a registration (10.105). Without this as a sanction, compliance with the requirement cannot be assured, and the provision that failure to send may give rise to a claim for damages is a largely ineffective safeguard for individuals who will not

be able to afford litigation.

The proposed basis for Register searches fails to address the issue of how much personal information will be revealed in search results and whether this is necessary for or proportional to the purpose of a search. Provision is made for narrowing a search to particular classes of collateral (10.111) but this appears to be entirely for searchers' convenience, not to protect the privacy of grantors/debtors. From the latter perspective, narrow search criteria and partial disclosure of only relevant details should be requirements and design features. As it stands, there would appear to be nothing to stop a person with a legitimate interest in a particular item of collateral finding out about all other unrelated interests pertaining to the same grantor. Fishing expeditions will be rife.

The Bill provides for searches for 'authorised purposes' (2.38 and 10.113). The purposes listed in the table in Clause 229 are alarmingly broad. A critical review of the justification for each of these purposes is required, and a comparison with the permitted uses of credit information under the Privacy Act would provide a useful benchmark – the ALRC has recently reviewed the arguments relating to those limitations.

The broad provision for use of the Register by government entities for general as well as law enforcement purposes (items 17 & 18 in the Table in Clause 229) are of particular concern, and go to the issue of function creep addressed in other respects below. These 'authorised purposes' are even more generous than the general exemptions from use and disclosure principles in the Privacy Act, which are themselves controversial (see the forthcoming ALRC Report).

Alarming potential for 'function creep'

In addition to the wide 'authorised purposes' for which government entities could search the Register, the Bill provides for the potential inclusion in the Register of other interests such as impounded vehicles (10.10). Such other interests could be added by Regulation. The Commentary speculates about linkages with other databases such as NEVDIS (10.34) There is not only wholly inadequate protection against major 'function creep' – it is even positively anticipated!

Wholly inadequate privacy safeguards

The brief treatment of 'interference with privacy' in the Commentary (10.114-10.117) simply illustrates the failure to adequately address privacy issues.

The provision that a search for an unspecified purpose would lay the searcher open to claims for damages for loss or damage suffered as a result of an unauthorised search (10.114) is an extremely blunt instrument and ineffective sanction. Few individuals would be able, practically, to pursue such a claim.

The Bill would make an unauthorised search an interference with privacy under the Privacy Act, but only if the searcher was an 'organisation' or 'agency' under that Act (10.115). The vast majority of individuals and small business organisations are not covered by these definitions, and thousands more organisations and agencies exempt from the Privacy Act would face no sanction for unauthorised searches. In this respect the note to Clause 230(1) in the draft Bill is actively misleading – since individuals are unlikely to be 'organisations' that are not exempt.

Even where an unauthorised search is carried out by an entity subject to the Privacy Act, making it merely an interference with privacy is a very limited remedy. Individuals would firstly have to know that the search had taken place, and then go to the considerable trouble of making complaint. Even setting aside the experience of privacy complaints taking many months and rarely giving complainants satisfaction, relying on this mechanism provides no real deterrent. To ensure unauthorised searches are not made, they need to attract at least a civil penalty, if not criminal sanctions. Again, the model of the credit reporting provisions in the Privacy Act, and sanctions in relation to other registers and databases should be used as benchmarks.