PRIVACY IMPACT ASSESSMENT REPORT

PERSONAL PROPERTY SECURITIES REGISTER PROJECT

For: Attorney-General's Department

JULY 2009

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

In May 2009 the Attorney-General's Department (AGD) asked Information Integrity Solutions Pty Ltd (IIS) to conduct a Privacy Impact Assessment (PIA) of the personal property securities (PPS) project.

The PPS Bill will harmonise and streamline more than 70 existing pieces of Commonwealth and State and Territory legislation and establish a national personal property securities register (PPSR) with electronic registration and search processes that would replace more than 40 different registers of security interests established under the existing legislation.

The main purpose of the PPSR is to provide a real-time online notice board of personal property over which a security interest has been, or may be, taken. The "notice board" is not intended to provide complete details about the details of a loan or other transactions that are secured by PP; it does not for example include the amount of loan, whether payments are being made or the value of the security. The PPSR would be administered by a Registrar.

The PIA comes towards the end of an extensive policy and legislation development process for an updated and streamlined PPS system for Australia. The PPS policy and proposed legislation have been progressively amended and refined during the process on the basis of the various consultations, including responding to privacy issues. Most recently prior to the commencement of this PIA, the Senate Standing Committee on Legal and Constitutional Affairs (the Senate Committee) conducted an inquiry based on the November 2008 exposure draft of the Personal Properties Securities Bill (the Exposure Draft).

The PIA was conducted as AGD made final amendments to the Personal Properties Securities Bill (the PPS Bill), including taking account of the Senate Committee's recommendations and the Government's response to those recommendations, prior to its introduction to Parliament. The PIA is therefore based on the November 2008 Exposure Draft of the Bill, and on the revised provisions as provided to IIS in the course of the PIA. The parallel nature of the processes means that some of the recommendations that IIS has made in the PIA have already been reflected in the Bill as introduced.

IIS understands there is considerable support for the concept of a national PPS system which is expected to improve the ability of individuals and businesses, particularly small-to-medium size businesses, to employ all their property in raising capital including by making the PPS system more certain, and consistent and to reduce costs.

While the benefits may be considerable, the PPSR also has the potential to impact on individual privacy; in particular the proposal that in some circumstances the register will include individual's name and dates of birth associated with personal property they own and the name of the secured party (the lender).

Potential privacy risks arise around the process by which personal information is included on the register, how the register can be searched, by whom and for what purposes, and dealing with the consequences of misuse of personal information, including the approach to enforcement.

Whether the risks are manageable and can achieve community acceptance, support and trust will depend on how the PPS system is designed (both in terms of policy and administrative arrangements and in terms of the supporting legislation), built and managed.

IIS notes that a number of changes have been made to the legislation leading up to the November 2008 exposure draft and further change leading up to the June 2009 PPS Bill all intended to mitigate further privacy risks that have been identified.

IIS considers that on the basis of the Privacy Impact Assessment reported here, much of the potential adverse privacy impact initially identified has been mitigated. However, there is always the possibility that actual experience will reveal privacy risks that have not been anticipate or controlled appropriately. As a consequence, a significant theme in the recommendations to come out of the PIA is that the 3 year review of the PPSR focus on a number of potential privacy risks that now appear to be mitigated but which experience may show otherwise.

The recommendations arising out of the PIA can be summarised as follows

Recommendations 1, 4 and 13: IIS recommends that the 3 year review of the PPS Act consider:

- the impact of the operation of the PPSR on individual grantor's privacy, in particular in relation to the inclusion on the PPSR of name and DOB for grantors in relation to consumer securities and the definition of consumer property;
- whether individuals are receiving sufficient and timely notice of inclusion of their name and DOB on the PPSR and if not, if additional information should be provided or additional enforcement measures including civil penalties applied; and
- whether the provisions in the Act have been effective for example in ensuring that the grantor details included in relation to consumer property is only used for permitted purposes

Recommendation 2: IIS recommends that any proposals to include additional personal information in the PPSR beyond that permitted in the June 2009 PPSR Bill should be subject to a published PIA before a decision is made to amend the legislation.

Recommendation 3: IIS recommends that secured parties proposing to register a security interest in consumer property where the registration will include an individual grantor's name and DOB be obliged to first advise the individuals concerned of the disclosure of personal information to the PPSR. To the extent that this obligation would not be satisfied by a secured party's existing obligation under the Privacy Act, IIS recommends that the PPS Bill should provide that failure to provide prior notice of a registration that relates to consumer property and would include name and DOB is an interference with privacy under the Privacy Act.

Recommendation 5: IIS notes that the AGD is now working on a records management framework as required by the *Archives Act 1983* for the PPSR and recommends that it include as a principle in the framework that personal information be held for the minimum time possible once a registration is no longer active.

Recommendation 6, 8 and 10: IIS recommends that the Registrar should ensure that public information and education about the PPSR should:

- alert individuals whose details are migrated from existing registers to the PPSR about the operation of the register and the processes to seek access and amendments;

- ensure that potential users are aware that searches of the PPSR using an individual's name and DOB, are not permitted for any direct marketing purposes such as the use of information for pre-screening of direct marketing lists.

Recommendation 7: IIS recommends that the Registrar and the Office of the Privacy Commissioner monitor the nature of concerns about accuracy or correction matters in relation to the PPSR raised with them and that they meet periodically to consider if there is a need for additional information or other measures to ensure that individuals can most effectively pursue their concerns.

Recommendation 9: IIS recommends the PPSR be designed so as to ensure that every person making a search of the register is asked to confirm that they are doing so for an authorised purpose and advising them of the consequences of making a false declaration about the nature of a proposed search.

Recommendation 11: IIS recommends that the Registrar develop a policy, which is available publicly, which sets out the process by which an individual could seek to have their name and DOB that would otherwise appear on the PPSR suppressed and the circumstances or criteria that would apply.

Recommendation 12: IIS recommends that if the Government considers that the Registrar would not be in an ideal position to consider requests to remove details from the PPSR in "emergency" situations that it considers other options for this role, including seeking input from the Privacy Commissioner or the Ombudsman.

Recommendation 14: IIS recommends that AGD should ensure that there is a person or body with responsibility for management and oversight of privacy of the PPSR that reports to a senior manager and, when appointed, to the Registrar. Roles and responsibilities should include developing and delivering a clear policy approach for privacy for the PPSR including in relation to:

- Educational material about the PPS scheme and the operation of the PPSR;
- Handling requests to remove individual grantor details from the PPSR where there are serious privacy concerns;
- Data retention;
- An appropriate privacy policy including in relation to notification of data breaches; and
- Further PIAs at significant points for example where there is any proposal to include additional personal information in the PPSR beyond that permitted in the June 2009 PPSR Bill, change nature of security interests listed on the PPSR or to the nature of permitted searches.

The person or body should also be responsible for ensuring that the Registrar conducts regular privacy audits of the operation of the PPSR and that it responds to any audit findings in a timely way. Audits should preferably follow an annual cycle with reports available to the public.

2 INTRODUCTION

In May 2009 the Attorney-General's Department (AGD) asked Information Integrity Solutions Pty Ltd (IIS) to conduct a Privacy Impact Assessment (PIA) of the personal property securities (PPS) project.

The PIA comes towards the end of an extensive policy and legislation development process for an updated and streamlined PPS system for Australia.[1] While there is considerable support for the concept of a national PPS system, there have also been concerns about the potential impact on the privacy of individuals whose details may be included on the PPSR. The PPS policy and proposed legislation have been progressively amended and refined during the process on the basis of the various consultations, including responding to privacy issues. Most recently prior to the commencement of this PIA, the Senate Standing Committee on Legal and Constitutional Affairs (the Senate Committee) conducted an inquiry based on the November 2008 exposure draft of the Personal Properties Securities Bill (the Exposure Draft).[2]

The Senate Committee report acknowledged AGD's efforts to consider privacy and stated, "ensuring appropriate security and privacy measures are in place is essential to the success of the proposed national register". It recommended a PIA to ensure that the government is certain that it has done everything necessary to address real privacy issues. The recommendations emphasised the need for independent expert involvement in the PIA and specified that if the PIA did not address all issues raised by the Office of the Privacy Commissioner (OPC) AGD should separately address these. The PIA has taken the Senate Committee report as a starting point and has aimed to identify privacy issues and to make recommendations to address these.

The PIA was conducted as AGD made final amendments to the Personal Properties Securities Bill (the PPS Bill), including taking account of the Senate Committee's recommendations and the Government's response to those recommendations, prior to its introduction to Parliament. The PIA is therefore based on the November 2008 Exposure Draft of the Bill, and on the revised provisions as provided to IIS in the course of the PIA. The parallel nature of the processes means that some of the recommendations that IIS has made in the PIA have already been reflected in the Bill as introduced.

2.1 BACKGROUND TO THE PIA

Australia is in the process of introducing a national framework for the regulation and registration of security interests in personal property. The framework was developed as part of the Council of Australian Governments' (COAG) PPS reform. The PPS Bill will harmonise and streamline more than 70 existing pieces of Commonwealth and State and Territory legislation and establish a national PPS Register (PPSR) with electronic registration and search processes that would replace more than 40 different registers of security interests established under the existing legislation.

Many Australians are affected by personal property securities laws – as buyers of property that is or may be subject to an encumbrance; as consumer or business borrowers; as investors who might be contemplating buying into a business; or as financiers who provide the funds to facilitate such

[1] Detailed information about the PPS reform including background papers, presentations and the November 2008 Exposure Draft of the PPS Bill is available at http://www.ag.gov.au/pps

[2] The Senate Committee report is available at http://www.aph.gov.au/Senate/committee/legcon_ctte/personal_property/index.htm

activities.

Personal property is any property other than land or buildings (real property). It may be either tangible (for example a car) or intangible (for example intellectual property such as copyright). A personal property security is created when a financier takes an interest in personal property as security for a loan or other obligation, or enters into a transaction that in substance involves the provision of secured finance.

The PPS reforms aim to give lenders more certainty as to who would have priority where competing interests exist and would also allow, for example, potential buyers of personal property to check if the property is unencumbered, or in the case of motor vehicles if it has been reported as stolen or written off. The PPS Bill would establish rules for creating valid security interests in personal property, as well as rules governing priority among competing interests in the same property. It would set out the processes for enforcing a security agreement following debtor default, which would operate in conjunction with enforcement provisions in the Consumer Credit Codes and security agreements between the parties.

2.2 Privacy and the PPS Project

While the PPS reforms are expected to deliver considerable economic benefits to the Australian community the PPSR does have potential to impact on individual privacy; in particular in some circumstances the register will include personal information about individual; specifically their name and date of birth (DOB).

Australians' privacy in relation to their personal information is protected by a range of legislative measures depending on where it is held and the nature of the personal information concerned. The PPSR will be operated by AGD, which must comply with the Information Privacy Principles (IPPs) in the *Privacy Act 1988* (Cth) (the Privacy Act). The National Privacy Principles (NPPs) in the Privacy Act will apply to many of the private sector organisations that seek to register securities on the PPSR.

The need to protect privacy has been a consideration in the design of the PPSR, particularly in relation to security agreements that relate to borrowing that is for personal, domestic or household purposes. The PPSR distinguishes between commercial and consumer property and includes a series of measures to ensure its operation is consistent with existing consumer protections for consumer credit and to protect privacy.[3]

Potential privacy risks arise around the process by which personal information is included on the register, how the register can be searched, by whom and for what purposes, and dealing with the consequences of misuse of personal information, including the approach to enforcement of privacy protections.

The kinds of privacy impacts most likely to cause most concern arise from:

- The nature of personal information on the register and the permitted uses;

[3] The June 2009 PPS Bill, s.10 defines consumer property "personal property held by an individual, other than personal property held in the course or furtherance, to any degree, of carrying on an enterprise to which an ABN has been allocated".

- Intentional misuse of the register and data in the register beyond the uses provided for in the legislation, ranging from profiling and marketing to various forms of theft, including identity theft;
- Intentional extension of the use of the register beyond that provided for by policy and in legislation (seen as "function creep" if considered inappropriate);
- Errors of fact in the register; and
- Inaccurate or inappropriate inferences or conclusions drawn from data on the register, whether or not it contains errors of fact.

Whether the risks are manageable and can achieve community acceptance, support and trust will depend on how the PPS system is designed (both in terms of policy and administrative arrangements and in terms of the supporting legislation), built and managed.

2.3 Purpose and scope of the PIA

ADG sought the PIA in part in response to the Senate Committee's recommendations. The purpose of the PIA was to assist AGD to refine the provisions of the PPS Bill with respect to the handling of personal information and to assist it to develop register processes and systems so that both privacy and project goals could be achieved.

The scope of the PIA was therefore to:

- Consider the PPS Bill, the issues the Senate Committee raised in its report, and proposed amendments as available to IIS during the PIA;
- Consider the privacy issues the OPC raised in its submissions to AGD and the Senate Committee;
- Develop a clear understanding of the proposed operation of the PPS system and register, including the permitted purposes, proposed search options, links with other systems, so that any new risks to privacy can be identified;
- Assess the proposed operation of the register against the IPPs and the NPPs in the Privacy Act and other relevant legislation and any other privacy risks that arise beyond those identified in the IPPs and NPPs; and
- Develop findings and recommendations to address the issues identified.

IIS notes that while it has endeavoured to take all the provisions of the Bill into account in its analysis, it has focussed particularly on Chapters 5 and 6 that have most relevance for the handling and protection of personal information and therefore the most impact (positive and negative) on privacy.

2.4 METHODOLOGY

A PIA is a process that enables organisations to "anticipate and address the likely impacts of new initiatives, foresee problems, and negotiate solutions."[4] IIS bases its approach on the PIA guides prepared by the Australian OPC and the Office of the Victorian Privacy Commissioner (VPC) and best practice identified elsewhere in current Australian and International approaches.[5]

The PIA sought to identify potential risks to compliance with the Privacy Act and consider if there are changes that could be made to minimise privacy risks, including any gaps in privacy protection, as the PPS scheme is introduced and implemented.

While ensuring an appropriate legal framework and ensuring compliance with it is one privacy risk that needs to be managed, IIS focuses in addition on issues that it understands individuals tend to be most worried about in relation to the handling of personal information about them. These include:

- loss of control by individuals of their personal information (including through unacceptable new uses of information seen as function creep);
- loss of control by the organisation holding their personal information (for example through security breaches or internal misuse, whether intentional or unintentional);
- whether the organisation is able to demonstrate that it can be trusted with the information (accountability and governance);
- bearing an unfair burden of risk when the system fails or otherwise malfunctions.

In developing its recommendations IIS has drawn on its "layered defence" approach that applies a number of possible "tools" to arrive at practical solutions that fit the particular circumstances. These tools include:

- "Business as usual" good practice, including education, process and culture change regarding the expectations about the way things are done by staff, and the actions that users need to take to protect themselves;
- Additional law where risks are particularly high, for example specific use and disclosure limitations, criminal penalties, special measures to ensure review before critical changes are made;
- Technology, including design limits on information collected, what can be connected and who can see what;
- Governance, including transparency and accountability; and
- Safety-net mechanisms for citizens when failure or mistakes happen

[4] See www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html

[5] See the Office of the Privacy Commissioner's *Privacy Impact Assessment Guide* available at www.privacy.gov.au/publications/pia06/index.html and note 2 above.

The PIA involved the following steps.

- Information gathering including reviewing the extensive material available with a particular focus on submissions to AGD as it developed the PPS approach, and to the Senate Committee, and on the provisions of the PPS Bill including the revised provisions as provided to IIS during the course of the PIA, and other material on the policy and operation of the register and also meetings with AGD staff – a list of the material considered is at Appendix 1.

- Analysis of the information using the multi-dimensional framework noted above to identify key aspects of the project that may potentially have an impact on privacy and privacy risks or issues– this phase resulted in a brief issues paper used in the consultations noted below;

- Consultation with some privacy regulators, privacy and consumer advocates and also with some business organisations. The meetings held are noted at Appendix 2. Participants, and other interested people not able to attend meetings, were invited to provide any additional comments in writing. The consultation process undertaken was relatively limited reflecting the time available to conduct the PIA and the extent of the earlier consultation processes, including the Senate Inquiry. The issues raised in consultations are reflected in the discussion at section 4 below; and

- Refining analysis of issues, including by reference to the IPPs structured by reference to the IPPs in the Privacy Act, and developing recommendations into a draft report and following discussions with AGD, developing this final report.

3 THE PPSR – PERSONAL INFORMATION HANDLING AND OPERATION

This section of the PIA provides a brief overview of the proposed operation the PPRS as known at the time IIS conducted the PIA. It reflects changes made to the PPS Bill prior to its recent introduction to the Parliament to the extent that they were made available to IIS in time to be included in the PIA report.

However, the key reference for the PIA continued to be the November 2008 Exposure Draft of the Bill, referred to in this PIA report as the PPS Bill, and so references to the legislation below are references to that draft of the PPS Bill unless specifically noted otherwise. The few references to the PPS Bill as it was introduced to Parliament in June 2009 are identified as relating to the June 2009 PPS Bill.

3.1 OVERVIEW OF THE PPSR

The PPSR would be established and maintained by the Registrar.[6] In its Revised Commentary (RC) on the PPS Bill, AGD identified the main purpose of the PPSR is to provide a real-time online notice board of personal property over which a security interest has been, or may be, taken. [7] The "notice board" is not intended to provide complete details about the details of a loan or other transactions that are secured by PP; it does not for example include the amount of loan, whether payments are being made or the value of the security. Rather the PPSR will flag the fact that a security exists over a particular piece of property. It is expected that registration will become the most commonly used method of perfecting a security interest for the purpose of enforcement.[8] A person would also be able to search the register to determine whether a prior registered interest exists in personal property when deciding to purchase it or to lend money on security of the property. [9]

The PPS Bill provides that the secured party (or someone on its behalf) would apply for registration of a personal property security. To do so, the secured party must believe on reasonable grounds that it holds, or will hold, a security interest in the property.[10] The secured party would provide the relevant information to the Registrar who would give effect to the registration if the application is in the approved form, the fee has been paid, the application is not frivolous or vexatious, or not permitted by the Bill or by the regulations.[11] The registration comprises, among other things, data about the secured party (essentially the lender), the grantor (essentially the borrower) and the collateral.[12] Applications must be in writing but would generally be lodged electronically through a web browser or through a business to government interface.[13]

The Bill would establish rules for creating valid security interests, as well as comprehensive and coherent rules governing the priority of competing security interests. Under the PPS Bill a secured

[6] PPS Bill, s186
[7] Personal Properties Securities Bill 2008 Revised Commentary – December 2008 www.ag.gov.au/www//rwpattach.nsf/VAP/(CFD7369FCAE9B8F32F341DBE097801FF)~PPS+-+Revised+Commentary+Dec+2008+-+11+Dec.pdf/$file/PPS+-+Revised+Commentary+Dec+2008+-+11+Dec.pdf
[8] RC Para 10.3-10.4
[9] PPS Bill, s.85
[10] PPS Bill s.190
[11] PPS Bill s.189
[12] PPS Bill s.191
[13] RC Para 10.14

party would not be compelled to register personal property in which there is a security interest, however there are incentives to register. By registering (a means of perfecting a security interest), a secured party (i) ensures priority (a) over any unperfected interests in the same property[14] and (b) generally over any later perfected interests in it and (ii) maintains their security in the event of the grantor's insolvency or bankruptcy.[15]

Provisions that establish when a person acquires personal property free of a security interest would complement the rules about creating valid security interests; for example where consumer personal property has a value of less than $5000.[16]

A collateral registration would be registered from the moment that it became available for search on the Register. The period of registration would be a maximum of seven years for consumer property and serial numbered property, and 25 years or indefinite for commercial property, extendable by amendment.[17]

A registration would be ineffective where it contained a seriously misleading error[18] or if the registration was affected by a specified defect such as where the registration was not disclosed by a search of the PPSR by reference to the grantor's details or a serial number where required.[19]

In this way, the PPS Bill provides protection to a party who does an appropriate search of the PPSR and finds no registration relating to the relevant property. Generally, that party could buy or lend against the property free of any existing security interests in it.

3.2 INFORMATION, INCLUDING PERSONAL INFORMATION, HELD ON THE REGISTER

In keeping with the notion of the register as a notice board, the PPRS will contain relatively limited, although still sensitive, information about grantors.

The table below sets out the information that will be contained in financing statements that are the basis of an application to the Registrar to register a security interest.[20] Importantly, and as set out in the June 2009 Bill, the PPSR will not contain personal information about a grantor where the personal property has been categorised as "consumer property" and it is possible (and required by regulations) for the collateral to be described by a serial number.

Table 1: PPSR Contents – Financing Statements with respect to security interests

Secured party	Grantor: One of the following options	The collateral and proceeds
Details about each secured party as prescribed by regulations	(a) No grantor details if the collateral is consumer property, and is required by the regulations to be described by serial number	The collateral must be described as either (i) consumer property or (ii) commercial property

[14] PPS Bill, s.100
[15] PPS Bill, s.233
[16] PPS Bill, s.88
[17] PPS Bill, s191
[18] PPS Bill, s198
[19] PPS Bill, s199
[20] June 2009 PPS Bill s. 153(1)

Address for service of notices (fax, email and any identifier provided)	(b) if the collateral is consumer property, and is not required by the regulations to be described by serial number—the grantor's name and date of birth, as evidenced in accordance with the regulations, and no other details;	The collateral may or must be described by serial number if allowed or required by regulations
	(c) in any other case—the grantor's details as prescribed by the regulations.[21]	The collateral must belong to a single class of collateral as prescribed by regulations and any description of proceeds must comply with regulations
		The end time for the registration must be specified (7 years for consumer collateral or 25 years for commercial collateral, unless amended)

At least in the early implementation of the PPSR it is likely that most registrations in relation to consumer collateral will be in relation to motor vehicles and so will be listed by serial number. It also appears unlikely that collateral worth less than $5 000, for example fridges and washing machines, will be registered whether or not it could be registered by a serial number; as noted earlier, the Bill provides that personal property of a personal, domestic, or household nature worth $5000 or less will be considered to be free of security interests.[22] In other words in these circumstances a purchaser of personal property would have good title over the property whether or not there was a security interest registered.

As will be discussed in detail in section 3.3 below IIS understands it is difficult to predict either the number of individuals whose personal information may be held on the PPSR at its inception or as it develops over time. However, IIS understands that is it expected that the PPSR would initially contain personal information about a relatively small subset of the grantor population (at the very most 140 000 individuals but in AGD's view likely to be considerably less).

The PPSR Register may also contain a limited amount of other important information about personal property, such as whether it has been confiscated under certain types of court orders. Each registration will also include a history, for example the time and date of registration, and any amendments made. Registrations may also include attachments, for example an image of the personal Property. AGD is yet to develop detailed rules here but expects that attachments will need to be in standard PDF format, be scanned for viruses and be of limited size, possibly up to 1 MB.

[21] IIS understands the details required would be similar, and would not include, for example a grantor's address – see PPS Discussion Paper: Regulation to be made under the PPS Act (Regulations DP) August 2008, available at www.ag.gov.au/pps
[22] PPS Bill, s.88

IIS understands that the Registrar will hold information, including personal information, in addition to that listed above. This information will be of four main kinds:

- Records relating to searches of the register in form of audit logs, or where searches are conducted by authenticated organisations that have established accounts with the Registrar to conduct searches, the records of those accounts, including searches conducted, invoices etc;
- Billing and payment records;
- Records of interactions with the Registrar in relation to particular registrations, including in relation to:
    - a demand for amendment;
    - a request to withhold information such as name and date of birth from the register; or
    - a complaint under the Privacy Act or an appeal, for example, under the *Administrative Appeals Tribunal Act 1975*;
- Historical copies of expired registrations where the Registrar is required to retain these in accordance with a disposal authority under the *Archives Act 1983*.

IIS notes that the PPRS will also have links to other databases, for example, the Australian Investment Securities Corporation's (ASIC) corporations register and the National Exchange of Vehicle and Driver Information System (NEVDIS). The intention here is that the PPSR will interrogate specified data sets to "verify" some of the information provided in financing statements at the time of registration and also to add value to PPSR searches. For example, as part of a registration process or search of the PPSR a serial number such as a Vehicle Identification Number (VIN) would be checked against the relevant register. Information obtained via links to other data sets may lead to an application for registration to be amended or in the provision of information as part of a search result. If the number were a valid number, details associated with the VIN, for example, vehicle make, colour and registration number, would be passed to the secured party applying to make a registration or in search results. As far as IIS understand there is no intention to conduct such checks in relation to personal information (name and DOB) submitted in relation to consumer registrations. In general the Registrar would have a record of the fact that a database has been interrogated but would not be adding any detail from these "interrogations" to the PPRS.

3.3 SCALE OF PPSR – POSSIBLE EXTENT OF PERSONAL INFORMATION HELD

Participants in the consultations undertaken as part of this PIA were interested in the likely size of the population of personal property that might be registered by grantor details rather than serial number.

AGD advised that the nature of the project is such that any volumes provided at this time can be only taken as a best estimate; this estimate is that, based on the operation of the New Zealand PPS Register, the Australian register would contain some 6.9 million registrations after 5 years of operation and around 4% (276,000) of these would contain individual grantor details.

In considering this estimate it has to be noted that while similar to the proposed PPSR, the New Zealand PPS Register does not work identically. For example, New Zealand collects grantor details for consumer motor vehicle registrations, while the PPSR will not. Also, AGD advises that there are variations in the threshold for registrations; in New Zealand the value of security could be as low as $2000 while in Australia, as discussed in section 3.2 above, it is unlikely to be below $5000.[23] The figure of 4% represents the proportion of current NZ registrations (i) where there are no specific listings of motor vehicles as collateral and (ii) one or more debtors is an individual.

It is important to note that the figure of 276,000 noted above would not necessarily be the number of individuals about which the PPS Register held information. Some individuals, particularly in a business context where they are acting as sole traders, are likely to have more than one registration against them. For example an independent supermarket may well receive stock on a retention of title basis, have leased freezers and fridges and separately leased checkout equipment. This would result in three registrations.

When the register commences operation IIS understands that it will contain around 4.7 million registrations migrated from existing registers. Some 97% of these registrations will relate to either motor vehicles or company charges. In neither case will the migrated registrations contain information about individual grantors. Some of the remaining 3% of migrated registrations (140,000) may include grantor details but it is not yet clear how many will do so.

After commencement it has been estimated that in the first year there will be 1.5 million new registrations and 1.2 million cancellations, with the number of transactions growing by 20% annually until it levels out. On this basis, there would be 6.9 million registrations after 5 years assuming transaction volumes were still growing.

3.4 Operation of the PPSR

Initially the PPSR will be held and managed within the AGD. However IIS understands that the system is being designed to operate on a relatively stand alone basis so that it could if needed be transferred to another agency.

AGD is currently working to a COAG time line agreed on 2 July 2009 that requires the core functionality of the register to be available by May 2010 following which stakeholders will have a 12 month transition period before the new scheme commences in May 2011. To meet this time line AGD has proceeded with the development of the concept and systems for the PPSR in parallel with the development of the PPS policy and the PPS Bill.

The Register would be operated at all times subject to limited exceptions. There are four main methods of incoming interaction possible with the Register, these being:

- Electronically, specifically via Web and B2G channels;
- Contact Centre, including vehicle search using interactive voice response;
- Physical lodgement via mail or fax, and

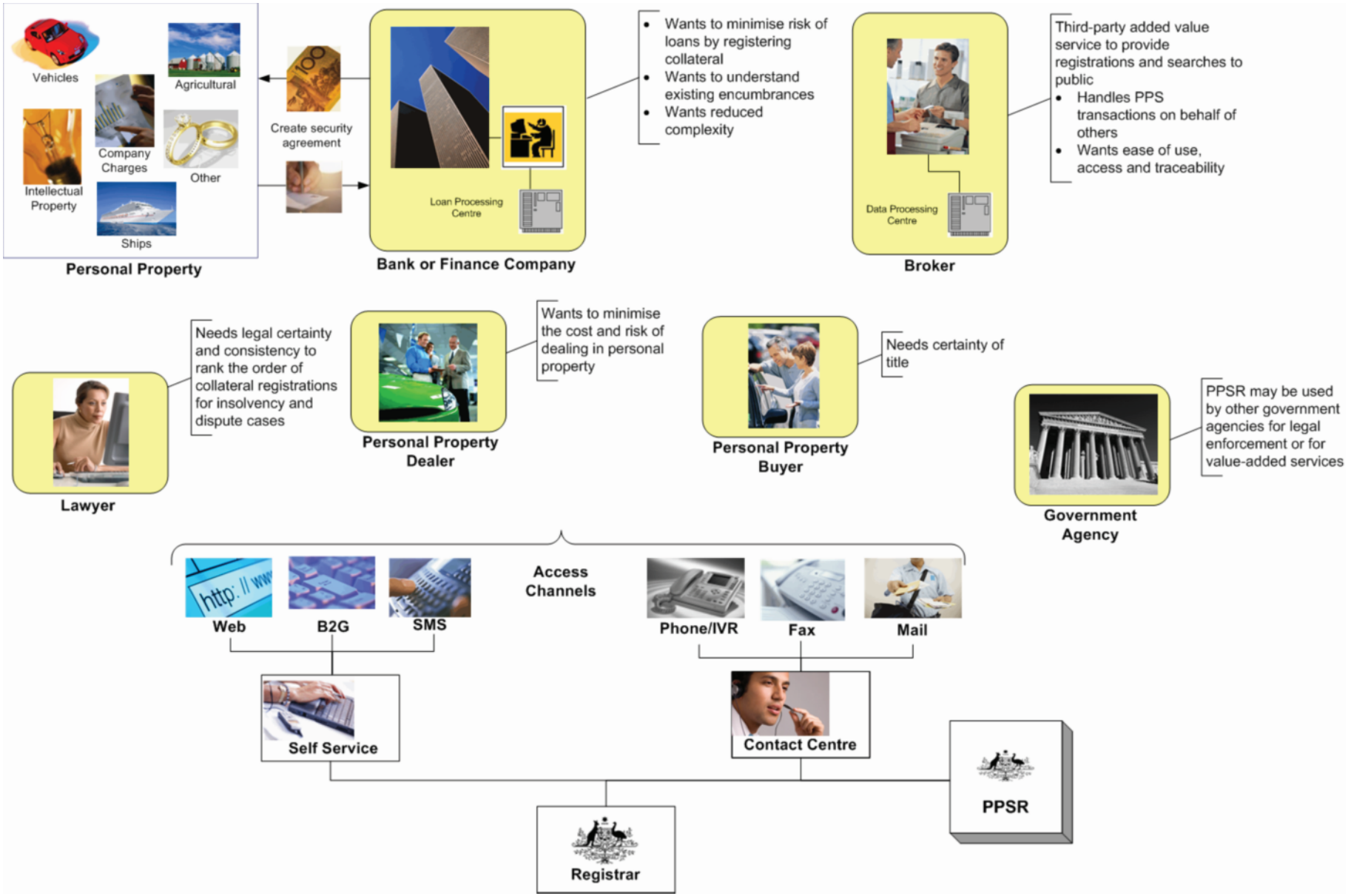
[23] PPS Bill s.88

- Mobile phone for vehicle search only using SMS.

It is expected that the primary means will be electronic (web browser or B2G), with the other methods provided to ensure breadth of access to the services offered by the PPSR

AGD plans to outsource the contact centre role but has not yet selected a provider. The contact centre staff will perform a limited range of functions including account management, conducting searches on behalf of people who do not have Internet access accepting hard copy applications for registration (again as an alternative to Internet applications).

A diagrammatic representation of the PPSR features user interactions described so far follows.


Vehicles
Agricultural
Company Charges
Other
Intellectual Property
Ships
Personal Property
Create security agreement
Loan Processing Centre
Bank or Finance Company
Wants to minimise risk of loans by registering collateral
Wants to understand existing encumbrances
Wants reduced complexity
Data Processing Centre
Broker
Third-party added value service to provide registrations and searches to public
Handles PPS transactions on behalf of others
Wants ease of use, access and traceability
Lawyer
Needs legal certainty and consistency to rank the order of collateral registrations for insolvency and dispute cases
Personal Property Dealer
Wants to minimise the cost and risk of dealing in personal property
Personal Property Buyer
Needs certainty of title
Government Agency
PPSR may be used by other government agencies for legal enforcement or for value-added services
Access Channels
Web
B2G
SMS
Phone/IVR
Fax
Mail
Self Service
Contact Centre
PPSR
Registrar

3.4.1 SEARCHING THE PPSR

According to the RC, a central feature of the PPSR would be the availability of reliable, low cost, fast and accessible search facilities. The register would be accessible for all purposes, including for searches, by direct online access twenty four hours a day, seven days a week, or by making a written application to the Registrar. This could be done through a web browser, a business to government interface, SMS message or written application. Even people located in the most remote areas of Australia would be able to access the register for search and other purposes.[24]

The PPS Bill provides that the Registrar must, generally speaking, give an applicant access to the register to search for data if the search is authorised, the application is in the approved form and the fee paid.[25] The register may be searched by reference to:

- the secured party's details;
- the grantor's details (including an individual's if permitted to be included);
- the serial number of the collateral;
- the time of the search or with the consent of the registrar an earlier nominated time; or
- any other criteria prescribed by the regulations.[26]

The RC goes on to state that persons searching the register for serial numbered goods, for example, motor vehicles used for consumer purposes, would be able to search the register by reference to the serial number only, as is already the practice in some State registers, for example, REVS and VRS, that do not record grantor details.[27] It also states that while the search criteria to be prescribed by regulation are not yet settled, it is proposed that a person would be able to search the register by reference to the unique identifier of the registration.[28]

If the collateral is of the type that does not have a serial number or unique identifier, a register search would be made by reference to the grantor's details, that is, the grantor's unique identification number (such as the ACN for a company) or, if the grantor is a natural person, his or her name and DOB. IIS understands that the register is being developed to allow only direct match searching. Fuzzy searches using only part name or DOB would not be permitted. Thus, when a search is made by reference to an individual secured party's or grantor's details, data would be returned only when the search information entered is exactly matched. In the case of an individual grantor this would require the searcher to enter the grantor's first name, last name and DOB. It would not be possible to enter a name and have the DOB returned.

The register search function would allow users to refine their searches according to their needs, for example, by searching against a grantor's name, DOB and a particular class of collateral.

[24] RC para 10.108-10.109
[25] June 2009 PPS Bill s.170(2)
[26] June 2009 PPS Bill s.171(1)
[27] RC para 10.112
[28] RC para 10.113. At the time of registration, secured parties would be able to enter a unique number (or unique identifier) devised by them in relation to a particular registration (RC, para 10.24).

The system would allow a retrospective search of the PPSR if the Registrar consents. This would enable an authorised User to search the Register at a point in time (date/time) to see what they would have returned had they undertaken a search at that particular point in time. It is noted that this type of search cannot return "verification" details at a point in time (that is the results of a check of, for example, NEVDIS or of ASIC databases) but can return PPSR details back to "go live".

3.4.2 SYSTEM ACCESS AND SECURITY

At the time this PIA was undertaken most of the detailed design work, including the user interface design was close to completion and work on infrastructure development was starting. To assist it to gain an understanding the operation of the PPSR and to identify any privacy issues at this stage in the system development, IIS reviewed documents including system requirements and solution architecture and received briefings from AGD and contractor staff.

IIS notes the following features of the proposed operation of the PPSR that it identified as relevant in considering the privacy and security of personal information held in the PPSR.

- As noted AGD will initially hold the PPSR. The user interface will sit within AGD in a purpose built area for public facing web services. The database will be behind another level of firewall. The arrangements, which will be similar to those in place for existing AGD services including AusCheck (a centralised background checking agency which is a branch of AGD), will be subject to high level security standards.[29]

- A design principle is that all PPSR system events must be traceable to the originator (individual or organisation);

- The PPSR will be able to be used (for registrations or searches) by "casual users" or by accounts customers. Other than where an account holder applies for credit, users will not be required to provide evidence of identity. However, all PPSR registrations and searches will be on fee basis and there will be a payment record (cheque or credit card) associated with every registration or search by a casual user.

- Where a credit card is used to pay fees the credit card details pass through but will not be stored within the system; every credit card transaction will be done as a pre-authorisation and the audit trail for the transaction will include a hash of the credit card number and bank authorisation code.

- The system is being designed to record all changes made to the PPSR. This includes every event that can occur within the security and business domains; for example a change of User permission in the Security Domain or a change of Collateral description in the Business Domain.

- The System is required to ensure audit logs/journals cannot be amended after creation. This should involve the use of cryptographic hashes (MD5/SHA) and other process and technology controls as necessary. The hashes should be stored in a separate secure location

[29] for information about AusCheck see www.ag.gov.au/www/agd/agd.nsf/Page/Organisational_StructureNational_Security_and_Criminal_JusticeAusCheck

and other appropriate controls implemented to ensure that the hashes cannot be altered after they have been written.

- A design feature is that the use of PPSR will be defined by roles. However, these roles will not be hard coded and it will be open to the Registrar to change the level of access permitted for particular roles.

- To interact with the system online users will need to have java script installed and turned on and will also need to have cookies enabled. The system will use cookies for a particular session; these will be deleted at the end of the session.

- Together, the legislative provisions and the system design guard against individuals or organisations downloading the whole register, for example to use in direct marketing systems. The features here include: searches are for specified purposes on a fee for search basis, only one search at a time with specific details entered and result returned for a direct match only.

- Although unlikely to be fine enough to identify one-off activity, for example casual looking by a neighbour or for celebrity listings (there are other deterrents here including fees to search and potential for criminal offence), the fact that the system records details for each transaction, including a hash of a credit card number, would facilitate identification of fraudulent activity or other misuse, for example where the same credit card is used to conduct a lot of casual searches, or for an account customer where there is a spike in usage against expected use.

IIS notes that the PPSR is still in an early stage of development and there are decisions yet to be made about the content of regulations and about elements of the system operation and design. IIS considers that the approaches taken to date are consistent with AGD's obligation under IPP 4 of the Privacy Act to take reasonable steps to protect personal information. However, it considers there should be security risk assessments and privacy audits undertaken as the PPSR implementation proceeds.

3.4.3 Interaction between PPS Bill enforcement provisions and Privacy Act protection

A feature of the PPS scheme, as set out in the June 2009 PPS Bill, is that, amongst other enforcement strategies, it creates two circumstances in which failure to comply with the provisions of PPS law will also constitute an interference with an individual's privacy under the Privacy Act; in these circumstances an individual will be able to complain to the Privacy Commissioner about the act or practice.

Although the Registrar will be able to investigate privacy complaints, there will be administrative arrangements in place to minimise any scope for dual investigation in relation to a complaint at any particular time. IIS understands that the idea would be that in general individuals would first approach the Privacy Commissioner. However, that would not mean the Registrar would not pursue a matter if the individual had not done so.

The following outlines the proposed approach.

- Section 13 of the Privacy Act would be amended to include a paragraph stating that failure of a secured party to provide a grantor with a verification statement, or conducting an unauthorised search, or unauthorised use of information obtained from a search, of the PPSR is an act or practice that constitutes an interference with an individual's privacy.
- Ss.157(4) and 173(2) of the June 2009 PPS Bill would provide that an unauthorised search or unauthorised use of information would constitute an act or practice involving an interference with the privacy of an individual for the purposes of section 13 of the Privacy Act.
- An individual could complain about an unauthorised search, or unauthorised use of information obtained from a search, of the PPSR to the Privacy Commissioner under section 36 of the Privacy Act. A note under subsections 157(4) and 173(2) will indicate that complaints can be made under section 36 of the Privacy Act.
- The Registrar would have an at large power to investigate a suspected contravention of PPS Act with respect to failure secured parties to provide grantors with verification statements or unauthorised search and/or use of information obtained from a search.
- The Registrar would also have an express power to decline to investigate a complaint. This would allow the PPS Registrar to refer complaints to the Privacy Commissioner by administrative means subject to a policy of referring complaints directly to the Commissioner in the first instance (unless the complaint involved an obvious case of serious interference with an individual's privacy).
- The Privacy Act would be amended so that the Privacy Commissioner must cease an investigation relating to the PPS Act if the Commissioner is satisfied that the complaint involves a serious interference with the person's privacy. The criteria for this mechanism would need to be developed. IIS understands that the criteria may relate to the number of unauthorised searches and the purpose and consequences of the search.
- The Privacy Commissioner would also have the discretion to decline or defer an investigation where the Commissioner becomes aware that the Registrar is investigating a relevant contravention of the PPS Act.
- The Privacy Commissioner would be empowered to revive an investigation in the event that the Registrar declined to investigate the complaint as referred or commenced or closed its investigation (other than where the investigation is closed due to the commencement of proceedings for a civil penalty).

- The Privacy Commissioner would have to discontinue dealing with a complaint except the extent that it concerns matters unconnected with the alleged contravention of the PPS Act where the Registrar or the DPP had applied for a civil penalty.
- The Registrar or the DPP, on behalf of the Commonwealth would be able to apply to the Federal Court for the imposition of a civil penalty. The DPP's power to institute proceedings would arise under the Director of Public Prosecutions Act 1983.

4 FINDINGS AND RECOMMENDATIONS

As noted in the Introduction at section 1, the PIA was conducted at the same time as AGD made final amendments to the Personal Properties Securities Bill (the PPS Bill), including taking account of the Senate Committee's recommendations and the Government's response to those recommendations, prior to its introduction to Parliament.

The discussion below is structured against the IPPs in the Privacy Act. However, the intention is to focus on key issues raised by the legislative and policy proposals rather than to conduct a provision-by-provision examination of the IPPs against the provisions of the Bill or the proposed operation of the PPSR. This is in part because of the project stage, which is at the design and development phase where a range of decisions are yet to be made, and also because this PIA comes at point where there have already been several processes to identify the areas of concern.

As noted earlier, in the course of the PIA IIS held consultations with privacy and consumer and business stakeholders. The matters raised in these consultations are reflected in the discussion. As noted earlier, IIS has also reflected the provisions of the June 2009 Bill but only to the extent that they were known to it as it prepared the PIA report. While a number of the privacy concerns raised in submissions have now been resolved, the discussion below still notes those issues and aims to describe briefly how the thinking on the issue developed. For each issue the IIS understanding at the point the PIA was finalised is identified.

4.1 COLLECTION OF PERSONAL INFORMATION

This section of the PIA considers the collection of the personal information in the context of the PPS project. IPPs 1-3 in the Privacy Act set out provisions to ensure that the collection of personal information is limited to that necessary to fulfil lawful functions or activities, that individuals have information about the collection that will allow them to make informed choices and that the collection is by fair and lawful means.

4.1.1 EXTENT OF PERSONAL INFORMATION ON THE PPSR AND HOW REGULATED

The content of the PPSR is of critical importance from the point of view of individual privacy and, in relation to grantors who are individuals could raises significant privacy risks. In earlier drafts of the Bill, the nature of the information about grantors that would be included on the register did not appear in the Bill but was to be left to the regulations.

If consumer goods that have a serial number, such as cars and boats, are identified by serial number alone and personal information about the grantor is not included on the register, the privacy risks are considerably reduced. In other cases, the extent of the privacy risk would depend on exactly what personal information would be included.

The content of the PPSR, and the privacy risks that might arise from it, was an issue addressed by a number of submissions. Submissions focused on two main issues:

- Should the matters to be included in the register be included in the primary legislation or in regulations?
- Should the register include the name and DOB of individuals, or more or less personal information?

The issue of whether the matters to be included on the register should be included in the primary legislation and or set out in the regulations was canvassed in a number of submissions, including the OPC, the VPC and the Women's Legal Service Victoria on behalf of Women's Legal Services Australia (WLS VIC).

While it is easier to make regulations than to secure the passage of an amendment bill, regulations still require scrutiny by Parliament. In its report, the Senate Committee recommended that the primary legislation for the personal property securities reform should include the key privacy protections for individuals, including a prohibition on making the address details of any individual public.

On the basis of its consultation with AGD in the course of the PIA, IIS was advised that the individual grantor details to be included in the register would be addressed the primary legislation, not regulations. As noted at section 3.2 above, the June 2009 PPS Bill now reflects that position.

As to how much or how little personal information should be included on the PPSR, submissions to the Senate Committee took as their starting point the assumption in the RC that a grantor's name and DOB would be included on the register where the secured property did not have a serial number. OPC stated that only the personal information necessary to achieve the objectives of the scheme should be included and that this did not include DOB. Linked to other information, DOB could potentially lead to the creation of comprehensive databases about individuals. OPC went on to say too much information would enable a casual browser to build up financial profiles of individuals. Too much detail would lead to safety concerns (Australian Privacy Foundation (APF)) and to the possibility of identity theft (APF, Consumer Law Action Centre (CALC)). APF noted that databases that contain personal information are generally not widely available and subject to strict controls, for example, births, deaths and marriage registers and the electoral register, in order to protect privacy and to prevent identity theft.

On the other hand, too little detail would not secure accuracy and lead to errors (APF, Veda Advantage (Veda)). In Veda's experience, a minimum of three identity elements are necessary to minimise the incidence of false matches and to gain greater confidence in search outputs. APF expressed concern that there would be pressure to add more identifiers to the register and WLS Vic and CALC were particularly concerned about the consequences for women and children escaping family violence of including residential addresses on the register. CALC was not confident that addresses would not be included in the future. In consultation, AGD noted, however, that address was the least stable of the three elements. The Australian Bankers Association (ABA) and the Australian Finance Conference (AFC) also noted this; the ABA noted that its members have a preference for name and DOB if only two identity elements are to be included on the PPSR.

Table 2: Collated views about what personal information should be included in the PPSR	
Personal information	Comments collated by IIS based on views expressed in the submissions
No personal information at all	If consumer property has a unique serial number, then that unique serial number would be included on the register; if not, consumer property should not be included on the register. Some property would not be included on the register; while the privacy risks to individuals would be largely eliminated, IIS understands that many businesses, especially sole traders, may be disadvantaged if proposed personal property securities could not be registered.
Name only	This would apply to property that does not have a serial number and cannot be adequately described. A person's name is not a unique identifier but it may be sufficient to achieve the purposes of the scheme if the number of such entries is relatively small. The name and a careful description of the collateral could be enough, especially if the name is the person's full name.
Name and DOB	This would apply to property that does not have a serial number and cannot be adequately described. Searches based on name and DOB provides a level of certainty as, in most cases, name and DOB limit the grantor to only one possible person.[30]
Name, DOB and residential address	This would apply to property that does not have a serial number and cannot be adequately described. This position would mean that for some individuals this relatively sensitive set of information would be accessible. There may then be a range of privacy risks depending on an individual's circumstances and how the information is used. A question that has been raised is how to mitigate these risks in the cases where there may be potential for real harm.

The consultations for this PIA were based on AGD's advice that address details would not be included on the PPSR. The question as to whether DOB, as well as name, should be included was the subject of considerable discussion in the consultations IIS held in the course of this PIA. The ABA, the AFC and Veda Advantage continued to argue strongly that as a minimum two elements were needed to accurately identify individuals; DOB was preferred over address as the second element. Veda Advantage also reiterated that a third element, which could be part of an address such as a postcode, would be its strong recommendation. It argued that if this additional element would not add to the privacy risk if it were only used to refine searches where the searcher already knows the postcode and enters it as part of the search criteria.

On the other hand, the privacy regulators and privacy and consumer advocates remained concerned

[30] In evidence to the Senate Committee an officer of AGD said that there are relatively few people with the same name and DOB, an assertion that is supported by Australian Electoral Office figures.

about the inclusion of individual's personal information on the register. While there was acknowledgement of the proposed measures to improve privacy, and of the clarification of some aspects of the operation of the register, including that most individual personal property would be identified by serial number alone meaning there will be a relatively small population affected, (see section 3.3 above), CALC and the APF in particular remained of the view that the preferable approach would be to exclude personal information from the register. The potential to disadvantage sole traders, whose personal property would under the current definitions in the PPS Bill, be classified as consumer property was noted. However, CALC suggested the solution here would be to clarify the distinction between consumer and commercial personal property, possibly by mandating the use of Australian Business Numbers (ABNs) and then to identify personal property that could not otherwise be identified by a serial number by an ABN.

CALC also considered separately the inclusion of DOB. CALC and the APF continue to oppose the inclusion of DOB. Concerns noted include that an individual wishing to sell an item of personal property may need to give their DOB to a prospective purchaser who would not otherwise have this information. CALC and the APF hold the view that there are viable options, including search on name refined once results were returned by reference to the description of the security.

Findings and Recommendations

IIS notes that the June 2009 PPS Bill provides that if the collateral is consumer property, and is required by the regulations to be described by serial number then no grantor details can be placed on the PPSR.[31] Where consumer personal property cannot be identified by serial number the June 2009 PPS Bill specifies that the only grantor details that may be provided to the PPSR are name and DOB.[32]

IIS supports these positions and in particular welcomes the step to specify the personal information that may be included on the PPSR in the primary legislation rather than in regulations.

IIS agrees that there are some privacy risks in including an individual's name and DOB on the PPSR. IIS notes that it is highly unusual in the Australian context for a register to make DOB details available. However, it is also important to note here that the PPSR does not allow anyone's DOB to be "looked up".

It is not easy to quantify or to assess the specific likelihood of privacy risks arising. It is also the case that there are potential economic benefits to the community as a whole and to individuals concerned if the PPSR facilitates appropriate borrowing that may not otherwise have proceeded. However, again is it difficult to quantify how much of the expected benefits may flow from the inclusion of personal property that cannot be identified by serial number and that may be related only to borrowing for domestic or personal reasons.

[31] S.153 June 2009 PPS Bill

[32] S.153 June 2009 PPS Bill

On balance IIS considers that it is reasonable for the PPSR to include name and DOB in the limited circumstances specified in the June 2009 PPS Bill. In reaching this view IIS notes the following factors that it considers mitigate the privacy risk:

- While the PPSR may contain an individual's name and DOB this information will not be accessible unless the searcher already knows both these details – in other words it will not be possible to use the register to find out any of this information about an individual (although if name and DOB are known it would then be possible to find out about any property the individual has offered as security and the details of the secured party);
- The fact that there will be a fee charged for all searches which while likely to be relatively low seems likely to discourage searches simply on the basis of casual interest, if other measures to prevent this sort of search fail, or attempts at bulk downloads;
- AGD advises that alternatives including searching on name and description of the security are not considered practicable, for example because of the range of possible personal securities and the difficulties in constructing reliable searches of free text;
- While it is the case that potential purchasers of personal property may request name and DOB so that they can search the PPSR the decision to provide this information will be under the individual's control and the $5000 threshold for acquiring personal property free of security interests suggests that it is unlikely that a PPRS search would be conducted for smaller consumer items;
- Excluding consumer personal property that cannot be identified by serial number from the PPSR may mean there will be individuals, both sole traders and individuals in a domestic or personal capacity, who will lose some ability to borrow;
- Finding a way to limit the impact on sole traders, for example as suggested by CALC by revising the definition of consumer personal property, would still leave a group of individuals in a domestic or personal context who may have less opportunity to borrow against their personal property, also a sole trader may have two or more ABNs, making any solution dependent on ABNs unworkable;
- If DOB is not included, a search on name only would return information about all people with the same name exposing more individuals to risks including privacy risks;
- The stronger privacy protection regime in the June 2009 PPS Bill including civil penalties in more areas.

IIS considers that it will important to keep the privacy impact of the PPSR under review at least in its initial implementation, in particular in relation to the impact of including name and DOB; it notes that the June 2009 PPS Bill provides for a review after 3 years.[33] As noted in the discussion above there is also interest in including address or some elements of address, on the PPSR. IIS considers that there may be risks and benefits in both options. It considers that any decision to include additional elements should be based on actual experience and a further PIA.

[33] s.343 June 2009 PPS Bill

IIS also considers that in making an assessment of privacy impact an important consideration will be the categorisation of personal property as either consumer or commercial property. As noted above, the June 2009 PPS Bill defines consumer property "personal property held by an individual, other than personal property held in the course or furtherance, to any degree, of carrying on an enterprise to which an ABN has been allocated".

CALC and the APF consider that this definition is likely to mean that personal property that has some personal, household or domestic use will nevertheless be categorised as commercial. They argued for consideration of alternatives, for example a definition that looks at dominant use, rather than any use.

The protections for individual grantors are generally the same regardless of the categorisation. For example, failure to provide a verification statement, conducting an unauthorised search or using information obtained as a result of a search for an unauthorised purpose could constitute an interference with privacy whether or not the personal property is consumer or commercial. The civil penalties applying to unauthorised searches or use would also apply. However, the limitation on including a grantor's name and DOB where the property can be identified by a serial number only applies for consumer property. In other words, a listing for commercial property could include a serial number and details about the grantor as permitted by regulations (the Regulation DP indicates these details would be name and DOB).

IIS considers that the possible impact of the commercial/consumer distinction is an area where it is difficult to draw a clear conclusion about the possible privacy risks and what measures may be needed, but on the face of it do not appear significant. It suggests that this is an issue that should be examined in the 3 year review of the PPS Act.

Recommendation 1 – IIS recommends that the 3 year review of the PPS Act consider the impact of the operation of the PPSR on individual grantors' privacy, in particular in relation to the inclusion on the PPSR of name and DOB for grantors in relation to consumer securities and any impact arising if the definition of commercial property means that property which is used predominantly for personal, domestic or household purpose is nevertheless able to be categorised as commercial property.

Recommendation 2 – IIS recommends that any proposals to include additional personal information in the PPSR beyond that permitted in the June 2009 PPSR Bill should be subject to a published PIA before a decision is made to amend the legislation.

4.1.2 INCLUSION OF PERSONAL INFORMATION ON THE REGISTER BEFORE SECURITY TRANSACTION IS COMPLETE

The PPS Bill provides for a registration to be made before the security transaction is completed and the transaction may never be completed. This means that a person may appear on the register without ever having taken out the loan he or she had been negotiating. In its submission, the AFC notes that its members advise that up to 20% of approved finance applications do not proceed to settlement.

The benefits of enabling a secured party to register a security interest before the transaction is complete are that it would enable the secured party to know its order of registration (and,

subsequently, its priority in the event of bankruptcy or insolvency) and would enhance business certainty.[34] On the other hand, AFC points out that registering a purchase money security interest at the time of finance approval would necessitate a significant and unproductive operational burden on financiers in removing non-settled registrations and would increase the amount of traffic and data on the register.

If the secured party is subject to the Privacy Act, the organisations will have an obligation to provide at least general notice of disclosure to the PPSR. However, If the secured party is not covered by the Privacy Act, for example, the secured party is an individual, small business or political party, there may be currently no obligation on the secured party to tell the grantor that the information collected will form part of the register. Under the PPS Bill, the grantor would be notified of registration only after it had occurred.

The risk is that, pre-settlement registration may introduce privacy risks to the individual inherent in being included on a public register unnecessarily and possibly without notice, until after the event.

This raises the question whether the PPS Bill should include an obligation on the part of the secured party to give prior notice of intention to register a security interest. It also raises the question whether a secured party who registers a PPS before completing the relevant transaction should be under a statutory obligation to remove the registration within a specified timeframe if the transaction does not go ahead. Notice requirements are considered in more detail in the next section.

Findings and Recommendations

This issue has since been addressed in the June 2009 PPS Bill which places an obligation on a secured party to remove a registration as soon as practicable or within five days whichever is earlier if they cease to have a reasonable belief that collateral secures or will secure and obligation. A civil penalty applies for failure to comply with this section. [35]

IIS finds that this is reasonable response to this issue and has no further recommendations here.

4.1.3 NOTICE OF INCLUSION ON THE PPSR

In recognition of the fact that individuals will be in a stronger position to be in control of personal information about them if they know what is happening to that personal information, privacy principles generally require organisations collecting personal information to make sure the individual concerned is aware of the collection, how the personal information will be used, to whom it may be passed on etc.

The RC notes the critical importance of notification procedures. It states that all people named in the register, particularly individuals, must have every opportunity to know about information that might affect their capacity to sell personal property and/or to secure finance.[36] The PPS Bill provides that when a registration is made, amended, removed or restored, the Registrar must inform the secured party by giving it a verification statement.[37] The secured party must notify the grantor as

[34] RC, para 10.46
[35] June 2009 PPS Bill s.151(2) and (3)
[36] RC para 10.99.
[37] PPS Bill s.223

soon as is reasonably practicable. Failure to do so does not alter the effectiveness of the security. [38] If the secured party fails to notify the grantor, an action for damages may be available to the grantor.[39]

If the Privacy Act applies to the secured party (that is, the secured party is not an individual, a small business to which the Privacy Act doe not apply or a political party) the NPPs will also apply. This would require the secured party at or before the time (or if that is not practicable, as soon as practicable after) it collects the information to take reasonable steps to ensure that the grantor is aware of, among other things, the purposes for which the information is collected, the organisations to which the organisation usually discloses information of the kind and any law that requires the particular information to be collected.[40]

Submissions addressed two main issues.

- On whom should the notification obligation lie?
- When should the grantor be notified that his or her personal information may be included on the register, before registration, or after?

In its submission, the AFC is concerned with business efficiency. It suggests that, consistent with the efficiency and effectiveness of the register, there is considerable interest in the register itself providing the facility through which notice can be given or responded to. This could be encouraged, in its view, by encouraging secured parties to establish and use a standard format and a dedicated electronic address.

In its submission to the Senate Committee, the VPC suggests that consideration should be given to making the Registrar responsible for giving notice to grantors. It suggests this because, as there would be no minimum threshold amount for registration, pawn brokers and small moneylenders, who are not bound by the NPPs, would be able to register their interest.[41] In its submission, the OPC suggests that the notice should come from the Registrar, not the secured party, and should be consistent with the provisions of the Privacy Act. It also considers that the notice should state why the information is being recorded on the register, what laws give authority to record it and that the information will be publicly available. If the notification function were to rest with the Registrar, however, the register would need to collect more information, in particular address details, whether or not the additional information were made publicly available. In consultations in the course of this PIA the, OPC noted that, for this reason, it is better on balance that the notification obligation should rest with the secured party.

OPC and WLS Vic suggest that the grantor should be notified before registration, as well as after. Prior notice, which the Centre considers should include specific details of information to be included on the register, would ensure that grantors know that their personal information would be

[38] RC para 10.107
[39] PPS Bill s.236
[40] NPP 1.3.
[41] There is, however, little incentive for a secured party to register such an interest because the Bill would provide that third parties take personal property free of a security interest when it is not serial numbered, predominantly used for domestic purposes and its value at purchase, and the price paid for it, are below $5 000.

accessible (OPC). Notification before registration would enable women to assess the safety implications of their names and dates of birth appearing on an easily accessible register (WLS Vic).

In consultations in the course of this PIA privacy regulators and privacy and consumer advocates again expressed a preference for notification both before and after registration. There was some discussion about whether the notice obligation in the NPPs would suffice as the source of obligation for the pre-registration notification.

NPP 1.3 requires organisations to

> At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:
>
> a. the identity of the organisation and how to contact it; and
> b. the fact that he or she is able to gain access to the information; and
> c. the purposes for which the information is collected; and
> d. the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and
> e. any law that requires the particular information to be collected; and
> f. the main consequences (if any) for the individual if all or part of the information is not provided.[42]

The APF considers that NPP 1.3 would not require a specific mention of the PPSR. For this reason and the gaps in coverage of the Privacy Act noted above for small business organisations etc, its preference is that the PPS legislation should contain a pre-registration notice obligation on secured parties.

These groups also considered that the option for grantors to pursue damages in the event that a secured party does not give them a copy of the registration certificate was an inadequate remedy. Both the APF and CALC considered there should be a civil penalty. They also considered that regulators should have an active role in monitoring performance in relation to notice obligations wherever they sit and that there should be additional regulatory options including barring access to the PPSR where a secured party continually fails to comply with obligations.

Findings and Recommendations

With respect to the timing of notice of inclusion IIS agrees that both prior notice of registration, and confirmation of registration after the fact, is important from a privacy perspective.

IIS understands that AGD considers that NPP 1.3(d) provides an obligation for bodies to which the NPPs apply to advise individuals specifically of the disclosure to the PPSR.

IIS considers that if this is the case then the combination of a NPP 1.3 notice and the provision of a verification statement following registration appear to provide individuals with a reasonable level of notice in the circumstances. However, this solution will only apply where secured parties are subject to the Privacy Act. The Privacy Act exempts some small businesses from it coverage and also would not apply in domestic contexts, for example where a loan to a family member is secured by personal property and that interest is registered on the PPSR.

[42] NPP 1.3 Schedule 3 of the Privacy Act available at http://www.privacy.gov.au/publications/npps01.html#npp1

IIS considers that the obligation to advise individuals of a proposal to register a security interest in relation to consumer property where the registration would mean the individuals name and DOB appears on the register should apply in all cases, whether or not the Privacy Act would otherwise apply.

Recommendation 3 – IIS recommends that secured parties proposing to register a security interest in consumer property where the registration will include an individual grantor's name and DOB be obliged to first advise the individuals concerned of the disclosure of personal information to the PPSR. To the extent that this obligation would not be satisfied by a secured party's existing obligation under the Privacy Act, IIS recommends that the PPS Bill should provide that failure to provide prior notice of a registration that relates to consumer property and would include name and DOB is an interference with privacy under the Privacy Act.

IIS notes that the June 2009 PPS Bill contains an additional remedy for individuals where the secured party fails to provide a copy of the verification statement to the grantor where a PPSR listing would include personal information. The Bill now provides that a person to whom the Registrar gives a verification statement must provide a copy of the statement to the grantor concerned and that failure to do so will constitute an interference with privacy under the Privacy Act.[43] The provision is designed to apply regardless of whether the secured party would otherwise be subject to the Privacy Act and means that the grantor concerned would be able to pursue a complaint to the Privacy Commissioner. IIS welcomes this additional remedy. IIS considers that ensuring that individuals are aware of the fact that their details have been included on the PPSR is of critical importance. It notes the comments by privacy and consumer advocates that the availability of remedies, such as seeking damages, or pursuing a complaint to the Privacy Commissioner, depends on the individual becoming aware that they have not received a statement and being in a position to pursue a complaint or damages. As noted IIS considers that the combination of prior and post notification is likely to be effective. However it considers that this is an area that should be monitored by the Registrar and considered closely in the context of the proposed 3-year review of the PPS Act.

Recommendation 4 – IIS recommends that the 3 year review of the PPS Act assess whether any obligation on secured parties under the Privacy Act and the PPS Act to provide prior notice of disclosure of personal details to the PPSR is sufficient to ensure individuals are in a position to make informed choices about proceeding with a credit application and whether these obligations are being fulfilled, or additional enforcement measures such as civil penalties, are needed to ensure that secured parties meet these obligations.

4.2 SECURITY OF PERSONAL INFORMATION

This section of the PIA considers the security of personal information in the context of the PPS project. NPP 4 in the Privacy Act requires organisations to take reasonable steps to protect personal information from misuse and loss and from unauthorised access, modification or disclosure.

[43] June 2009 PPS Bill s.157

4.2.1 SEARCHING THE PPSR: HOW

This section of the discussion focuses on the process of searching the PPSR as a security issue. Section 4.4 below considers the purposes for which the PPSR may be searched, and how personal information obtained in searches can be further used.

The RC states that persons searching the register for serial numbered goods, for example, motor vehicles used for consumer purposes, would be able to search the register by reference to the serial number only, as is already the practice in some State registers, for example, REVS and VRS, that do not record grantor details. [44] It also states that while the search criteria to be prescribed by regulation are not yet settled, it is proposed that a person would be able to search the register by reference to the unique identifier of the registration.[45]

If the collateral does not have a serial number or unique identifier, a register search would be made by reference to the grantor's details, that is, the grantor's unique identifying number (such as a company's ACN) or, if the grantor is a natural person, his or her name and DOB. The register search function would allow users to refine their searches according to their needs, for example, by searching against a grantor and a particular class of collateral.[46]

AGD reports that the register is being developed to allow only direct match searching. Thus, when a search is made by reference to an individual secured party's or grantor's details, data would be returned only when the search information entered is exactly matched. In the case of an individual grantor this would require the searcher to enter the grantor's first name, last name and DOB. It would not be possible to enter a name and have the DOB returned.

There are potential privacy risks inherent in a system that is intended to provide low cost, fast and accessible search facilities. In particular, there are potential privacy risks to individual grantors whose collateral cannot be described by a serial number. A person who searches the register by reference to an individual's name and DOB may find that a finance company or other institution has taken security over various items of personal property. Inferences, accurate or not, might be made about the grantor's financial situation. If, for example, security were held over a large number of valuable paintings, or a collection of valuable jewellery, it may be felt worthwhile to consider ways of tricking the grantor into handing over the property or even burgling the house. Alternatively, a credit provider might infer from the existence of a security over a person's personal property that the person would not be a not a good credit risk. Although only relatively few people share the same name and DOB, there is a potential for inaccurate conclusions to be drawn about a person who happens to share the same name and DOB of someone on the register.

A number of submissions to the Senate Committee address the issue of search criteria in relation to individual grantors. At least one commercial submission suggested that multiple matches and search criteria were needed (Australian Institute of Credit Management). Veda suggests that periodic bulk access should be allowed. Other submissions, however, suggest that the search criteria should be limited. CALC contrasts the search provisions in the PPS Bill with similar repositories of personal information, including credit information files, telephone number listings

[44] RC Para 10.112

[45] RC Para 10.113, also at the time of registration, secured parties would be able to enter a unique number (or unique identifier) devised by them in relation to a particular registration (RC, para 10.24).

[46] RC Para 10.114-10.115)

(which can be silent) and electoral rolls. Several submissions say that searches in relation to individual grantors should be by serial number, not by name (APF, CALC), certainly where this is possible (WLS Vic). Others say DOB should not be included (for example, because name and DOB would allow the searcher to go on a fishing expedition (WLS Vic)), or, if so, the search should be on a challenge-response basis, rather than returning actual DOB (OPC). At least one submission focuses on IT issues. The Australian Bankers' Association Inc (ABA) believes that a key element to the success of the new system will be the successful interfacing between banks' IT systems and the online register.

Table 3: Collated comments on searching the register

Search criteria	Comments collated by IIS based on views expressed in submissions
Serial number only	Personal information is protected because it is not available but not possible to search for encumbrances on property that does not have a serial number.
Name and DOB	This would allow for searches where there is no serial number or unique identifier.
Serial number, if applicable, and name only	This would limit personal information available and significantly limit possible misuse. However, depending on how many securities there are that do not have a serial number this may reduce effectiveness of the register.
Serial number, if applicable, and name and DOB	Despite possible "twins" issue, name and DOB limits grantor to only one possible person in most cases. It would therefore give potential security holder or vendor of goods maximum protection. The cost is, however, to the privacy of the grantor, who is more or less uniquely identified.
Serial number, if applicable, and name, DOB and address	It is difficult to see how this improves the potential security holder or vendor's protection. However, it would constitute a serious privacy risk to the grantor whose details would be accessible to anyone at any time. It would also pose serious risks to the safety of people fleeing violence.

The criteria for searching the register are of considerable importance to lenders and to consumers. It is clearly in the commercial interests of lenders that the criteria are broad enough that they can accurately identify personal property that is already secured and the owners of that property. The success of the PPS reforms depends on this. On the other hand, safeguarding the privacy of individuals is important, not only to the individuals themselves, but to the integrity of the scheme. These competing interests require that a balance be found between the interests of business and individuals.

Findings and recommendations

In IIS's view, and subject to the other recommendations in this PIA, inclusion of name and DOB in the Register and the corresponding search restrictions seem to find an appropriate balance. Measures are provided to minimise the number of times a search requires name and DOB rather than serial

numbers. Searchers are required to enter data that they already know and only get a return on an exact match. Moreover, where search based on details of the grantor is undertaken, name and DOB is a measure that helps protect the privacy of grantors of the same name who are not relevant. Ensuring that a search can be made only on an exact match basis will help ensure against fishing expeditions in the register. IIS also notes that where regulations require consumer personal property to be registered by its serial number, no information about the grantor will be included on the register. In other words, for consumer property a search of the PPSR by serial number will never return results including grantor details.

IIS notes that s.171 of the June 2009 Bill specifies the search criteria which can include grantor details but only as they can be included on the PPSR under s.153.

IIS is satisfied with the approach in the June 2009 Bill and has no further recommendation here.

4.2.2 Data Retention

As noted at section 3.3 above, it is difficult at this point to estimate the number of individuals whose details may be included on the PPSR. However, over the years this may amount to a very large collection of information about an individual identifiable by name and DOB, and will include some information about their financial history. The PPS Bill does not provide for the destruction of this information after it has been deleted from the register, or after a period of time. Instead, it provides that the removal of data from the register does not prevent the Registrar from keeping a record of the removed data in whatever form the Registrar considers appropriate. [47] The IPPs, unlike the NPPs that apply to private sector organisations, do not require the destruction or de-identification of personal information no longer needed.

The existence of such a large, historical database may give rise to privacy risks to individuals whose personal information continues to be stored long after it has become irrelevant.

In addition, as noted at section 3.4.2 above, the intention is that all transactions, changes etc to the PPSR will be logged. Again, over time audit logs could contain significant information about an individual's interactions with the PPSR.

Findings and recommendations

IIS appreciates that there may be sound reasons to retain historical records of the PPSR, including audit logs. However, while personal information is held it can be used or misused for new or unwelcome purposes.

Recommendation 5 – IIS notes that the AGD is now working on a records management framework as required by the *Archives Act 1983* for the PPSR and recommends that it include as a principle in the framework that personal information be held for the minimum time possible once a registration is no longer active.

4.2.3 Security of the PPSR

As noted at section 3.4.2 above, IIS has considered the approaches AGD is adopting to protect information including personal information held on the PPSR. IIS notes that the PPSR is still in an

[47] PPS Bill s.218

early stage of development and there are decisions yet to be made about the content of regulations and about elements of the system operation and design. IIS considers that the approaches taken to date are consistent with AGD's obligation under IPP 4 of the Privacy Act to take reasonable steps to protect personal information. However, it considers there should be security risk assessments and privacy audits undertaken as the PPSR implementation proceeds- this issue is addressed in recommendation 15 below.

4.2.4 Potential for inclusion of personal information on the PPSR to contribute to ID theft or fraud

A question raised in submissions and in evidence to the Senate Committee was the potential for an individual's name and DOB included on the PPSR to increase the risk of identity theft or identity fraud. There is not a clear answer here. IIS considers that the PPSR is unlikely to be a "preferred source" of information for these nefarious purposes (the limited information held on the PPSR, the requirement for prior knowledge of search term, the fee to search, and the fact that there is some record of all transactions mitigates against this). IIS understands that AGD is of a similar view. However, it is not impossible that the PPSR would be used in this way. IIS considers that an important protection will be to ensure that individuals are aware that their details may be included on the PPSR and what this means so that they then can make informed choices about whether or not to proceed to borrow. It considers that the Registrar should include this information in PPSR education and information campaigns and that the Registrar should monitor the possible misuse of the PPSR as source of information in ID fraud or theft activities.

Findings and recommendations

On the evidence available at this time, IIS considers that the PPSR is unlikely to be a "preferred source" of information but that this needs to be monitored closely.

Recommendation 6 – IIS recommends that the Registrar should ensure that public information and education about the PPSR should include information about its availability for searches and that the Registrar should monitor the potential for the PPSR to be used as source of information in ID fraud or theft activities.

4.3 Accuracy and Amendment

This section of the PIA sets out issues to do with the accuracy of the personal information held on the PPSR and the ability for individuals (and others) to seek amendment to registrations. Accuracy of information, and the ability to seek correction to information that is not accurate are important aspects in ensuring that the handling of personal information is privacy protective. IPPs 7 and 8 in the Privacy Act set out obligations for agencies that include taking reasonable steps to make sure personal information is accurate, up-to-date and complete and to respond reasonably to requests for alteration or correction.

4.3.1 Accuracy of name and DOB details

As has been noted elsewhere in this PIA, there is no obligation on secured party to register a security interests although there are incentives for them to do so. Where a registration proceeds, the secured party is generally responsible for its accuracy, with obligations in this regard under the Privacy Act if it applies.

IIS notes that submissions from the business community have expressed some concern about the potential for registrations to be inaccurate, particularly as far as spelling or variations in names or in relation to the entry of serial numbers. The PPS Bill, proposed regulation and the proposed operation of the PPSR include a number of measures to help ensure registration are accurate, including checking serial numbers against other registers, such as NEVDIS, and requiring secured parties to enter a grantor's details in the same form as a number of specified sources (for example as it appears on a drivers' licence).

A grantor concerned about the accuracy of a registration could pursue the issue directly with the secured party concerned. If the matter is not resolved they may then pursue a complaint with the OPC or in some circumstances, could make a demand for amendment of the registration to the Registrar.

Findings and recommendations

IIS considers that there is some possibility that there would be overlap in a grantor's right under the Privacy Act and the PPS Bill to seek an amendment to a record.

Recommendation 7 – IIS recommends that the Registrar and the Office of the Privacy Commissioner monitor the nature of concerns about accuracy or correction matters in relation to the PPSR raised with them and that they meet periodically to consider if there is a need for additional information or other measures to ensure that individuals can most effectively pursue their concerns.

4.3.2 MANAGEMENT OF HISTORICAL REGISTER RECORDS

As a Commonwealth agency, the Registrar will be subject to the Privacy Act and the IPPs, in particular IPP 4, governing storage and security of personal information.

The PPSR will replace approximately 40 existing Commonwealth and State and Territory electronic and paper based registers that exist for the purpose of recording security interests in personal property, for example, motor vehicles. The information that is contained in existing registers will be migrated to the PPSR. It is expected that when the PPSR begins operation it will contain about 4.7 million registrations migrated from existing registers. About 97% of these registrations will relate to motor vehicles or company charges. In neither of these cases will the registrations contain information about individual grantors. However, it is possible that some of the remaining 3% of registrations to be transferred to the PPSR would include the personal information of grantors whose personal property cannot be identified by a serial number.

Findings and Recommendations

IIS understands that the personal information transferred from the records in historical registers may not include much "consumer information"; where it does this is likely to be in relation to co-operatives, crops liens or bills of sale. IIS also understands that AGD is expecting the data will be cleansed before it is migrated to assist in ensuring that migrated data is as current and as accurate as possible when the PPSR commences operation.

While one option of responding to any accuracy issues (and to ensure individuals are aware that their details may appear on the PPSR) would be for the Registrar to contact each individual, this would not be possible as, appropriately, the Registrar will not hold any contact details for grantors.

IIS considers that the privacy risks in the data migration process are likely to be small. However, it encourages the Registrar to consider advice to individuals in publicity and education campaigns associated with the introduction of the PPSR.

Recommendation 8 – Recognising that it will not be possible for the Registrar to directly notify individuals whose details are migrated from existing registers to the PPSR about the operation of the register, IIS recommends that the Registrar include information in any publicity and education campaigns about the PPSR encouraging individuals to check the PPSR and to seek amendment if appropriate.

4.3.3 AMENDING THE REGISTER WHERE A REGISTRATION DOES NOT PROCEED

There are circumstances when registration of a security interest is no longer appropriate. The loan may have been repaid; in fact, the loan might never have been made. (A secured party can register a security interest before it attaches to the property.) The PPS Bill provides for four circumstances in which the Registrar would be able to amend the register:

- on application by a secured party
- following an amendment demand and an administrative process
- following an amendment demand and a judicial process or
- to correct an error or omission made by the Registrar.[48]

When the time comes, for example that, the loan is repaid, the secured party is required to end the registration of a consumer good or serial numbered property within five business days.[49] If this were not done, a consumer would have two remedies: he or she could follow an amendment process provided for in the Bill, or could sue for damages. The amendment process involves making a written demand to the secured party for amendment and, if the secured party fails to amend within five business days, pursuing an administrative or a judicial process for amendment.

As noted above, a lender may register a security interest in personal property before the security agreement has been completed. This gives the secured party a degree of protection during the negotiation period. If the loan does not proceed, however, and the registration is not removed, the other party (the would be borrower) may be seriously disadvantaged. He or she may approach another lender, which, on searching the register, would find a prior security already there.

Few submissions address amendment of the register. WLS Vic suggests that the provisions are more favourable to secured parties than to grantors. Legal Aid Queensland (LAQ), however, describes this process as "vitally important" to grantors because it sets out a clearly defined process by which a grantor would be able to seek to have the register amended. It notes, however, that a grantor trying to sell property may not have enough time to go through that process. As a result a contract for sale may be held up or fall through because the registration has not been amended in a timely manner. In LAQ's view, if a secured party fails to respond to an amendment demand on time, the secured party should be subject to a fine.

[48] PPS Bill s.201
[49] PPS Bill s.206

The privacy risk to a person seeking to borrow money arising from a secured party's failing to apply to amend the register to remove a security interest that did not eventuate is such that there should be an obligation imposed on the secured party to do so and to do so as soon as possible after negotiations for the loan have ended. The PPS Bill should specifically provide for this.

Findings and Recommendations

As noted at section 4.1.2 above the June 2009 PPS Bill provides a clear obligation on the secured party to remove a registration that has been made before the security agreement is complete but where the security is subsequently not actually needed, for example no subsequent loan is made that requires that security.

IIS does not have further recommendations here.

4.4 USE AND DISCLOSURE OF PERSONAL INFORMATION ON THE REGISTER

This section of the report considers the use and disclosure of personal information contained on the PPSR. IPPs 10 and 11 in the Privacy Act set out provisions to ensure that personal information is only used for the purposes for which it was collected unless a specified exception applies and is not disclosed in circumstances the individual would not expect unless a specified exception applies.

4.4.1 PPSR SEARCHES – PERMITTED PURPOSES AND USES

The PPS Bill provides that anyone can apply to the Registrar to search the register. The Registrar must give the person access as long as the search is authorised, is in the approved form, the fee paid and access is not prohibited by the regulations.[50]

IIS understands that there will be essentially two regimes applying to searching the PPSR. Effectively there are no limits on the reasons for a search on criteria other than an individual's details (as noted above, these searches will not return personal information). The PPSR is in general intended to support the transparency of the market and AGD advised it would be more difficult to meet this objective where searches are limited by purpose.

Where searches will reveal personal information about individual, there is a need to balance the objective of transparency of the market with the possible impact on individual privacy. The key to achieving this balance adopted in the PPS Bill is to permit searches only where authorised.

A search is authorised if it is for one of a long list of purposes in the Bill. These include:

- For a secured party or a grantor, a purpose that relates to a security interest attached to collateral described in the registration;
- Establishing whether to provide credit etc to someone; and
- For the holder of a lien or charge or a creditor, a purpose that relates to enforcement of the lien or charge, or the creditor's rights.[51]

[50] PPS Bill s.225

[51] PPS Bill s.227(1), items 2,3, 7 and 19

The Bill provides that, except for the purpose specified, a person must not search the register or use data obtained as a result of searching it, unless the data has been lawfully obtained from another source.[52] A person who breaches this obligation would be liable to a claim for damages. Furthermore, an unauthorised search by an agency or organisation to which the Privacy Act applies would amount to an act or practice interfering with the privacy of an individual, and remedies under the Privacy Act may apply.[53]

The June 2009 PPS was amended to provide that these provisions apply regardless as to whether the Privacy Act would otherwise apply to the activity.[54]

AGD advises that functions are being built into the register which would assist the Registrar identify suspicious search activity. It also advises that, in addition, criminal penalties would apply. Anyone searching the register would be required to confirm they are searching for an authorised purpose; if not, he or she would be liable to a criminal penalty under the Criminal Code Act 1995 for knowingly making a false declaration to the Commonwealth.

A number of submissions address this issue. APF believes that the scope of "authorised purpose" is too broad. As CALC points out anyone can purport to have an authorised purpose for a search; it considers the possibility of a criminal penalty would not be much of a deterrent as it is unlikely that the offence would be known about or in one-off cases at least prosecuted.

On the other hand, Veda suggests that the Registrar should have the power to add to the list of people who are entitled to search the register. However, if an unauthorised search takes place and the grantor becomes aware of this, the only remedy provided by the Bill is a claim for damages. OPC suggests that there should be a warning notice to users of the consequences of making an unauthorised search.

Requiring every person making a search of the register to confirm that they are doing so for an authorised purpose and advising them of the consequences of making a false declaration would certainly act as a reminder of the limits on searching the register and as a deterrent against making an unauthorised search. While IIS notes that in the consultation process on this PIA CALC was not convinced this measure would be of value, it understands that AGD expects this could be a mechanism to pursue large-scale misuse or fraudulent use of the PPSR.

IIS also notes that CALC and the APF expressed some reservations about the list of permitted searches in the June 2009 PPS Bill.[55] In particular, the APF and CALC were concerned that the item 7 and 8-10, which expressly provide for searches to find a named individual with an interest in personal property in relation to making decisions about providing credit, or to make investment decisions, conflict with the credit reporting provisions in part IIIA of the Privacy Act.

[52] PPS Bill s.227(1) and s. 227(2)
[53] PPS Bill s228, RC, para 10.120-10.121.
[54] June 2009 PPS Bill s. 173(2)
[55] June 2009 PPS Bill s.172

Findings and Recommendations

IIS has considered the specific question of the use of the PPSR to make decisions about whether to grant credit in the following section 4.4.2 below. It considers that it would be desirable to make reference to the possible criminal sanctions for making a false declaration in the PPS Bill but that if this approach is not adopted then the Registrar should ensure this protection is included in the PPSR design.

Recommendation 9 – IIS recommends the PPSR be designed so as to ensure that every person making a search of the register is asked to confirm that they are doing so for an authorised purpose and advising them of the consequences of making a false declaration about the nature of a proposed search.

4.4.2 PPSR AND THE CREDIT REPORTING PROVISIONS IN PART IIIA OF THE PRIVACY ACT

Credit reporting agencies essentially provide services to credit providers to assist them to manage credit risk, including by collating lists of loan defaulters. Part IIIA of the Privacy Act regulates such credit reporting databases and provides safeguards for individuals in relation to "consumer" credit reporting. In particular, Part IIIA governs the handling of credit reports, which are essentially about individuals' defaults where outstanding for over 60 days, and other credit worthiness information about individuals by credit reporting agencies and credit providers. The Act ensures that the use of this information is restricted to assessing applications for credit lodged with a credit provider and other legitimate activities involved with giving credit.[56]

Among the purposes for which a person may search the register under s 227 is the purpose of establishing whether to provide credit to, or obtain a guarantee or an indemnity from, an individual who may be on the register. In its submission, OPC suggests that the results returned from such a search may be considered a "report" as defined under s 18N of the Privacy Act, which limits disclosure by credit providers of personal information contained in reports relating to creditworthiness.

Under s 18N(9) a report includes a credit report, or any other record of information, whether in written, oral or other form, that has any bearing on an individual's credit worthiness, credit standing, credit history or credit capacity, but not if the only information relating to individuals is publicly available information.

Privacy regulators and privacy and consumer advocates consulted in the course of the PIA expanded on this concern, querying if the use of the PPSR in some way undermined the strict protections that credit providers may obtain from credit reporting agencies for the purposes of assessing applications for credit. CALC and the APF considered that permitting searches for general decisions about lending was too broad. More specifically, they also considered that searches should not be permitted when making general decisions such as who to send credit marketing offers to. They sought a provision similar to that recommended by the Australia Law Reform Commission (ALRC) in its 2008 review of privacy law to the effect that the use of credit reporting information for direct marketing purposes should be prohibited, including the use of information for pre-screening – where lenders use the information to "exclude" individuals from their direct marketing offers list of

[56] See the Privacy Commissioner's website at www.privacy.gov.au/act/credit/index.html for information about the credit reporting provisions and Part IIIA of the Privacy Act.

names, rather than for genuine credit assessment.57

Findings and Recommendations

IIS agrees that there are similarities between the PPSR and credit reporting databases in that both hold personal information that could be used to assess credit applications. It notes that financial and credit information is generally considered to be very sensitive and that misuse of such information can have a significant impact on individuals, particularly those who are vulnerable and less able to negotiate the credit system.

As noted above, submissions have raised the question as to whether information obtained from the PPSR would be considered "credit worthiness" information and therefore subject to s. 18N of the Privacy Act. IIS understands from AGD that it has the view that this would not be the case. IIS has therefore not specifically considered that provision here. Rather, IIS has considered the issues from the perspectives of the privacy risk that could arise if information from the PPSR is available to be used broadly to assess credit applications and the privacy protection frameworks of the two systems. To assist in this analysis IIS has considered some of the key features of the two systems; these are set out at Appendix 3.

IIS notes that personal information about individuals held on credit reporting databases is considerably more sensitive and detailed than that held on the PPSR; it includes current and historical address information and information about failure to make loan repayments. On the other hand, the PPSR contains some information that credit reporting agencies are prohibited from including in credit reporting databases; that is details of personal property offered as security and details of credit providers where there has been no default. However, IIS notes that the ALRC has recommended that, subject to certain preconditions, credit reporting agencies be permitted to include some information about current credit providers in credit reports whether or not there has been a default.[58]

The purposes for which, and the people or organisations that may, access the PPSR and credit reporting databases in assessing credit applications are similar. Access to the credit reporting databases, and use and disclosure of personal information obtained from databases is more closely enforced; credit reporting agencies have strict obligation to limit access to their databases to credit providers and other permitted people and there are significant criminal penalties, ranging from $30 000 to $150 000 for unauthorised use or disclosure of credit reporting information, providing false or misleading credit reports, or unauthorised access, including by false pretences, to credit reports.[59] However, as noted, these stricter provisions protect such sensitive information as an individual's current address and the fact that they have defaulted on a loan.

Overall, the protections applying to the two systems (as summarised in Appendix 3) are similar. One variation IIS observes is the obligation on credit providers to advise individuals if a decision to deny credit is based on information in a credit report. However, IIS notes that this provision in the Privacy

[57] For Your Information: Australian Privacy Law and Practice (ALRC 108) Recommendation 57-3 available at www.austlii.edu.au/au/other/alrc/publications/reports/108/57.html#Heading225

[58] For Your Information: Australian Privacy Law and Practice (ALRC 108) Recommendations 55-1 – 55-5 available at www.austlii.edu.au/au/other/alrc/publications/reports/108/55.html#Heading592

[59] Part IIIA of the Privacy Act, s.18P, s.18Q, s.18R, s.18S and s.18T

Act acts partly as a prompt to allow individuals to ask what credit information is being held and, if necessary, to seek to correct it or to take other action. The PPS Bill already includes such a prompt; the verification statement from each secured party should mean that a grantor would already know what is on the PPSR.

While credit providers may use information from the PPSR to assist them to take decisions about credit, IIS understands that this is only one of the additional pieces of information that credit providers might rely on that does not come within the Part IIIA framework, for example information that is in the public domain. On balance, IIS has decided against suggesting an additional notification obligation at this point. However, it considers that the extent to which credit providers are materially using the PPSR to assist in decision making in relation to consumer credit should be tested as part of the 3 year review of the PPS Act.

IIS also notes that the permitted searches as set out in the June 2009 PPS Bill would not include searches for direct marketing activities. It also considers that, given the nature of the information on the PPSR and manner in which it can be searched, it is probably unlikely that the PPSR would be widely used for direct marketing activities. It is therefore not recommending an additional provision in the bill in this regard. However, IIS considers that it will be important for publicity about the PPSR to address the restriction on use of the PPSR, amongst other things, to obtain information for direct marketing purposes, and also that the review of the PPS Act should investigate whether it has been effective in ensuring that the PPSR is only used for permitted purposes.

Overall IIS considers that the more sensitive nature of personal information held in credit reporting databases is rightly protected by the provisions in Part IIIA and that the possible risks to individuals where the PPSR is used to make decisions about credit application are reasonably balanced by the protections already included in the June 2009 PPS Bill and in this PIA Report.

Recommendation 10 – IIS recommends that publicity about the PPSR should ensure that potential users are aware that searches of the PPSR in relation to consumer property, where the search criteria include individual's name and DOB, may only be conducted for permitted purposes, and these purposes do not include any direct marketing purposes such as the use of information for pre-screening of direct marketing lists. IIS also recommends that the review of the PPS Act should investigate whether the provisions in the Act have been effective in ensuring that the grantor details included in relation to consumer property is only used for permitted purposes.

4.4.3 LINKS TO OTHER DATABASES

The RC anticipates that the register may link with other databases, such as the NEVDIS, which would return information about whether a vehicle has been reported as written off or stolen.[60] Both OPC and VPC express concerns about data matching. VPC states that data matching between government databases for the purpose of data cleansing inevitably raises privacy concerns. Other databases may not be an accurate source of information. OPC recommends that the Bill should state that data matching with other databases should occur within well-defined parameters. It notes that it has itself issued voluntary guidelines for data matching by agencies and that its guidelines could form a basis for an appropriate privacy framework if there is any data matching between the register and other databases.

[60] RC Para 10.35

IIS agrees with the observations about the privacy risks in matching whole databases against other whole for databases for data cleansing or other purposes and that where relevant the OPC Data-matching guidelines should be applied. IIS understands that in the case of the PPSR the intention is to check aspects of individual registrations, for example the VIN, a company number or a boat registration number, to relevant registers in real time and to provide some information back to the secured party. This information may include confirmation or not that serial number is correct and some additional information about the personal property. In the case of motor vehicles this could include registration number, and vehicle colour and make.

In these circumstances IIS does not propose to make a recommendation in relation to this issue.

4.4.4 SUPPRESSING AN INDIVIDUAL'S PERSONAL INFORMATION

The PPS Bill foreshadows that there may be circumstances in which information on the PPSR should not be accessible. Section 225(3) provides that the Registrar must give a person who applies to search the register access to search the register if the search is authorised, the application is in the approved form, the fee paid and "access to the data is not prohibited by the regulations".[61]

In its PPS Discussion Paper: Regulation to be made under the PPS Act (Regulations DP) issued in August 2008, AGD proposes that access to data would be prohibited in two circumstances:

- an individual has applied to the Registrar to have data withheld because a court has ordered that it should be withheld from a search result, a court order provides sufficient basis on which to withhold data or other circumstances provide sufficient basis on which to withhold data and
- the Registrar considers in all the circumstances that it would be appropriate to withhold data.[62]

As has been set out elsewhere in this report, the PPSR contains relatively limited personal information. However, there are circumstances in which there may be very serious consequences for an individual in having some details available on register which effectively be searched by anyone who knows their name and DOB (as discussed elsewhere there may be civil or criminal penalties for an unauthorised search). For example, the possibility exists that the combination of the individual's name, the name of the secured party and/or the description of the personal property, could help to help locate an individual resulting in serious harm, up to, for example, the murder of a witness to a serious criminal offence, or violence against the children of a vengeful parent who has been denied access to them. In such circumstances the risks of access to the personal information on the register are so serious to the potential victims that they clearly outweigh the benefits to lenders, and potential lenders, of universal access.

Submissions to the Senate Committee address this issue. CALC suggests that a grantor should be able to apply to the Registrar to have his or her personal information suppressed. WLS Vic suggests that the Registrar should be able to deny access to a grantor's details from the outset. The VPC states that it is important that an individual should have the ability to apply to the Registrar to have his or her personal information withheld from appearing on the register. Individuals should be

[61] PPS Bill s.225(3)(d)
[62] Regulations DP – Para 182

notified directly by the Registrar of this right, and the suppression mechanism should be provided for in the primary legislation, not the regulations.

There are two issues that need to be considered.

- In what circumstances should the Registrar be empowered to withhold personal information from a search of the register?
- Should the circumstances in which the Registrar may withhold the data be included in the primary legislation or in the regulations?

This issue was highlighted again in consultation during this PIA. Privacy regulators and privacy and consumer advocates saw a strong need for the Registrar to have the facility to suppress details on the register in "emergency circumstances".

In discussions, AGD noted that the focus of the Registrar's role to provide an efficient PPSR and that this would generally involve very limited involvement in making decisions in relation to the content of the register. AGD anticipates that the Registrar would act on a request based on a court order but is yet to consider the other circumstances in which the Registrar would decide to suppress an individual's details.

Participants in the consultation discussions were of the view that if an active role in making decisions to suppress information in emergency situations was not consistent with the anticipated role of the Registrar, then the role should be located elsewhere, possibly with the Privacy Commissioner. The discussion also noted that suppression of details could have consequences for individuals including affecting their ability to obtain or maintain credit.

Findings and recommendations

In IIS's view the proposed regulation in the Regulations DP adequately addresses the circumstances in which it might be appropriate for the Registrar to be empowered to withhold data from a search. Circumstances, now unforeseen, in which an individual may be put at serious risk if information on the register is made available may arise and need to be dealt with quickly. It is easier to amend a regulation than to amend the primary legislation and this is a circumstance where ease of amendment may be important. IIS considers that the circumstances in which it should be appropriate for the Registrar to be empowered to withhold data from a search should be outlined in a regulation, not the primary legislation, so as to allow maximum flexibility and responsiveness. However, it considers that the way in which the Registrar will use this power should be transparent.

Recommendation 11 – IIS recommends that the Registrar develop a policy, which is available publicly, which sets out the process by which an individual could seek to have their name and DOB that would otherwise appear on the PPSR suppressed and the circumstances or criteria that would apply.

Recommendation 12 – IIS recommends that if the Government considers that the Registrar would not be in an ideal position to consider requests to remove details from the PPSR in "emergency" situations that it considers other options for this role, including seeking input from the Privacy Commissioner or the Ombudsman.

4.5 ENFORCEMENT OF PRIVACY PROTECTIONS

4.5.1 DEALING WITH THE CONSEQUENCES OF PRIVACY BREACHES

The PPS Bill provided for two main ways of dealing with breaches of individual privacy: damages and remedies under the Privacy Act.[63] In each case, there would be considerable onus on the individual seeking redress. In its report, the Senate Committee recommended that the scope and content of the enforcement provisions of the exposure draft bill be reviewed by the Department with particular attention to ensuring that the provisions are comprehensive and adequate.

The PPS Bill provides that if a person fails to discharge any duty or obligation imposed on the person under the Bill, the person to whom the duty or obligation is owed, or any other person who can reasonably be expected to rely on performance of the duty or obligation, has a right to recover damages for any loss or damage that was reasonably foreseeable as likely to result from the failure.[64] The obligations, non-compliance with which would give a right to recover damages, include:

- Applying for registration of a personal property security in the absence of a belief on reasonable grounds that a security interest in the property is, or will be, held by a person stated in the application to be a secured party;[65]
- Applying for an amendment of a registration of a personal property security in the absence of a belief on reasonable grounds that a security interest in the property has been, or will be, granted to a person registered as a secured party or stated in the application to be a secured party;[66]
- Failure to apply for an amendment of a registration before the end of 5 working days after the day an unperfection time occurs;[67]
- Failure to give a verification statement (that is, notice of registration) to a grantor;[68] and
- Unauthorised search of the register, or the use of data obtained as a result of an unauthorised search, unless it has been obtained from another source.[69]

The PPS Bill provides specifically that an unauthorised search of the register, or unauthorised use of personal information, constitutes an act or practice involving interference with the privacy of an individual for the purposes of the Privacy Act.

The PPS Bill also notes that criminal penalties under the Criminal Code or the Criminal Code Act may apply in some circumstances. For example, giving false or misleading information in a statement to the registrar may constitute an offence under the Criminal Code.[70]

Few submissions address the issue of enforcement. The APF points out that it may be very difficult

[63] The Bill also notes the availability of criminal sanctions under the general law in some circumstances.
[64] PPS Bill s.236
[65] PPS Bill s.190
[66] PPS Bill s.203
[67] PPS Bill s.206
[68] PPS Bill s.223
[69] PPS Bill s.227
[70] PPS Bill ss. 209, 210

to establish that an unauthorised search has taken place as there is no audit trail. CALC notes the inherent weaknesses in an enforcement regime that relies solely on private parties to seek private remedies for statutory breaches. OPC points out that the Privacy Act does not apply to individuals and small businesses, which may make an unauthorised search or use data obtained as a result of an unauthorised search. OPC suggests that there should be additional offence provisions.

An examination of the remedies available under the PPS Bill reveal gaps in the protection provided for a grantor's personal information. The Privacy Act may not apply to a secured party. This exposes some grantors (including those dealing with a secured party that is an individual, a small business or a political party) to privacy risks that do not apply to others. The issue of prior notice of registration has been dealt with above.

The second area where there would be a gap in protection is in the case of an unauthorised search. As noted above, the PPS Bill as currently drafted provides that making an unauthorised search, or using data obtained in one, constitutes an interference with an individual's privacy under the Privacy Act. If, however, the Privacy Act does not apply because the person who made the unauthorised search or used the data was an individual, a small business or political party, a remedy under the Privacy Act would not be available. In such a case, a grantor may have no remedy available other than an action for damages. This remedy puts a heavy onus on the aggrieved party, an individual, to take legal action, possibly against a large corporation, not a practicable option for most individuals.

IIS notes that there are amendments to the Bill so that these provisions apply regardless of whether the person or organisation responsible is otherwise subject to the Privacy Act.[71] It also notes that the Bill now includes civil penalties in relation to unauthorised search or use of personal information.[72]

Findings and recommendations

As has been discussed through this PIA report, the June 2009 PPS Bill has been strengthened in a number of ways including by the introduction of civil penalties and by ensuing that the ability to take a complaint to the Privacy Commissioner on specified issues applies regardless of whether the Privacy Act would otherwise apply to the individual or organisation responsible. IIS also noted in section 3 that the fact that there will be a payment record associated with each PPSR transaction means that there will be some ability to investigate unauthorised searches or other misuse of the PPSR. IIS considers it difficult to establish at this point in the process whether there are sufficient measures in place to ensure that individual privacy is appropriately protected. IIS considers that while there will be areas where the protection could be strengthened the package of protections is on the whole reasonable. However, it does consider that this will be an important area of review once the PPS Act has been in operation for a period.

Recommendation 13 – IIS recommends that the 3 year review of the PPSR consider whether the enforcement framework is effective in protecting individual privacy or whether additional measures are needed.

[71] June 2009 PPS Bill s.173
[72] June 2009 PPS Bill s.172

4.5.2 REGISTER NOT A "A GENERALLY AVAILABLE PUBLICATION"

In its submission OPC raised the question whether the register would be meet the definition of a "generally available publication", that is, one "that is or will be generally available to members of the public".[73] If the register is a generally available publication, the Privacy Act may not apply in full to the handling of personal information on the register. The IPPs would, however, apply to the personal information the agency collects for publication on the register and then continues to hold in its own database.

IIS notes that to the extent that it contains personal information the PPSR may only be searched for specified purposes, that searches are subject to the payment of a fee and that initially a search can only be conducted on the basis of details already known to the searcher. Given these circumstances it is possible that the PPRS would not be a generally available publication under the Privacy Act.

Findings and Recommendations

IIS understands that it is AGD's view that the PPS register will not be considered a "generally available publication". It notes that a statement to this effect has been included at paragraph 5.99 of the Explanatory Memorandum to the June 2009 PPS Bill.

IIS is satisfied with this approach and has no further recommendation.

4.6 POTENTIAL FOR WIDER DEFINITION OF SECURITY INTEREST OR WIDER USE OF THE PPSR (FUNCTION CREEP)

The PPS Bill defines security interest as "an interest or right in relation to personal property provided for by a transaction that in substance secures payment or performance of an obligation (without regard to the form of the transaction or the identity of the person who has title to the property).[74] The Regulations DP anticipates that the regulations would prescribe certain interests in personal property other than a security interest would be included on the register. It states that the other interests could include interests arising out of State and Territory motor vehicle impoundment legislation, confiscation of the proceeds of crime legislation and guardianship orders issued by State and Territory trustees over motor vehicles.

In their submissions, OPC and APF express concern about the breadth of the definition of "security interest" and note that it would include personal property interests other than security interests. This could potentially lead to the register becoming a repository of large amounts of personal information that could be used to develop a personal profile of an individual. OPF and APF both fear, that is "the incremental expansion in the purpose of a system to the point where information is used for purposes not initially agreed to or envisaged and unrelated to the original intent".[75]

It is possible that like other schemes that have preceded it, this scheme may be widened to achieve goals beyond the original purpose. An example of an initiative being extended beyond its original purpose is the extension in the use of tax file numbers, for example to the superannuation environment. There are two initial areas of concern: defining "security interest" to include interests other than security interests and extending the list of people who can search the register, and the

[73] Privacy Act s.6
[74] PPS Bill s.28
[75] Office of the Privacy Commission submission to the Senate Committee p5

purposes for which they can search it. There is also a concern that what constitutes an authorised purpose for a register search may be extended beyond those listed in the Bill. The Bill does not specifically provide for the making of regulations to extend the purposes for which a person can search the register. There is, however, a general regulation making power in the Bill. [76] While the courts have held that such a power will not support attempts to widen the purposes of the Act, to add new and different means of carrying them out or to depart from or vary the plan which the legislature has adopted to attain its ends, there is potential for stakeholders, including individual grantors, to be affected in unexpected ways.

Findings and Recommendations

IIS notes that the Explanatory Memorandum to the June 2009 PPS Bill now explicitly addresses this issue at paragraphs 5.8 and 5.9 which state that:

> During development of the Bill, concerns were expressed about possible scope creep of the PPS Register. These concerns related to two particular functions of the Register. The first concern was a possible increase in the authorised purposes for which a search could be made by reference to the name and date of birth of an individual. Consequently, the authorised purposes for searches by reference to the name and date of birth of an individual could only be altered by the Parliament. It would not be lawful to alter the authorised purposes without Parliamentary scrutiny.
>
> The second concern was the type of interest that could be included on the Register. The definition of security interest could only be amended by the Parliament. However, the Bill would also allow for the registration of other interests in classes of personal property determined under the regulations. Any regulations made under this provision would take account of privacy concerns, including the preparation of a Privacy Impact Assessment if appropriate.

IIS considers this is a reasonable approach in the circumstances. However, it also considers that the Registrar should have in place governance arrangements to proactively manage privacy issues for the PPSR in general as well as in relation to the potential for the PPSR to be used for new or additional purposes.

Recommendation 14 – IIS recommends that AGD should ensure that there is a person or body with responsibility for management and oversight of privacy of the PPSR that report to a senior manager and, when appointed, to the Registrar. Roles and responsibilities should include developing and delivering a clear policy approach for privacy for the PPSR including in relation to:

- Educational material about the PPS scheme and the operation of the PPSR;
- Handling requests to remove individual grantor details from the PPSR where there are serious privacy concerns;
- Data retention;
- An appropriate privacy policy including in relation to notification of data breaches; and
- Further PIAs at significant points for example where there is any proposal to change nature of security interests listed on the PPSR or to the nature of permitted searches.

[76] PPS Bill s.275

The person or body should also be responsible for ensuring that the Registrar conducts regular privacy audits of the operation of the PPSR and that it responds to any audit findings in a timely way. Audits should preferably follow an annual cycle with reports available to the public.

5 APPENDIX 1 REFERENCE DOCUMENTS

ORGANISATION	TITLE AND DATE
Australian Bankers Association	Personal Property Securities Bill 2008 – Exposure Draft (Bill), 23 December 2008
Australian Institute of Credit Management	AICM Submission to Senate Legal and Constitutional Affairs - Committee – Inquiry into the Personal Property Securities Bill 2008
AGD	Exposure Draft of the PPS Bill, issued in November 2008
AGD	Personal Property Securities Register RFT 08/9769 Statement of Requirements Release Version 6 May 2008
AGD	Personal Property Securities Register System Integration Solution Architecture Version 0.03 April 2009
AGD	The Revised Commentary to the PPS Bill
AGD	PPS Discussion Paper: Regulation to be made under the PPS Act (Regulations DP) issued in August 2008
AGD	RFT 08/9769 Personal Property Securities Register Attachment F Schedule 7 Existing Registers
Australian Privacy Foundation	Submissions made to AGD by Australian Privacy Foundation, dated February 2007, August 2008 and October 2008
Australian Privacy Foundation	Personal Property Securities Reform Regulations to be made under the Personal Property Securities Act Discussion Paper August 2008 – Submission to the Commonwealth Attorney-General's Department October 2008
Australian Privacy Foundation	Inquiry into the Personal Property Securities Bill 2008 [Exposure Draft] – Submission to the Senate Standing Committee on Legal and Constitutional Affairs, December 2008
Consumer Law Action Centre	Personal Property Securities Bill 2008 – Exposure Draft, 19 December 2008
Legal Aid Queensland	Submission to Inquiry into Personal Property Securities Bill 2008, 16 December 2008
Office of the Privacy Commissioner	Exposure Draft Personal Property Securities Bill 2008 Submission to the Senate Legal and Constitutional Affairs Committee, December 2008
Office of the Privacy Commissioner	Personal Property Securities Reform Discussion Paper – Regulations to be made under the Personal Property Securities

	Act August 2008, November 2008
Office of the Privacy Commissioner	Consultation on Personal Property Securities Bill and Commentary (Consultation Draft), August 2008
Office of the Privacy Commissioner	Review of the law on Personal Property Securities – Discussion Paper 1 Registration and Search Issues, February 2007
Office of the Victorian Privacy Commissioner	Inquiry into the Personal Property Securities (PPS) Bill 2008 – Exposure Draft
Senate Standing Committee on Legal and Constitutional Affairs	Exposure draft of the Personal Property, Securities Bill 2008 March 2009
Veda Advantage	Submission to Senate Legal and Constitutional Affairs Committee Inquiry into The Personal Property Securities Bill 2008 (Exposure Draft)
Women's Legal Service Victoria	Submission on the Personal Property Securities Bill, December 2008

6 APPENDIX 2 – PARTIES CONSULTED FOR THIS PIA

Meetings held	
25 May 2009	Office of the Privacy Commissioner
	Office of the Victorian Privacy Commissioner
	Australian Privacy Foundation
5 June 2009	Australian Bankers Association
	Australian Finance Conference
10 June 2009	Veda Advantage
Additional submissions received	
June 2009	Consumer Action Law Centre
June 2009	Australian Privacy Foundation

7 APPENDIX 3 – PPSR AND PART IIIA OF THE PRIVACY ACT

The table below sets out a brief comparison of some of the key features of the PPSR and the operation of credit reporting databases.

	IIS understanding of the operation of the PPSR including a set out in the June 2009 PPS Bill	**IIS understanding of credit reporting databases including privacy protections in Part IIIA of the Privacy Act**
Database objectives	Not specified in the June 2009 PPS Bill. IIS understands that the aim of Personal Property Security Reform is to improve the ability of individuals and businesses, particularly small-to-medium size businesses, to employ all their property in raising capital, by making the PPS system more certain, and consistent and to reduce costs.	Not specified in Part IIIA of the Privacy Act. IIS understands that the main purpose of credit reporting databases is assist credit providers to manage credit risk. For consumer credit, credit reporting databases are essentially a list of loan defaults overdue by more than 60 days. Part IIIA protects individual privacy in relation to consumer credit by setting strict limits on: the type of information which can be held on a person's credit information file by a credit reporting agency; who can obtain access to a credit file; and purposes for which a credit provider can use a credit report, which include assessing an application for credit and to collect overdue payments.
Collection	Name, DOB, description of personal property and specified details of secured party	Information about the individual including: full name, including any known aliases, sex and date of birth; a maximum of three addresses consisting of a current and last known address and two immediately previous addresses; name of current or last known employer; driver's licence number; a record of a credit provider having sought a credit report to assess an application for consumer or commercial credit; default information (note that information may only be included here if the individual is at least sixty days overdue and the credit provider has taken steps to collect the amount outstanding); and certain items of publicly available information such as court judgments and bankruptcy orders (s.18E of Part III A of the Privacy Act)
Notice	Prior to registration – As discussed at section 4.1.3 of report, individuals may be given notice before registration under NPP 1.3 (where organisations are subject to the Privacy Act), also the secured party must give the grantor a copy of the verification statement once the registration is finalised	Credit providers generally cannot provide information about a loan default to a credit reporting agency unless individual was told this may happen when taking out the loan (s.18E(8)(c)). Also, credit providers need to advise individuals if a refusal to provide credit was based wholly or partly, as the case requires, on information derived from a credit report relating to that individual that a credit reporting agency has given to the credit provider (s.18M).

Use and disclosure	Any person can access a listing on a PPSR (after paying a fee and submitting an application in an approved form) provided it is for a purpose set out in the June 2009 PPS Bill – this includes establishing whether to provide credit. Use of information or results from the PPSR limited to these purposes unless the information was also obtained lawfully from another source	Essentially access to the credit reporting system is limited to credit providers and bodies with related functions, for example mortgage insurers but excluding mercantile agents. Permitted organisations are prevented from using personal information in a credit report for any purpose other than assessing an application for credit made to the credit provider by the individual concerned unless specified exceptions apply
Access	IPP 6 individuals able to seek access to personal information held on the PPSR	Part IIIA of the Privacy Act, and the associated Code of Conduct, give individuals the right to a copy of their credit information file, in some cases without charge. (S.18H and Clauses 1.6 – 1.8 of the Credit Reporting Code of Conduct)
Security	PPSR, Credit Providers and Credit Reporting Agencies have same obligation under the Privacy Act to take reasonable steps to protect personal information	
Accuracy, correction	PPSR, Credit Providers and Credit Reporting agencies have similar obligations under the Privacy Act to take reasonable steps to ensure personal information is accurate up-to-date and complete and to consider requests to correct personal information or attach correcting statements from individuals.	