Min-it Software

Submission –

Review of the Privacy Amendment (Enhancing Privacy Protection) Bill 2012

Senate Legal and Constitutional Affairs Committee

09 July 2012

Contact:

Haydn Cooper

Director

Min-it Software
PO Box 1367
Sunnybank Hills
QLD 4109

Telephone : 07 3038 3044
Fax: 07 3870 0813
Mobile:
e-mail:

TABLE OF CONTENTS

Foreword

The writer welcomes this opportunity to assist the Committee in its deliberations regarding the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* ("the Bill") currently before Parliament that proposes amendments to the *Privacy Act 1988 (Cth)* ("the Act").

Should the Committee wish to discuss further any information contained in this submission, please do not hesitate to contact me.

Haydn Cooper, Director

Background Information

This submission is made by Min-it Software following consultation with a number of clients. Aside from the software produced in-house, specifically by or for franchised organisations, Min-it Software is the leading internet-based industry software supplier to the small amount, short term finance sector in the Australian market.

As our client base crosses both payday, micro-lending and commercial (non-regulated) sectors of the lending industry, we are able to offer our comments based on substantial knowledge of these very different markets to the Committee.

Neither the writer nor his business partner has any financial interest in any credit provider.

The writer holds a Master of Technology Management (Griffiths) degree and a number of that degree's coursework subjects contained elements of how privacy can be managed when interacting with business.

We provide comments on significant areas that will impact on our clients and on a number of matters that address concerns in respect of an individual borrower's right to privacy.

Matters of definition

Uncertain interactions with other legislation

APP7 relating to the use of personal information for direct marketing states that under 7.8, it does not apply to either the *Do Not Call Register Act 2006 (Cth)* or the *Spam Act 2003 (Cth).* Given the way the APP is worded and, with the increasing prevalence of web-based marketing and interactivity in lending and broking activities, it would appear it is intended that these two Acts completely override this APP. If this is the case, to provide far better certainty, we submit it would be better to redraft it so that it starts with this statement and one then works backwards from there, rather than it being the afterthought it currently appears to be.

Cross-border disclosure of information

Whilst APP8 and s.16C cover cross-border disclosure of personal information about an individual to a person (the 'overseas recipient'), neither the Act nor the Bill defines "person". Whilst one may attempt to rely on the definition of "person" contained within s.2C of the *Acts Interpretation Act 1901(Cth)* ("AIA"), we submit that as the Act does define "corporation", there is an argument that "person" is meant to be a natural person only and the wider AIA definition does not apply because neither the Act or this Bill contains a clause, similar to clause to s.211 of the National Credit Code ("the Code"), that specifically covers this point. That clause reads:

211 **Effect of express references to bodies corporate and individuals**

In this Code, a reference to a *person* generally (whether the expression "person", "party", "someone", "anyone", "no-one", "one", "another" or "whoever" or another expression is used):

a) does not exclude a reference to a body corporate or an individual merely because elsewhere in this Code there is particular reference to a body corporate (however expressed); and

(b) does not exclude a reference to an individual or a body corporate merely because elsewhere in this Code there is particular reference to an individual (however expressed).

On this basis, under the wording of this Bill at present, there appears to be no restriction on an APP entity providing personal information to an overseas corporation or the Australian corporate subsidiary of a foreign corporation transferring that personal information to its foreign-domiciled

corporate parent who in turn, provides it to another foreign corporation with impunity. We do not believe this should be the case and the Bill requires amending to clarify this point and to provide for substantial penalties.

On the other hand, if a corporation, domestic or otherwise, is covered by the definition of "person", by how exactly is the requirement under APP8.1 that "the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information" going to be determined? We question what steps will be considered "reasonable"? If any damage, as a result of the misuse of the personal information, is caused or has already been done, which entity – the APP entity, its foreign parent, the foreign corporation receiving and then misusing the personal information – is to be liable and accountable to those individuals? What happens if the foreign parent is required to or does submit the Australian personal information to its government under its laws? What rights does the individual whose personal information has been misused have in relation to such breaches?

We submit this does not appear to have even been considered and it is too important to leave to uncertainty. The Bill must be amended to ensure that any such misuse is properly covered and enshrined in law.

Credit Reporting

Definition of 'credit' widened and its implications

As a credit industry software developer, we must express concern that the Bill definitions relating to "credit" differs from that contained within the *National Consumer Credit Protection Act 2009 (Cth)* ("NCCP Act") by the addition of s.6M(3) and "credit provider" widened by the provisions of Section 69 in terms of s.6G(2)(b) of the Act. Consequently, the number of credit providers (as defined by this Bill) will be considerably greater than those licenced under the NCCP Act and this is solely for the benefit of the credit reporting businesses. Australian Credit Licence ("ACL") holders already have to hold and retain far more personal information than is really necessary due to NCCP Act, the Code and ASIC's requirements but rather than further limiting who has access to personal information, this Bill will allow additional credit providers to seek, hold and collect personal information they currently cannot access.

Consequently, if many others have access to an individual's personal information through their work, an individual's right to privacy has been considerably and directly diminished by this legislation. Regardless of any legislative provisions providing possible punishment and relief, allowing many other APP entities to hold such information will create increased opportunism for the theft of such information on a far greater scale than has been seen to date. The writer personally considers this to be a serious and retrograde step as any punishment will come, if at all, far too late and any relief will be little consolation to those affected.

Only those that have had their identity or personal information stolen know what damage this can do, what hurdles the individual then has to jump through to prove it was not you that did something and how long it can take to resolve. Despite taking the greatest of care for many years, the writer's own personal information and identity was stolen by bank employees within this country and supplied to others overseas. Over a period of almost 9 weeks, this involved numerous telephone calls and personal attendances at a Police station, a variety of Government Departments, banks and other businesses, producing statutory declarations from myself and others that could vouch for me, simply to get access back to bank accounts, credit cards and other documents of identity that are taken for granted in our daily lives. As a result, the writer now takes every step possible to minimise any further risk of this re-occurring but acknowledges even this may be insufficient for determined thieves.

Credit defaults and personal privacy

It is interesting to note that in the UK, rather than taking this wider approach as to what constitutes "'credit", a reduced approach is considered necessary after Kitchin J, in an England and Wales High Court case last year (*Office of Fair Trading v Ashbourne Management Services Ltd and others [2011] EWHC 1237*) declared that the registration of credit defaults on a contract of gym membership was an invalid practice as the contracts were not credit contracts under the UK's *Consumer Credit Act 1974* ("UKCCA"). The Court found the gym club's practice of describing members who wished to terminate their agreements before the end of the minimum period as defaulters, essentially where the member dishonoured or missed payments, and then registering or threatening to register that information with credit reference agencies was inaccurate because the payments were nothing more than an amount which the gym club considered the gym club was entitled to in damages. The Court noted reporting or threatening to report the fact that an individual owed a debt which was, in reality, nothing more than unliquidated

damages was an unfair commercial practice and harmed the collective interests of consumers contrary to the UK's Consumer Protection from Unfair Trading Regulations 2008 SI 2008/1277 (CPRs).

Effectively, the Court stated that unless the credit was provided under a consumer credit contact as defined by the UKCCA, then no credit default could be registered. Implementing this same practice here by limiting credit defaults to those with credit contracts under the NCCP Act and allowing for those commercial loan defaults would reduce some of the current income received by the credit reporting businesses but given the tightness by which ASIC now controls the finance industry, it would provide individuals with far safer and more secure control.

Definition issue - Serious Credit Infringement

We are extremely concerned at the further restrictive definition contained within s.63 that adds, by way of the amendment, a new dimension to serious credit infringement in s.6(1) of the Act. Under this Bill, the credit provider must either prove fraud or be able to comply with subsection (c) (i) and (ii) and wait until "at least 6 months have passed since the provider last had contact with the individual". In contrast, the existing definition merely requires **"**that a reasonable person would consider indicates an intention, on the part of the first-mentioned person, no longer to comply with the first-mentioned person's obligations in relation to credit.**"**

If, in the opinion of the credit provider, the individual no longer has or appears to no longer have the intention to fulfill his or her obligation under the credit contract after contacting or having attempted to contact the individual, we question why is this insufficient to act at that time? The requirement to wait at least 6 months from the time the credit provider last had contact with the individual defeats the timely registration of a serious credit infringement to alert other credit providers to the individual's actions and exacerbates the indebtedness of the individual to the original credit provider.

The situation is compounded where the consumer deliberately evades contact from the credit provider.

If the consumer contacts the credit provider but still does not act, the compliant credit provider has just two legal options. The first is to write off the debt and put it down as a cost of doing business but this ultimately increases the cost to everyone including those that do meet their obligations. The second option is pursue the debt in the Courts. As researched and outlined by the Finance Industry Delegation in its submissions to the *Consumer Credit and Corporations*

Legislation Amendment (Enhancements) Bill 2011 (the "Enhancements Bill"), a third option of collecting the debt may be utilised or at least considered by those with bikie gang partners or relationships. It may even be the impetus for some to take on such relationships.

If the requirement to wait 6 months from when the credit provider last has contact is not removed, all this will do is harden the resolve and attitude of credit providers generally. Some will inevitably determine that, coupled with the provisions of the Enhancements Bill passed by the Commonwealth House of Representatives but yet to be debated and voted on in the Senate, this Government is firmly anti-competitive and anti- the credit industry generally and look to exit the industry. This will leave consumers much the worse off with reduced choices as far as credit providers go and/ or credit exclusion to deal with.

Expanding the reach of "Government" - Recognition of EDR providers

We are very disturbed that the proposed Bill will considerably enhance existing EDR providers' interference in circumstances where privacy is an issue (e.g., s.20E (3) (c) (i), s.20U (3) (c) (i), s.25, s.S48, etc.) and the APP entity is a party to a "recognised external dispute resolution scheme". We do not believe that it is appropriate to give the two private companies (which are not statutory authorities) engaged in providing EDR for credit even greater power than they currently have, particularly at the expense of direct contact with the Privacy Commission.

Credit industry participants and legal professionals have already expressed a number of concerns about the approach that the two External Dispute Providers under their interpretation of the NCCP Act are having on the credit industry.

Whilst the philosophy behind EDR is meritorious, how it works in practice leaves much to be desired. A number of legal professionals and industry participants are concerned that Parliament has not traditionally endorsed a statutory body like ASIC creating its own sub-regulations applicable to a body that is not within the Government structure and for whom a Minister has no direct responsibility. It might be useful for the Committee to explore whether, under the Constitution, it is permissible for Parliament to allow a Federal Government Department to effectively subrogate the powers it has been granted by Parliament to non-statutory entities as effected under this Bill.

As an example of the different treatment currently operating, if a consumer were to skip their existing address and leave no forwarding address and that consumer then had a number of credit

defaults created by a credit provider, a utility provider and a video hirer, in the event of a dispute as to the legitimacy of those credit defaults being registered, the consumer may take its disputes with the utility provider and the video hirer, if they cannot be resolved by them, to the Credit Reporting Agency who is required to make a decision. If the consumer is dissatisfied with that decision, the matter may be referred to the Privacy Commissioner for a decision, all at no cost to either the consumer or the other business entities involved.

For the credit defaults lodged by a credit provider, however, and in light of this Bill, the credit EDR providers will charge the credit provider a 'complaint' and possibly other fees. The Committee must recognise that one of the two credit EDR providers recently introduced a change in its Rules so that if a consumer approaches that body, its ' members' are forced to pay a fee no matter how vexatious or lacking in substance an alleged complaint by the consumer may be. The writer suggests this cannot be dismissed because a mechanism that incurs unwarranted and unnecessary expense ultimately leads to a breakdown in the fundamental platform upon which the Committee's concerns, as evidenced by its terms of reference, are constructed. Aside from this Bill providing some form of legal recognition to what the credit EDR providers are currently doing, it is inequitable that a credit provider is treated substantially different from a business entity that is not a credit provider.

There is also further inequity possible in that as a result of there not being just one arbiter, the Privacy Commissioner, involved in the ultimate decision-making process for all decisions, it is highly likely that differing standards will be applied to identical situations if any other party, including EDR providers, are granted some form of legal recognition to make determinations as though they were the Privacy Commissioner through this Bill.

Before allowing EDR providers to make decisions in respect of credit reporting matters, the Committee may find it useful to explore whether these schemes exist to dispense social justice rather than justice that should be dispensed by a Court. We suggest credit EDR providers should not be able to make decisions pertaining to credit reporting matters and the Privacy Commissioner insist the existing provisions of the Act apply.

Abuse by access seekers - Credit 'Repair' companies

The industry believes there is widespread abuse by credit repair companies, who would act as an access seeker under the Bill, taking 'complaint' allegations to EDR providers to the credit and finance industry where the credit provider refuses to remove a default listing. These companies charge the consumer a fee for their service and a success fee for each credit default they

manage to have removed.

If the credit provider does not agree to remove the default listing, generally on the basis of it was incorrectly made, they take their 'complaint' to the credit provider's EDR scheme. As stated above, that action causes the credit provider to incur a fee, even if the decision is correct, yet had the matter been referred to the Credit Reporting Agency or even the Privacy Commissioner for determination, it would have been totally free for both parties.

It would be a concern to all credit providers were the credit reporting system's integrity to be threatened, simply because it is financially more expedient to change a default listing than incur a fee.

Repayment history – reasonably necessary?

Under the amendment to s.6N (Meaning of credit information), an individual's repayment history, default and payment arrangement history, including whether or not a new arrangement, is regarded as personal information. Under APP 3, personal information (other than sensitive information) must not be collected unless the information is reasonably necessary for one or more of the entity's functions or activities.

Whilst such information will be obtained and retained out of necessity in the ordinary course of credit being provided over the term of such credit, it is our opinion that the reporting of such information to a credit reporting business is not a necessary function nor one reasonably necessary for the credit provider it to perform its responsible lending or other credit activities. It is also not reasonably necessary, though it might be convenient from a commercial practice perspective, for another credit provider to see such history where that credit provider uses or is provided with a scoring mechanism supplied by the credit reporting business.

We would also bring to the Committee's attention that some credit providers misuse the current reporting system and discriminate against those that use some non-ADI credit providers. UK experience shows that even having a good repayment history with such a lender remains a barrier to those attempting to get back to using mainstream lenders.

On that basis, whilst we believe an individual will have no right to refuse a credit provider collecting such information because it will anyway, if the credit is to be provided, we do believe an

individual should have the right to individually authorise his or her approval to pass such repayment information onto a credit reporting business.

Given the subscription terms of at least one credit reporting business right now, however, we believe the credit reporting businesses will attempt to enforce the transfer of such repayment, default and arrangement information to them simply through a contractual arrangement between it and the credit provider. If individuals are to retain their privacy, such a practice must not be permitted under any circumstances and we strongly recommend the Bill be amended to provide for a specific opt-in for the transfer and reporting of repayment history and not an opt-out process or an all-encompassing approval requirement.

Whilst some may see this as an individual interfering in the credit provider's contractual arrangements with its suppliers, an individual must be given the right to refuse the credit provider's request on the basis it is neither reasonably necessary nor required for it to perform its functions. If approval is given, then the credit provider must ensure that it passes on only those individuals personal information to the credit reporting businesses and no other. From a software perspective, this is not difficult to do.

Consumer Credit Information - Unwillingness to supply

The writer is aware that members of one credit organisation refuse to supply a reference to other credit providers unless they are also members of that same organisation, despite holding properly authorised Privacy Statements authorising other credit providers to provide relevant credit information. The writer has personally tried to assist clients obtain such information from at least two of that organisation's members to no avail, citing policy requirements as a reason. We believe that the Committee should be concerned about such restrictive trade practices as it may result in reduced interest rates for the consumer.

We recommend the Committee look at amending the Bill to encompass such a requirement.

Consumer Credit Reports - variable pricing

Privacy and the concurrent appropriate use of information can be seriously eroded if the negative impact of cost intrudes. It is the writer's view that the Committee must be aware that the opportunity of credit providers being forced to avoid legitimate credit reporting agencies and encouraging the introduction of underground suppliers of credit information that are not transparent and available to be regulated under the Privacy protection regime is highly likely in the current circumstances. If there is a substantial move to utilising credit reporting services that lack the regulatory rigour currently imposed on the legitimately established credit reporting agencies, then there is a substantial risk the privacy of some 750,000 small amount, short term borrowers each year will be put at risk. Much will depend on cost.

If the Committee is inclined to recommend concepts that will attract extra cost, it might be useful for the Committee to consider the current cost circumstances associated with the legitimate credit reporting agencies that hold massive amounts of personal information. To that end, we bring to the Committee's attention the concerns raised by the Hon. Bill Shorten when addressing industry representatives, including the writer, on 09 September 2011 in his Monee Ponds Electorate Office over compliance costs. The Minister was extremely concerned to note the huge pricing differences charged by one of the major credit reporting agencies between credit providers for credit reports obtained from it, given that he has introduced interest capping mechanisms under the Enhancements Bill. Under this latter Bill, the credit provider would not be able to recover such costs and they would erode the credit provider's revenue capability to the point of being uneconomic for some loans.

The writer, representing our clients, along with representatives from the Financiers Association of Australia and the National Financial Services Federation met with senior management of this credit reporting business to discuss the possibility of an industry wide pricing mechanism. During that meeting, we were advised it dealt with credit providers on an individual basis, not an industry wide basis. The Committee may care to consider this point when reviewing what this Bill will achieve for those insisting that credit reports be obtained from such credit reporting businesses, particularly those subject to interest rate caps and in the light of a possibility that the credit EDR providers may require all of their 'members' to compulsory use such reports.

Concluding comments

Australians need to have faith that those collecting their personal information will do so with care and hold it in a safe and secure environment, particularly so when those holding it are private companies and so subject to takeover or merger. If massive identity theft or large scale loss of personal data occurs from the credit reporting companies or even the credit providers themselves, the test for this legislation will occur after, rarely before, the damage has been done.

We also would recommend that Government engages in a comprehensive education programme so that individuals are made aware of their privacy rights and business are made aware of the changes well before the Bill becomes law.