AUSTRALIAN BANKERS' ASSOCIATION INC.

Name Ian Gilbert
Policy Director

AUSTRALIAN BANKERS' ASSOCIATION INC.
Level 3, 56 Pitt Street, Sydney NSW 2000
p. +61 (0)2 8298 0406 Ext **f.** +61 (0)2 8298 0402

www.bankers.asn.au

13 November 2013

Professor Barbara McDonald
Commissioner
Australian Law Reform Commission
GPO Box 3708
Sydney NSW 2001

Email to: privacy@alrc.gov.au

Dear Commissioner McDonald,

Inquiry into Serious Invasions of Privacy in the Digital Era – Issues Paper

The Australian Bankers' Association (ABA) is pleased to have the opportunity to provide comments on this Issues Paper.

The writer appreciated the prior opportunity to meet with you and your colleagues to discuss some of the concerns the ABA would have with the proposed cause of action if the Government decided to enact this measure. It was helpful to understand some of the complexities that your Commission will be facing in the course of the inquiry.

This submission comprises some preliminary concerns about the nature if this inquiry and answers to selected questions set out in the Issues Paper.

The ABA is grateful for the short extension of time to complete this submission.

The ABA is the peak national body representing banks (other than mutuals) that are authorised by the Australian Prudential Regulation Authority to carry on banking business in Australia. The ABA's membership of 25 banks comprises the four major banks, former regional banks that now operate nationally and foreign banks that are represented and carry on banking business in Australia as Australian banks.

1. Inquiry Terms of Reference

The ABA is particularly concerned with the inquiry's Terms of Reference dated June 2013. In this ALRC Issues Paper, the ALRC will not be undertaking a de novo inquiry into this issue as the Terms of Reference appear to limit the scope of the inquiry.

There does not appear to be any requirement in the Terms of Reference or for the inquiry itself to take into account formal consideration of the submissions made by interested parties on previous occasions.

The ABA considers that the primary question in this inquiry should be asked whether respondents support or oppose the statutory cause of action and why as this was asked in the previous consultations.

The form and substance of the cause of action are subsidiary matters which do not go to whether there is a need, based on identified market failures in Australia, for such a cause of action irrespective of its form.

It is unfortunate that the main thrust of the Terms of Reference appears to be that the ALRC should make recommendations about legal forms of redress and prevention without first addressing the primary question of what has occurred to warrant the making these recommendations.

2. The ABA's Position

The ABA does not support the introduction of a statutory cause of action for serious invasion of privacy (statutory cause of action).

This had been recommended by the Australian Law Reform Commission (ALRC) in its 2008 Report 108 "For Your Information".

In September 2011, the Commonwealth Government's Department of Prime Minister and Cabinet (PM&C) released an Issues Paper with a proposal for the introduction of a Commonwealth statutory cause of action for a serious invasion of privacy. The ABA opposed this proposal again.

In June 2013 the previous Commonwealth Attorney-General referred the same issue of a statutory cause of action to the ALRC to inquire into and report by June 2014.

This is the third occasion on which the ABA has considered and provided a submission on this issue.

The substance of this submission is a restatement of the ABA's previous submissions.

2.1. The Key Reasons for the ABA's position

(a) The ALRC's Report 108 "For Your Information" and the September 2011 PM&C Issues Paper did not identify a demonstrated need for regulatory intervention.

(b) What may have occurred overseas to prompt calls in Australia for regulatory intervention does not constitute a demonstrated need for a statutory cause of action in Australia.

(c) The High Court has clearly left open the way for the common law of Australia to develop an Australian approach and there is evidence of this occurring.

(d) Existing Australian telecommunications laws deal with the types of conduct identified in the UK and to the extent those laws are not sufficient they can be specifically amended without the need to go further.

(e) Significantly, the introduction of the statutory cause of action could change, fundamentally, the administration of Australia's privacy regime from a regulator administered system to one administered substantially by the courts.

(f) The cause of action, if enacted, would be broad in its scope, imprecise and would create uncertainty for businesses, particularly banks, and introduce a level of risk for businesses in conducting commercial activity with potential impacts on the economy.

(g) The scope or reach of the proposed cause of action is of its nature broad and defined according to a range of circumstances that would have to be interpreted and assessed in any given situation.

(h) Examples of this activity include the activities of banks and other credit providers in recovering loans in default, enforcing rights under mortgages and other securities, the collection and verification of information in order to comply with legislated identity validation, "know your client" requirements and for banks' and others insurance businesses to investigate fraud.

(i) Banks and other businesses hold sizeable amounts of personal information about their customers. Banks must know about their customers for legal and practical reasons and are required under the Privacy Act to take reasonable care of this information throughout the course of its collection use and disclosure cycle.

(j) Currently, banks are highly regulated in how they collect, manage, use, disclose and protect customer information. Recent amendments to the Privacy Act will further enhance these protections including prescriptive requirements and limitations on the collection, use and disclosure of credit information under Part IIIA of the Privacy Act.

(k) Confidentiality and security of customer information is critical to Australia's banks. Australian banks recognise that information, privacy and security are central to maintaining the trust of their customers and the community. Privacy and security of this information is a core banking principle and essential to on-going viability.

(l) For almost one hundred and fifty years the common law has imposed a contractual duty of confidentiality on banks not to disclose the affairs for their customers unless the disclosure falls within four limited exceptions.

(m) Banks have a history of dealing with customer complaints about their banking services, including complaints about confidentiality and privacy. These arrangements are entrenched in legislation requiring banks to have internal complaint handling procedures for their retail customers and access to a free, independent dispute resolution service (in most cases the Financial Ombudsman Service) for these customers.

(n) It is important to recognise that banks not only have a legal obligation to secure personal information that they collect from their customers but also that they have a very strong commercial incentive to ensure customer information is properly protected.

(o) Banks play a critical role in the Australian economy and are subject to a wide range of prudential and market conduct regulation. Banks must conduct banking business in accordance with these requirements with integrity, prudence and professional skill.

(p) In this instance, regulatory intervention into the private sector would be inconsistent with Australia's principles of best practice regulation. The creation of the statutory cause of action with potential liability for banks would add unnecessarily to the body of strong regulation to which banks are currently subject. The statutory cause of action would require banks to take steps significantly over and above current and proposed requirements under the Privacy Act and the common law to anticipate and guard themselves against the risk of action, including from the rising presence of third party

litigation funders and class action specialists. This would lead to a significant increase in business compliance costs with resulting business dislocation.

2.2. Absence of the regulatory policy case

In its 2008 Report the ALRC's analysis and recommendation for its support for the statutory cause of action relied on:

1. Uncertainty, piecemeal and fragmented development of a tort by common law courts;
2. The potential benefits of national uniformity and consistency in the application of the law for invasion of privacy;
3. Other local law reform commissions' recommendations;
4. Overseas developments particularly in the U.S. and in the U.K; and
5. Submissions during the ALRC's consultation process

to conclude that:

> *"Individuals should be protected from unwanted intrusions into their private lives or affairs in a broad range of contexts, and it is the ALRC's view that a statutory cause of action is the best way to ensure such protection".*

The ABA's view is that, fundamentally, the above factors do not support a regulatory policy case for the introduction of the statutory cause of action.

The ALRC having concluded this in 2008, the ABA is concerned whether this further inquiry which is able to proceed on the basis of regulatory design is able to move outside of that scoping framework or do the Terms of Reference prevent this?

3. The questions posed in the Issues Paper.

The ABA provides answers to some of the questions posed in the Issues Paper.

Please note that the answers provided are to be read subject to and conditioned by sections 1 and 2 of this submission.

It should not be concluded that in not selecting all questions for comments, the ABA is necessarily conceding the import of those questions to which it has not provided answers.

When referring in our answers to applicable privacy principles in the Privacy Act we will use the Australian Privacy Principles (APPs).

3.1. Q 1 - Principles guiding reform

The ABA agrees that the stated principles are appropriate. A further principle should be included to ensure that "privacy is balanced with "the requirement for the free flow of information and the right of business to achieve its objectives efficiently".

3.2. Q2 and 3 – Impact of a statutory cause of action

The ABA is concerned that in seeking examples of activities that ought to be covered and not covered in the statutory cause of action, this is likely to increase public expectations that the scope of the cause of action model will be broad and all encompassing. The ABA considers that the grounds for action should be limited, specific and clear.

In particular, noting that questions 22 – 25 directly raise the point, the ABA is very concerned that a recommendation to extend the proposed statutory cause of action to breaches of the Australian Privacy Principles of the Privacy Act would change, fundamentally, the existing regime for administration of the Act.

The risk is that the regime would move from a regulator administered regime by the OAIC to a court based model. One result would be the proliferation of class actions and third party litigation funding which are increasingly becoming features of Australia's private sector economy and which are largely unregulated.

Another relevant aspect is that banks and other financial services organisations have in place proven, well-functioning external dispute resolution arrangements as required under legislation. These arrangements are supervised by regulators, ASIC under financial services and credit legislation and next year the OAIC in the case of the Privacy Act. The same services are available under the ABA's Code of Banking Practice.

Individuals are able to access these arrangements free of charge.

Further, in the case of banks, courts would have to work through a series of complex, and in some cases conflicting legislative and regulatory requirements if the statutory cause of action were introduced such as with interaction with the APPs, AML/CTF[1] legislation which is characterised in obligations in many other countries in which banks' cross border operations are conducted.

There are many activities that are necessary for a business to carry on its functions and activities. APP 3 recognises this. It provides that collection must be by lawful and fair means. For example, a bank that is seeking to locate a defaulting customer or an insurer conducting surveillance of a claimant where there has been cause to suspect that the claim may be fraudulent, would be unlikely to infringe APP 3. But these inquiries would be unwelcome by the individual and therefore could be interpreted as an "invasion of privacy" under the statutory cause of action model.

The scope of the statutory cause of action would be far wider than APP 3 and conflict with APP 3 requiring only proof of, for example, an "interference with an individual's home or family life" (one of a possible non-exhaustive list of invasions) to establish the basis of the case for action.

The data security principle, APP 11, is another example where the standard for compliance is based on an organisation taking reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure. The statutory cause of action is expected to have no such tolerance.

An example of an additional measure to be taken by an organisation could include guarding against the risk that a court may determine that an organisation had been reckless in that its information systems had been compromised by a third party and so triggering the cause of action despite the organisation having taken reasonable steps in compliance with the Privacy Act to protect those systems from misuse or unauthorised access.

3.3. Q 6 – Privacy and the threshold of seriousness

3.3.1 A reasonable expectation of privacy

It is not clear on what basis would a court conclude "there is a reasonable expectation of privacy" – the individual's, the community's - and how would this be judged or would it be a judge's view?

The word "privacy" is itself imprecise.

[1] Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Their Honours Gummow J. and Hayne J. in Lenah Game[2] observed this aspect of the decision in Douglass v. Hello! in this way:-

> *"Nothing in Douglas suggests that the right to privacy which their Lordships contemplate is enjoyed other than by natural persons. Further, the necessarily tentative consideration of the topic in that case assumes rather than explains what "privacy" comprehends and what would amount to a tortious invasion of it. The difficulties in obtaining in this field something approaching a definition rather than abstracted generalisation have been recognised for some time".*

The plaintiff would bear this onus of proof. The onus of proof should extend to establishing not only the plaintiff's expectation of privacy but also that this was known or ought reasonably to have been understood by the respondent.

3.3.2 Highly offensive to a reasonable person of ordinary sensibilities

The Issues Paper questions whether this form of test is too high which could disallow otherwise meritable claims. This test would be interpreted objectively and the plaintiff would carry the onus of proof.

It is unclear how this onus would be discharged and ultimately upon whose view this threshold had been established other than, perhaps, in the most extreme cases where it would be self-evident. In the analysis, while this test could appear to be high and may prove to be "vague and nebulous" (to use the ALRC's former words) and uncertain for business to apply in any given case, the ABA submits it should not be lowered.

Both limbs are intended to be balanced with the interest of the public in maintaining an individual's privacy and other matters of public interest, for example, the public's right to know, the constitutional consideration of a right of free speech and the communication of ideas about government and politics.

By way of illustration, the Privacy Act recognises the right of a business to engage in direct marketing yet there are sections of the community that consider certain aspects of direct marketing to be offensive, possibly even highly offensive, for example the direct marketing of credit products.

Another illustration is that it may be assumed that there is a public interest in ensuring the ability of a bank to recover a debt owed to it and to enforce a security right in aid of recovery. However, public interest considerations tend to move with public opinion. What may have been the case about a debtor's obligation yesterday may not necessarily be the case tomorrow if a public interest consideration includes recognition that a departure from the strict performance of a debtor's repayment obligation is not necessarily inappropriate.

3.4. Qs 7 and 8 Privacy and public interest

There should be a public interest defence that recognises the right of business to achieve their objectives efficiently.

It would be appropriate for the legislation to include this in a list of factors to which the court would be required to take into account.

3.5. Q 9 - Fault

The cause of action given its likely scope and imprecision should not be cast in the tortious framework of negligence. Rather it should apply only to an intent to seriously interfere with a person's privacy or to do so with reckless indifference to that result and this has occurred.

[2] Australian Broadcasting Corporation v. Lenah Game Meats Pty Ltd ("Lenah Game")

In the earlier ALRC Report 108, recommendation 74-3 proposed that the cause of action would be restricted to, among other things, an intentional or reckless act on the part of the respondent. At 74.161 of the ALRC Report 108 section 5.4 of the Criminal Code (Cth) is cited as a possible definition of "reckless". As the statutory cause of action would be a civil action recklessness may have to be determined by application of the civil common law. Courts tend to apply an objective test to the issue of recklessness.

In the result, for banks and other business organisations this would involve going beyond what is required to be implemented in the way of compliance with the requirements of the Privacy Act to guard against accidental, but no less intentional, acts on the part of an employee.

There is the possibility that the statutory cause of action could be activated by conduct that amounts to a failure to act. This would broaden the scope of the cause of action requiring a business to develop compliance mechanisms that seek to control its activities by its personnel and also to anticipate where a failure to take action could result in triggering the statutory cause of action. An example could include a bank failing to identify and correct an error on its internal system or file that resulted in an applicant for a credit facility being declined or falling into default and this appearing on the applicant's credit file.

This can be contrasted with a number of the APPs in the Privacy Act where an organisation's compliance obligations go only as far as taking reasonable steps as may be necessary in the circumstances.

3.6. Q-10

The cause of action should not include a *per se* breach given the likely scope and imprecise nature of the cause of action.

Further, the trend in legislation to more strict liability provisions associated with the imposition of civil penalties continues to be a major concern for the private sector.

3.7. Q-12 Defences and exemptions

Compliance with the Privacy Act should be a complete defence to the statutory cause of action particularly as some of the compliance obligations in the Act are conditioned by concepts of reasonableness and the particular circumstances.

Further, there are circumstances in which an act (or omission) on behalf of an organisation may occur inadvertently or accidentally, but in good faith. This should be reflected in a defence if the person had acted in good faith, honestly and reasonably and ought fairly to be excused.

Another example where a defence should exist is in the case of decisions by company officers that are able to be adjudged under the business judgment rule in the Corporations Act. A modified version of this rule could be available for organisations and their employees.

If the Government decides to proceed with the creation of the statutory cause of action the ABA requests that a special consultation is convened to discuss the range of defences that should be available to banks as a necessary part of their conduct of banking business under a range of regulatory instruments.

3.7.1 Defences and the bankers' duty of confidence

A further defence should be available to banks where they are compliant with the bankers' duty of customer confidentiality.

Banks are subject to a common law contractual duty to keep the affairs of their customers confidential. There are four exceptions to this duty; disclosure

- with the consent of the customer,

- under compulsion of law,
- under a duty to the public, and
- in the interests of the bank.

This rule of confidentiality provides protection to bank customers (individuals and corporations) because of the confidential nature of their banking business and affairs.

The proposed defences available to an organisation do not align exactly with the exemptions that are available to banks under the duty of confidentiality.

In the interests of consistency, these exemptions should receive recognition as defences for an exemption for banks if the statutory cause of action is enacted.

Each of the four exceptions is explained below.

1. Consent of the customer

The customer's express or implied consent to a disclosure would be self-evident of a lack of a reasonable expectation of privacy.

2. Disclosure under compulsion of law

Where the exemption from the duty is a disclosure under compulsion of law, there are areas of uncertainty where a judgment whether to disclose in the belief it is required by law proves to be erroneous.

For example, legislative obligations on banks include duties to enquire, obtain, verify and record a wide range of information about their customers. Under AML/CTF law banks have obligations to report certain suspicious transactions or persons where the bank has reasonable grounds to suspect the same.

It is unclear under the AML/CTF law whether a bank is relieved from the consequences of providing a report to the regulatory authority where the suspicion may be found subsequently not to have arisen on reasonable grounds. In any event, protection to the bank would be likely to be confined to the application of the AML/CTF law.

Therefore, a report about a person or transaction to the regulatory authority could be actionable under the statutory cause of action if it were made in the mistaken belief that reasonable grounds to suspect existed. These reports are generally of a very serious nature and could result in serious consequences for the person concerned.

Another example relates to the responsible lending obligations on banks and other credit providers under the National Consumer Credit Protection Act 2009 (NCCP) that require a credit provider to obtain information from an applicant about their objectives, requirements and financial situation. The information about the applicant's financial situation generally must be verified.

It is almost inevitable that this process will involve aspects of an applicant's home and family life. What would be the implications for a credit provider over anxious to ensure compliance with these obligations if a court considered that the information obtained by the credit provider or verified with third parties was unreasonable and therefore amounted to a serious invasion of privacy?

3. Duty to the public to disclose

This exception has been the subject of considerable case law.

Under the proposed statutory cause of action would a court reach the same conclusion as the Federal Court in Allied Mills[3] in which Sheppard J. stated:

> *"The authorities establish that the public interest in the disclosure (to the appropriate authority or perhaps the press) of iniquity will always outweigh the public interest in the preservation of private and confidential information".*

Allied Mills concerned a company's private documents given to the regulator by an informant. Perhaps the principle of disclosure in this case would be likely to be more strictly applied under the statutory cause of action because a case would involve the personal information of an individual.

4. Disclosure in the interests of the bank

This exception to the duty of confidentiality permits disclosure of a customer's information, for example, in court documents.

Pleadings in litigation are increasingly more detailed particularly in stating particulars of the claim. The court can strike out a pleading on the ground that it is vexatious, scandalous or simply irrelevant. Would the statutory cause of action provide a right of recourse by the innocent party because the pleading disclosed information that was otherwise expected to be private and was of a highly offensive nature?

A further example is where customers or their representatives use media in any of its forms to seek to embarrass banks with details of their claims and where banks must respond to correct errors or distortions to protect their own interests.

The ABA contends that the potential for conflict in court decision-making between the law relating specifically to banks and the existence of a long standing, well established foundation for banks to protect the confidentiality of their customer's affairs should be recognised.

The statutory cause of action should not apply in cases of banks and the duty of confidentiality.

3.8. Q-20 Institution of proceedings

Given the scope and imprecise nature of the statutory cause of action, consideration should be given to whether standing to bring the action should be limited to the Privacy Commissioner.

Alternatively, standing of the individual to bring the action could include whether the individual had exhausted all reasonable means of access to mandatory industry internal and external dispute resolution services which in the case of banks would include an external dispute resolution scheme recognised by the Privacy Commissioner under the new provisions of the Privacy Act.

As an alternative there could be a requirement for some other mandatory procedural threshold to be reached before a court action based on the statutory cause of action could be commenced.

A threshold could require the parties to engage in a good faith mandatory mediation process, perhaps convened by the Privacy Commissioner, as a pre-condition to the exercise of the right of action. The process would be confidential. Evidence of anything said or admitted and a document prepared for the purposes of the mediation would be inadmissible in any court proceedings.

[3] Allied Mills Industries Pty Ltd v. Trade Practice Commission (1980) 55 FLR 125

3.9. Qs – 22 -25 Interaction of the statutory cause of action with the existing regulatory environment

3.9.1 Australia's privacy regulatory paradigm

It is noted the ALRC considers that the proposed statutory cause of action should be enacted in federal legislation because the cause of action would extend beyond information privacy and would give the Federal courts jurisdiction to entertain these actions.

If this is the case, as the ABA has mentioned above it foresees a substantial shift in Australia's approach to privacy protection if the statutory cause of action is introduced. Private sector amendments to the Privacy Act (other than credit reporting) were made in 2000 and were broadly embraced by major private sector organisations. The amendments were characterised by the government of the day as "light touch", coupled with powers for the Privacy Commissioner to administer the new laws and handle privacy complaints. Banks and other major business organisations supported this approach.

The December 2012 amendments to the Privacy Act confirm this approach although the amendments to Part IIIA are not considered all to be "light touch".

In contrast, the statutory cause of action would represent a substantial shift to a litigious model in privacy law in Australia. Business would be the main sector impacted by this change to a court administered cause of action. Creating the statutory cause of action would rekindle calls for extending that court based litigious approach to the Privacy Act itself. This could lead to consumer detriment in terms of access to justice while at the same time being seen by the business community as another unnecessary and unreasonable impost on business.

Litigation funders (one leading litigation funder is a listed company) and class action firms specialise in the type of commercial opportunity that a statutory cause of action would create. Plaintiffs in these actions are protected from adverse costs orders unless the litigation funder is financially unable to indemnify them.

As a concluding observation, political parties, politicians and their contractors enjoy an exemption under Australia's Privacy Act for their political acts and practices. Media organisations also enjoy an exemption under the Act for acts or practices in the course of journalism and the organisation has publicly committed to privacy standards. In enacting a statutory cause of action would government agencies and these participants in the political and journalistic processes be exempt from the cause of action?

4. Conclusions

In summary

1. The ABA submits that the statutory cause of action is not warranted and, if created, it would result in additional risk, compliance obligations and costs of carrying on business for Australian banks. The Government had the opportunity to consider including the statutory cause of action in the Privacy Act amending legislation but opted for another (a third) consultation process.
2. The ABA is concerned that the Issues Paper focuses more heavily on how to introduce the cause of action rather than examining whether there is a demonstrated need for its introduction.
3. If the statutory cause of action is to be enacted it should not be included in the Privacy Act but in its own stand-alone statute. Including the statutory cause of action in the Privacy Act would compromise the complaints handling processes administered by the Privacy Commissioner and potentially alter the framework of privacy regulation generally in Australia.

4. The Privacy Act should continue to be the primary source of regulation of banks in respect of the collection, handling and protection of an individual's personal information in its information cycle.
5. The statutory cause of action would be likely to conflict with provisions of the Privacy Act and the non-curial alternative mechanisms for handling banking complaints and under the Privacy Act.
6. Should the government proceed to enact the statutory cause of action, appropriately designed defences need to be available to banks that recognise their significant existing privacy and confidentiality obligations and the complaint and external dispute resolution arrangements that they provide for their retail customers.
7. The cause of action should be a civil action only.
8. Completion of a mandatory good faith mediation process should be a pre-condition to the commencement of a statutory cause of action proceeding. Alternatively, standing for commencement of the action should be limited to the Privacy Commissioner.

The ABA would be pleased to meet again with your team as necessary and, if possible, to provide more examples that may be of assistance to your inquiry.

Yours sincerely,