4 December 2020

The Attorney-General
Australian Attorney-General's Department
Commonwealth Parliamentary Offices
Exchange Plaza
2 The Esplanade
PERTH WA 6000

By email: PrivacyActReview@ag.gov.au

Dear Sir

Re: AFMA Submission on the Privacy Act Review: Issues Paper

The Australian Financial Markets Association (AFMA) welcomes the opportunity to make comment on the Review of the Privacy Act consultation.

AFMA supports a principled approach to individual privacy and recognises that given the substantial growth in personal data collection and its commercialisation in recent years, a review and update of existing arrangements is appropriate. AFMA fully supports the reasonable and proportionate safeguarding of personal information and requirements around this aim must be kept up to date to respond to evolutions in the field. Financial services firms are centred on the protection and accurate processing of private data, so these updates are of particular relevance to this sector.

We are concerned, however, that the proposals that seek to remove balance from existing arrangements. If this is the outcome the proposal risks being at odds with the Government's deregulation agenda and intention of driving economic growth, as well as with the Data Availability and Transparency Bill, suggesting a lack of integration of the Government's policy approach across departments.

We support the view that where extensions to the current regime are made they should be done so in a way that is aligned with standard practices elsewhere, where those practices have proved to work well and are compatible with Australian values and policies. This includes the approaches in the GDPR.

However, we caution against the wholesale importation of GDPR. The GDPR, notably its enforcement penalties are widely regarded as draconian. Australia should avoid the excessive costs of the GDPR regulations.

At this time of economic recovery from the impacts from the COVID-19, it is appropriate for the Government to prioritise measures that support economic growth and jobs. It is not appropriate to restart the machinery of the prior period which placed constant demands on business resources and changes that were damaging to the business environment.

Part of the solution is to proceed slowly and take care to better engage with industry. A high-quality consultation process can avoid issues needing to be addressed in the Senate Committee process. While AFMA is especially supportive of the provision of an issues paper, a four-week turn-around is insufficient for a full consideration of the complex issues associated with a redesign of the privacy framework. Particularly as many agencies have released consultations at around the same time due to COVID-19 delays, many with Exposure Drafts that require immediate consideration prior to the next sittings of Parliament.

Any changes to the Privacy Act will have complex flow on implications for other regimes including the Consumer Data Right (CDR). AFMA raised concerns around the highly complex design of the CDR's extensions of the Privacy Act. Revisions to the Privacy Act would likely require significant systems reengineering to ensure compliance of these systems. Any redesign must ensure it is coordinated with integration into the CDR regime, and it may be appropriate to consider rationalisation of the CDR extensions.

More generally we see an opportunity to rationalise and streamline the current disjointed approach to privacy which currently sees four regulators in the financial services sector alone enforcing overlapping and inconsistent privacy related regulations.

We offer some focussed answers to some of the questions in the below letter. Please do not hesitate to contact us for further information.

Yours sincerely

Damian Jeffree

Senior Director of Policy

Objectives of the Privacy Act

1. Should the objects outlined in section 2A of the Act be changed? If so, what changes should be made and why?

AFMA strongly opposes removing a requirement for balance from the Act.

It is deeply concerning that the Government is seeking to move to an unbalanced regime, which is the implication of the requirement to remove this object of the current Act.

That the proposals are incompatible with a requirement for balance that was legislated by the Federal Parliament suggests the proposals may not be appropriately calibrated. We acknowledge that the report prepared by the Australian Competition and Consumer Commission (ACCC) suggested that the Act should 'place a greater emphasis on privacy protections for consumers'[1] as a justification for moving away from a balanced regime. The ACCC is being entirely consistent with its mandate as a consumer commission to present the case for a fully consumer approach.

AFMA too supports robust protections for consumer data in the evolving threat environment we face. There are risks, however, that outcomes for consumers could be adversely affected if sufficient balance is not given to the wider policy and business environment. For example, if costs to business are made excessive by an unbalanced regime these costs might be ultimately borne by consumers in increased service costs or a reduction of services.

An unbalanced approach risks restraining data-driven innovation. In contrast, a balanced approach that promotes privacy is more likely to help Australia's economic progress and the welfare of consumers.

Definition of personal information

2. What approaches should be considered to ensure the Act protects an appropriate range of technical information?

We do not see an overarching need to amend the definition of personal information to expressly include technical information.

The current definition of personal information does not imply the potential for exclusion of technical information as constituting personal information. We note the current definition is broad in scope, sufficiently so to include technical information to the extent that the information reasonably identifies an individual when combined with other data fields.

We submit that it would not be appropriate to extend the definition of personal information to include personal information of the deceased given the well-recognised legal principles already applied in the Privacy Act.

3. Should the definition of personal information be updated to expressly include inferred personal information?

[1] Consultation Paper, page 15.

AFMA cautions that inferred information is a broad category and there is a risk that a general inclusion of all inferred personal information could create confusion and inconsistent application by entities subject to the Act.

4. Should there be additional protections in relation to de-identified, anonymised and pseudonymised information? If so, what should these be?

While we agree that the risk of de-identification must be regularly reviewed for appropriateness, we submit that government should clarify that de-identified information is not personal information where there is low risk of re-identification. We support the establishment of robust controls in this regard, for instance having protection built into the handling of de-identified data on an ongoing basis.

5. Are any other changes required to the Act to provide greater clarity around what information is 'personal information'?

Flexibility of the APPs in regulating and protecting privacy

6. Is the framework of the Act effective in providing flexibility to cater for a wide variety of entities, acts and practices, while ensuring sufficient clarity about protections and obligations?

The current primary and secondary use tests in the Privacy Act 1988 (Cth) (the Act) cater for the majority of encountered circumstances. Any revisions to the Act to make it more similar to the GDPR should establish other lawful bases to supplement any changes to consent. In particular, it is critical that the Act permits businesses to continue to use and disclose personal information in connection with regulatory investigations, litigation, and internal investigations into unlawful activity or serious misconduct.

We note that any mirroring of the GDPR-like lawful bases or exceptions should also include a 'legitimate interests' basis. The benefit of this approach would be to allow businesses sufficient flexibility to use and disclose personal information for legitimate business purposes, such as to:

- undertake fraud prevention activities;
- ensure network and information security;
- process employee personal information; or
- undertake administrative transfers within a corporate group.

We submit that restrictions around the use and disclosure of government-related identifiers should be updated to clarify that such identifiers can be used and disclosed in a sale of business context within the reasonable expectations of the customer.

Additionally, we submit that it should be permissible for businesses to communicate to a customer about any of its products or services based on the relevant information the business lawfully collects and analyses.

Further, we note that amendments are required to consolidate various use cases of personal information. For example, a customer can receive communications from a bank by telephone, email, direct post and SMS. We consider that all of the above channels of communication use personal information and all forms require express or implied consent. We note this does not support the technology neutrality principle, and we submit that the Act should consolidate ancillary legislation to adopt this principle.

Exemptions

Small business exemption

7. Does the small business exemption in its current form strike the right balance between protecting the privacy rights of individuals and avoid imposing unnecessary compliance costs on small business?

8. Is the current threshold appropriately pitched or should the definition of small business be amended? a. If so, should it be amended by changing the annual turnover threshold from $3 million to another amount, replacing the threshold with another factor such as number of employees or value of assets or should the definition be amended in another way?

AFMA has previously noted in the context of the Compensation Scheme of Last Resort that using number of employees as a criterion for determining whether a business is small or not can be problematic. In the financial sector a business may manage many billions of dollars yet have only a small number of staff. Similarly, many local arms of large international businesses may have only a small number of local staff.

9. Are there businesses or acts and practices that should or should not be covered by the small business exemption?

10. Would it be appropriate for small businesses to be required to comply with some but not all of the APPs? a. If so, what obligations should be placed on small businesses? b. What would be the financial implications for small business?

11. Would there be benefits to small business if they were required to comply with some or all of the APPs?

12. Should small businesses that trade in personal information continue to be exempt from the Act if they have the consent of individuals to collect or disclose their personal information?

Employee records exemption

13. Is the personal information of employees adequately protected by the current scope of the employee records exemption?

14. If enhanced protections are required, how should concerns about employees' ability to freely consent to employers' collection of their personal information be addressed?

If enhanced protections are required then alternate legal bases would need to be provided such as GDPR's performance of the contract, legitimate interest of the data controller, and for sensitive data. We note that in Singapore the concept of "freely given consent" is not as limited as it is in Europe. Singapore has recently passed amendments to PDPA extending the legal bases for data collection to support a balance with the needs of business while maintaining appropriate consumer protections. Under the PDPA there is also a "deemed consent" concept.

We note that within the region where new Data Protection (DP) laws are enacted the approach typically tries to align the legal bases with GDPR, for example in the Philippines and Thailand.

15. Should some but not all of the APPs apply to employee records, or certain types of employee records?

The initial decision to include the employee exemption related to the existence of laws that governed such data and the desire to avoid interference with those laws. AFMA could in principle support a redesign of the employee records exception if the changes did not disrupt the existing data flows.

The current arrangements could benefit from a more robust framework around what constitutes personal information in a record, where that record is then subject to a right to request access under APP 12. For example, to assist consistent interpretation on what is personal information, as highlighted in Telstra Corporation Limited and Privacy Commissioner [2015] AATA 991 (18 December 2015) in relation to the Privacy Act in force prior to 12 March 2014.

In the event changes are made to align Australia more with global standards through the removal of the employee records exemption this would need to be accompanied by the introduction of a lawful basis for the use of staff employment data in the broad course of employment.

Political exemption

16. Should political acts and practices continue to be exempted from the operation of some or all of the APPs?

Journalism exemption

17. Does the journalism exemption appropriately balance freedom of the media to report on matters of public interest with individuals' interests in protecting their privacy?

18. Should the scope of organisations covered by the journalism exemption be altered?

19. Should any acts and practices of media organisations be covered by the operation of some or all of the APPs?

<u>Notice of Collection of Personal Information</u>

Improving awareness of relevant matters

20. Does notice help people to understand and manage their personal information?

AFMA recognises that notices must be clear, transparent and meaningful. As such, we consider that by committing to any notification reform, the policy outcomes must benefit individuals who are the subject of data processing.

We support promoting transparency around the uses and disclosures of personal information; however, we caution against a radical reform that can alter the purposes of collection. We submit that limiting and restricting data use to narrow channels would place an operational impact on high-volume complex data businesses to tag, track and segregate those data choices. Further, we note that in order to avoid the provision of excessive notices and notifications such that consumers may become desensitised, the regulator should encourage the adoption of layered, just in time, notices.

We welcome a principles-based approach to improve transparency around disclosures, in addition to clearer guidance on the regulator's expectations.

21. What matters should be considered to balance providing adequate information to individuals and minimising any regulatory burden?

AFMA notes that currently the APPs provide sufficient flexibility in terms of appropriate methods in providing notice.

There is a strong risk that the proposed introduction of more rigorous requirements for notice, especially for implied data collection and third-party data collection, may not result in any tangible benefit to the individual. Challenges of introducing more notice obligations include impeding the ability for entities to use such information and analytics to derive meaningful customer insights, such as identifying early signs of vulnerability. Restrictions on the ability to perform such analysis may limit firms' ability to remain aligned with requirements contained within the Australian Banking Association's Banking Code of Practice (BCoP) as it relates to the treatment of vulnerable customers.

A departure from the current APPs may introduce an undue cost on businesses to provide notice each time personal information is collected or implied, without a material benefit to the individual.

22. What sort of requirements should be put in place to ensure that notification is accessible; can be easily understood; and informs an individual of all relevant uses and disclosures?

AFMA suggests that the privacy policy published on the firms' websites and accessible in other forms upon individual's request should be sufficient. Some notices are excessively long and detailed and may fail to serve any meaningful purpose, as noted in the answer above.

Third party collections

23. Where an entity collects an individual's personal information and is unable to notify the individual of the collection, should additional requirements or limitations be placed on the use or disclosure of that information?

AFMA notes potential negative consequences of adding limitations or restrictions on the use of personal data by third parties that are unable to directly notify the individuals. In some large organisations, where tracking of every disclosure requirement is extremely challenging, further limitations are an impractical approach. The existing framework effectively requires APP entities to ensure recipients honour and abide by APP principles when handling personal information and this is an appropriate outcome.

The inclusion of additional limitations or restrictions could disrupt the existing data flows without meaningfully promoting additional protections of personal information of individuals.

Limiting information burden

24. What measures could be used to ensure individuals receive adequate notice without being subject to information overload?

25. Would a standardised framework of notice, such as standard words or icons, be effective in assisting consumers to understand how entities are using their personal information?

Consent to collection and use and disclosure of personal information

Consent to collection, use and disclosure of personal information

26. Is consent an effective way for people to manage their personal information?

Consent is a valuable method to permit collection and use of personal information. We note that any amendments to the consent regime should align to global benchmarks as opposed to being implemented in a fragmented manner that would unnecessarily differentiate Australia's compliance framework from our international counterparts.

27. What approaches should be considered to ensure that consent to the collection, use and disclosure of information is freely given and informed?

28. Should individuals be required to separately consent to each purpose for which an entity collects, uses and discloses information? What would be the benefits or disadvantages of requiring individual consents for each primary purpose?

Compliance with the requirement of a separate consent to each 'purpose' would be onerous for organizations which already implement robust processes to ensure clients are properly informed on the products and services offered to them. There is reason to believe that frequently seeking consents from clients would unnecessarily damage their client experience. Alternate GDPR-like bases other than consent should help in this regard.

We note that, where explicit protections or prohibitions may be introduced on implied personal information, the analytics capabilities of businesses would be impractically

disadvantaged. By introducing more granular consent requirements, this may make it more difficult for organisations to perform meaningful analysis of information that, on the outset, may not have an explicit purpose to collect.

We note that the proposal for enhanced protections or prohibitions would likely impact the ability of firms to faithfully remain aligned with their requirements under the BCoP, such as providing additional protections for vulnerable customers. Further, firms would be limited in their ability to continue to offer emergency support in response to economic and natural disasters such as COVID-19 and the recent 2019/20 Australian Bushfires. The current legal and regulatory framework permitted firms in the above circumstances to use predictive analytics for primary and secondary purposes.

We submit that by diverting from the current process in this regard would directly impact firms' customers beyond any perceived benefit the proposed change may seek to achieve.

> 29. Are the existing protections effective to stop the unnecessary collection of personal information? a. If an individual refuses to consent to their personal information being collected, used or disclosed for a purpose that is not necessary for providing the relevant product or service, should that be grounds to deny them access to that product or service?

AFMA understands that the existing protections are effective to stop the unnecessary collection of personal information.

a. This depends on if the information collected is sufficient to fulfil other regulatory requirements, e.g., suitability requirement. If not, firms should be able to reserve the right not to provide such products/services to the client.

> 30. What requirements should be considered to manage 'consent fatigue' of individuals?

We understand that consent can be a vaguely understood concept that may result in customers experiencing 'consent fatigue'. For example, customers will frequently encounter instances of having to click 'I agree' to privacy related disclosures, potentially without taking the time to meaningfully appreciate the objective and effect of the disclosure. A lawful bases model, similar to the GDPR in which consent is an option, may be a more effective way to empower privacy control and transparency.

Implied consent

We note that businesses must, in some circumstances, rely on implied consent in its legitimate use and disclosure of personal information. We submit that, establishing express consent as the main way in which to permit personal information processing, would cause practical concerns for businesses with a significant customer base. For example, the administrative impost that would be incumbent on many financial institutions may likely compromise the ability to effectively communicate with their customers to the standard proposed.

AFMA suggests considering the following steps to minimise 'consent fatigue':

1) Establish which processing operations are subject to the requirement for consent.
2) Allow for exceptions or deemed consent, e.g. data processing limited to purposes deemed reasonable and appropriate such as commercial interests, individual interest or societal benefits with minimal privacy impact can be exempted from formal consent.
3) Focus should be centred on improving transparency rather than requesting systematic consents

We also submit that consent should be supplemented by allowing customers to choose what information they receive and how we use their personal information in the context of bank-to-customer communications. This notion applies a model similar to the Consumer Data Right to a broader privacy context.

We submit that the express consent proposal may constrain businesses beyond the expectation of customers and may impede the operation of business models that operate under the principle of good faith. This would not be to the overall benefit of consumers.

Exceptions to the requirement to obtain consent

31. Are the current general permitted situations and general health situations appropriate and fit-for-purpose? Should any additional situations be included?

Pro-consumer defaults

32. Should entities collecting, using and disclosing personal information be required to implement pro-privacy defaults for certain uses and disclosures of personal information?

Obtaining consent from children

33. Should specific requirements be introduced in relation to how entities seek consent from children?

The role of consent for IoT devices and emerging technologies

34. How can the personal information of individuals be protected where IoT devices collect personal information from multiple individuals?

Financial institutions have some of the most mature technological frameworks to ensure IoT security. Like other information security challenges IoT security requires robust data management frameworks and information rights management. Physical security, encryption, access controls, authorisation and access approval all play a role in protecting personal information. Reference to a set of standard guidance on IT and Cyber security should be considered for consistency. In this regard, the current regulatory landscape where multiple agencies (APRA, ASIC, ACCC) enforce overlapping and often inconsistent globally isolated guidance on information security is not an optimal approach to ensuring security outcomes.

Inferred sensitive information

35. Does the Act adequately protect sensitive information? If not, what safeguards should be put in place to protect against the misuse of sensitive information?

AFMA understands that current consent requirements sufficiently protect sensitive information. Firms adjust their security measures to the sensitivity of the collected data and some global firms have uniform security measures applied across the globe.

36. Does the definition of 'collection' need updating to reflect that an entity could infer sensitive information?

Direct marketing

37. Does the Act strike the right balance between the use of personal information in relation to direct marketing? If not, how could protections for individuals be improved?

AFMA understands that the right to object to direct marketing is reasonably included in the Act and aligned with GDPR.

Withdrawal of consent

38. Should entities be required to refresh an individual's consent on a regular basis? If so, how would this best be achieved?

As previously mentioned, frequently seeking consents from clients would unnecessarily damage the client experience. The data subject can have the right to withdraw their consent anytime. Organisations can also provide appropriate notifications to inform the individual of the purpose of the intended collection of personal data, with a reasonable period (provided that it's clearly defined) for the individual to opt-out of the collection, use, or disclosure of their personal data for that purpose.

39. Should entities be required to expressly provide individuals with the option of withdrawing consent?

Please refer to the answer above.

40. Should there be some acts or practices that are prohibited regardless of consent?

The principles of fair and lawful collection are sufficient to indicate the boundaries of practices involving personal information.

Emergency declarations

41. Is an emergency declaration appropriately framed to facilitate the sharing of information in response to an emergency or disaster and protect the privacy of individuals? 11

Regulating use and disclosure

42. Should reforms be considered to restrict uses and disclosures of personal information? If so, how should any reforms be balanced to ensure that they do not have an undue impact on the legitimate uses of personal information by entities?

Control and security of personal information

Security and retention

43. Are the security requirements under the Act reasonable and appropriate to protect the personal information of individuals?

APP11 references the Australian Government Cyber Principles which are not identical (though there are similarities) to the global NIST controls framework which many global firms employ.

Consistent frameworks for cyber controls consistent with global standards such as NIST best support good security outcomes. Again, AFMA cautions against creating new, overlapping and inconsistent guidance for securing information.

44. Should there be greater requirements placed on entities to destroy or de-identify personal information that they hold?

Access, quality and correction

45. Should amendments be made to the Act to enhance: a. transparency to individuals about what personal information is being collected and used by entities? b. the ability for personal information to be kept up to date or corrected?

Right to erasure

46. Should a 'right to erasure' be introduced into the Act? If so, what should be the key features of such a right? What would be the financial impact on entities? 47. What considerations are necessary to achieve greater consumer control through a 'right to erasure' without negatively impacting other public interests?

AFMA supports the notion of data minimisation and appropriate retention policies and procedures. We support a limited clearly defined framework for responding to data deletion requests in certain circumstances.

AFMA does not support a general 'right to erasure' as it is impractical in practice given the multiple complex offsite and archival (typically tape) storage arrangements that are necessary to comply with financial services law. Modern systems and data architecture make erasing data practically difficult e.g. information stored in back up emails may not be possible to erase. Blockchain data can be similarly unerasable.

Clear principles on how firms should respond to requests for erasure or destruction of data, should balance customer fairness and allow the banking and financial services sector

to continue to operate in good faith. Data erasure will not always be possible and it will often be not economic.

Any requirements around erasure must be limited to a best endeavours obligation and it must not apply to backups or challenge data owners to overcome technological challenges such as removing data piecemeal from back-up tapes. At a minimum, there must be exceptions that allow firms appropriate exemptions for regulatory reasons or to defend legal claims.

There is significantly more consultative work that should be undertaken before changes in this area are further progressed. This is an example of where the balance currently legislated in the objectives of the Act is essential to good policy outcomes. Any absolute requirements with uneconomic cost implications would increase service costs for all customers for limited benefit for the few.

Overseas data flows and third-party certification

48. What are the benefits and disadvantages of the current accountability approach to cross border disclosures of personal information? a. Are APP 8 and section 16C still appropriately framed?

AFMA recognises that the current APP framework is broadly suitable for overseas transfers of data. However, we note the government should consider further alignment of the principles to international standards, which will assist in reducing confusion or friction in operationalising overseas transfers domestically and offshore.

For this reason, we submit that government should adopt the recommendation in the ALRC Report 108 that the either the government, or the OAIC, should develop and publish a white list of laws and binding schemes in force outside of Australia that provide privacy protections that are substantially similar to the protection afforded by Act. This amendment would provide greater clarity as to the jurisdictions which Australian businesses may transfer personal information to.

Further, there are circumstances in which firms disclose personal data to overseas recipients, not on the "service provider - service received" basis but for the purpose of a business transaction. The recipient is not a processor of data on behalf of the disclosing firm but is a separate controller that complies with the local law applicable to it. In addition to the existing exemptions, we propose that APP8 should include allowing disclosure to overseas recipients for clearly defined permitted purposes.

49. Is the exception to extraterritorial application of the Act in relation to acts or practices required by an applicable foreign law still appropriate?

50. What (if any) are the challenges of implementing the CBPR system in Australia?

The APAC CBPR system has some challenges in its limited adoption both on a jurisdictional basis and by the larger data storage providers.

51. What would be the benefits of developing a domestic privacy certification scheme, in addition to implementing the CBPR system?

52. What would be the benefits or disadvantages of Australia seeking adequacy under the GDPR?

The benefits would be easier exchange of personal information between Australian entities and GDPR and GDPR-adequate countries. Most of the global institutions comply with GDPR requirements but are not formally recognized as adequate because of the local data privacy law.

Enforcement powers under the Privacy Act and role of the OAIC

53. Is the current enforcement framework for interferences with privacy working effectively?

54. Does the current enforcement approach achieve the right balance between conciliating complaints, investigating systemic issues, and taking punitive action for serious noncompliance?

We observe that at least four financial services regulators can enforce overlapping aspects of privacy regulation, namely with the greatest convergence on cyber-security risks (i.e. APP 11.1 and the Notifiable Data Breaches scheme, CPS 234, CDR Rules and ASIC's licensing requirements). These requirements are inconsistent and the approaches by regulators variant, creating an inefficient regulatory environment.

In the event of a single breach, in theory an organisation may be subject to sanctions from multiple different regulators. The misalignment between various regulators and their use of remedial action powers causes an imbalance in the relationship dynamic between industry and regulators, whereby excessive penalties may apply for any given breach event. We submit that due to the intersection of various regulations, there should be alignment between the various penalties that could apply. There is a significant opportunity for a rationalisation of the regulatory framework that would benefit the business environment and economy.

A further observation is that the regulators should be clear and consistent on what standards are applicable to cyber security. For example, a cyber-security incident may cause a notifiable data breach under the Privacy Act, but also attract regulatory action from ASIC. We suggest that in an effort to faithfully comply with APPs, regulatory agencies should align their agendas and avoid overlap.

Further, we encourage government to consider this review in the context of international best practice and perhaps aim to ensure that our domestic regulatory regime aligns to, or at least keeps up with, global standards.

55. Are the remedies available to the Commissioner sufficient or do the enforcement mechanisms available to the Commissioner require expansion? a. If so, what should these enforcement mechanisms look like?

AFMA has previously argued against excessive penalty regimes as inconsistent with the recommendations of the Attorney General's *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, distortionary and thereby inefficient, and unprincipled where they lack connection to the nature of the breach. Extremely high penalties were opposed by the Financial System Review[2] and would seem an unlikely path to prosperity.

During the COVID-19 period the regulatory stance altered by necessity to one of increased cooperation and accommodation. This type of approach is far more likely to optimise economic growth than punitive and more antagonistic stances.

Direct right of action

56. How should any direct right of action under the Act be framed so as to give individuals greater control over their personal information and provide additional incentive for APP entities to comply with their obligations while balancing the need to appropriately direct court resources?

The existing enforcement framework strikes the right balance of addressing individual complaints, providing organizations an opportunity to rectify, and taking measures against such organizations that do not take reasonable actions to remediate privacy violations.

More work is needed to consider how any proposal for a direct right could work efficiently without adversely affecting business activity and the courts. There are substantial risks involved in the direct right of action approach including that it could dis-incentivize transparency and hinder privacy innovation.

The punitive or abusive use of a direct right could add significant costs to the economy that would be ultimately not in the best interests of consumers. The Federal Government has recently tightened regulatory arrangements for litigation funding. It would be prudent to allow these reforms to settle before creating another potential source for this type of litigation. It may not be appropriate to introduce such additional costs at this time as businesses recover from the impact of COVID-19.

Statutory tort

57. Is a statutory tort for invasion of privacy needed?

A tort scheme could risk similar issues as those related to the creation of a direct right of action. Please refer to our answer to question 56.

[2] *Financial System Inquiry Final Report*, November 2014 p. 252.

58. Should serious invasions of privacy be addressed through the criminal law or through a statutory tort?

59. What types of invasions of privacy should be covered by a statutory tort?

60. Should a statutory tort of privacy apply only to intentional, reckless invasions of privacy or should it also apply to breaches of privacy as a result of negligence or gross negligence?

61. How should a statutory tort for serious invasions of privacy be balanced with competing public interests?

62. If a statutory tort for the invasion of privacy was not enacted, what other changes could be made to existing laws to provide redress for serious invasions of privacy?

Notifiable Data Breaches scheme – impact and effectiveness

63. Have entities' practices, including data security practices, changed due to the commencement of the NDB Scheme?

Most firms in financial markets have a high standard of data security and data breach escalation practices and policies that are based on the GDPR requirements.

64. Has the NDB Scheme raised awareness about the importance of effective data security?

65. Have there been any challenges complying with the data breach notification requirements of other frameworks (including other domestic and international frameworks) in addition to the NDB Scheme?

Interaction between the Act and other regulatory schemes

66. Should there continue to be separate privacy protections to address specific privacy risks and concerns?

67. Is there a need for greater harmonisation of privacy protections under Commonwealth law? a. If so, is this need specific to certain types of personal information?

68. Are the compliance obligations in certain sectors proportionate and appropriate to public expectations?