PRIVACY ACT REVIEW

SUBMISSION TO THE ATTORNEY-GENERAL'S DEPARTMENT

5 December 2020

EXECUTIVE SUMMARY

1. ANZ thanks the Attorney-General's Department (**AGD**) for the opportunity to comment on the Issues Paper *Privacy Act Review* (**Issues Paper**).

2. With the rapid development of the digital economy and the exponential increase in data, Australia's privacy regime is now more critical than ever. We welcome the Issues Paper as an important step towards ensuring that Australia's privacy settings empower consumers, protect their data and serve the Australian economy.

3. Technological advances have demonstrated the potential of data to change our lives for the better in a variety of ways. Combined with algorithms it can be used to predict future behaviour or events and inform the decisions of government, organisations and individuals. Australia's future prosperity will depend on innovation and sound data driven decisions. ANZ currently provides direct feeds of de-identified aggregate credit and debit card transaction data to the NSW government's Data Analytics Centre to enable faster, better understanding and responses to the economic and social impacts of the COVID-19 pandemic. The value of access to different types of data in responding to the pandemic was highlighted by Dr Steven Kennedy, Secretary to the Treasury.

> *The Weekly Payroll Jobs and Wages series developed by the ABS using Single Touch Payroll Data enabled us to track the labour market in close to real time. We also used data on unemployment benefit claims from the Department of Social Services, data on spending from the banks, customs data from the Department of Home Affairs, data on insolvencies from ASIC and novel data such as from supermarkets, Google, Apple and Seek…These information sources proved to be invaluable, and we have drawn on them heavily as we have adjusted our forecasts.*[1]

4. While technologies like artificial intelligence (**AI**) offer enormous potential, they may also result in unintended harms. The privacy of individuals may be compromised. Bias in data sets can result in insights which discriminate unfairly. These sorts of outcomes will undermine trust in the technology.

5. For emerging technologies to fulfil their promise to drive prosperity and improve our lives, it is essential to balance robust privacy protections with data utility. Strong data governance requirements will help to promote consumer trust and enable data to be

[1] 05 NOV 2020: TREASURY: Transcript of the Secretary to the Treasury's, Dr Steven Kennedy's, Speech at the Australian Business Economists - 'Policy and the evolution of uncertainty'

safely used and shared for innovative purposes. The privacy regime, together with other safeguards,[2] should underpin these two objectives.

6. To assist the AGD achieve its policy objectives, we have made some observations below on selected questions in the Issues Paper. These comments are made within the context of our overall support for a strengthened privacy regime which is fit for the digital economy. The comments are organised into:

    - First, our key points in response to questions in the Issues Paper; and
    - Second, responses to other selected consultation questions in the Issues Paper.

7. Our key points are summarised below. We set these points out in more detail in the section that follows the summary.

    - **Appropriately define the scope of personal information** – We support updating the definition of personal information to provide greater certainty as to when it captures technical data. We question whether defining 'personal information' in line with the *General Data Protection Regulation* (European Union) (**GDPR**) will necessarily provide legal certainty in Australia.
    - **Promote more accessible notices suited to digital channels** – We support the use of layered notices and a standardised privacy language and framework for notices.
    - **Strengthen requirements for obtaining valid consent** – We agree that requirements for valid consent should be strengthened to include 'a clear affirmative act that is freely given, specific, unambiguous and informed'[3] and that consents should generally not be bundled. We support retaining the use of consent as a basis for collection, use or disclosure of personal information as currently permitted under the *Privacy Act 1988* (Cth) (**Privacy Act**). We do not support requiring organisations to obtain consent for any collection, use or disclosure unless it is necessary for the performance of a contract to which the

[2] Anti-discrimination law and related technical guidance will be important safeguards in driving responsible and thoughtful use of new data driven technologies. The Australian Human Rights Commission, collaborating with the Gradient Institute, Consumer Policy Research Centre, CHOICE and CSIRO's Data61 have recently published a technical paper *Addressing the problem of algorithmic bias* offering guidance to avoid unfairness in decision-making systems. The Australian Human Rights Commission is also expected to release its report on human rights and technology in early 2021 commenting on various proposals to encourage responsible and ethical use of emerging technologies including in relation to law reform and ethical frameworks.

[3] Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, June 2019) Recommendation 16(c), p. 35

consumer is a party, required under law or in the public interest.[4] Valid concerns about excessively expansive uses of existing grounds of use could be addressed through guidance on the scope of those grounds.

- **Enable the utility of data** – We caution against imposing obligations which overly restrict the use and disclosure of de-identified information. We believe the current scope of regulating personal information in the Privacy Act is appropriate and that the constraints in the law are sufficient to protect the privacy of individuals. We recognise that de-identifying personal information is technically complex and the use or release of poorly de-identified information gives rise to privacy risks. These risks could be addressed by measures concerning robust de-identification measures and prohibiting improper re-identification of data.

8. We look forward to the next steps in the AGD's review and would welcome the opportunity to discuss the points in this submission with the Department if this would be useful.

[4] Ibid

KEY POINTS

Appropriately define the scope of personal information

Questions responded to:

2. **What approaches should be considered to ensure the Act protects an appropriate range of technical information?**
3. **Should the definition of personal information be updated to expressly include inferred personal information?**

General

9. ANZ supports greater certainty and clarity in Australia's privacy law to enhance (1) consumer understanding and trust regarding the handling of their data and (2) business compliance.

10. The definition of 'personal information' triggers the operation of the Privacy Act. Data which falls outside the scope of 'personal information' is not regulated. The Grubb case[5] highlighted this definition's legal uncertainty as it applies to technical data 'about an individual'. We agree that the definition of 'personal information' should be updated to provide greater certainty as to when technical data constitutes 'personal information'.

Technical information

11. In the Grubb case the Federal Court considered the definition of 'personal information'. The Court clarified that determining whether information falls within the definition requires factual evaluation as to whether (1) the information is about an individual and (2) the identity of the individual can be reasonably ascertained.[6]

12. The Australian Competition and Consumer Commission (**ACCC**) has suggested updating the definition of personal information in line with the GDPR.[7] Under the GDPR 'personal data' captures 'any information relating to an identified or identifiable natural person.'[8] In the light of the Grubb case, we question whether changing the expression from 'about an' to 'relating to' an individual will provide greater certainty in Australia in respect of the definition of personal information. Determining whether information 'relates to' an individual may also require evaluation based on the facts of each case.

13. It will be important that any revised definition specifies that different categories of technical data, including online identifiers, will be personal information only when they are

[5] *Privacy Commissioner v Telstra Corporation Ltd* [2017] FCAFC 4
[6] Ibid, [63]
[7] Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, June 2019), p. 458
[8] GDPR, Article 4

sufficiently connected to an identifiable individual rather than assuming that particular types of data are always personal information. For instance, if IP addresses were specified as 'personal information' in most cases, it would be difficult for an organisation to comply with the Privacy Act's notification requirements as, for the most part, there will be no identifiable individual linked to the information. If a tracked IP address were linked to an online environment where an individual is authenticated, such as internet banking, then it would be personal information.

14. We note the Office of the Australian Information Commissioner's (**OAIC**) guidance that "[d]etermining whether a person is 'reasonably' identifiable will require a contextual consideration."[9] It may be appropriate to extend this guidance to provide examples as to when different categories of technical information are regarded as sufficiently connected to an identifiable individual to satisfy the definition of personal information.

Inferred information

15. We believe that inferred information applied to an identified individual's profile is already captured by the definition of personal information: It is an opinion about that person. This position could be made explicit to remove any ambiguity. In doing so it will be important to ensure that there is clarity as to when inferred information is 'collected' and becomes personal information relating to an identified individual. When inferred information (such as an insight about a particular cohort of people) is applied to or collected and held against an individual's profile, the inference would be personal information. If that inference is not applied or collected against the profile it is not personal information.

Biometric data

16. We would also welcome further guidance on the definition of the Privacy Act's terms of 'biometric information', 'automated biometric verification', 'biometric identification' and 'biometric templates'. For example, will behavioural characteristics such as gait, mouse use recognition or typing recognition be considered 'biometric information'; and when might biometric data not be 'sensitive information'?

Promote more accessible notices

Questions responded to:

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

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

[9] Office of the Australian Information Commissioner, *What is personal information?* May 2017, p.8

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?

General

17. Appropriate notice is essential to ensuring consumers understand how, why and what data is being captured about them. This transparency underpins consumers' trust and confidence in the organisations they choose to engage with.

18. We recognise that terms and conditions, privacy policies, and collection notices can be opaque and complex. We support measures that would make privacy notices more accessible.

Layered notices

19. We would support changes to the law that make collection disclosures more suitable for digital channels and allow them to be arranged in a way that optimises consumer understanding. Specifically, the Privacy Act could better facilitate layered disclosure. A layered notice organises information into key topics with short summaries at the top layer and provides links to subsequent layers that give more detailed information about each topic.[10] Layered notices offer the advantage of efficient and more targeted disclosure, allowing consumers to view higher level information about, for instance, purposes for collection, secondary purposes and third party disclosures, with the ability to 'click through' to more detailed information about areas of particular interest.

20. Australian Privacy Principle (**APP**) 5 requires organisations to provide collection notices at or before the time of collection, or if not practicable, as soon as practicable after collection.[11] The required act is to either 'notify the individual' of the relevant matters or 'otherwise ensure that the individual is aware' of any such matters. We do not believe these existing provisions are flexible enough to permit organisations to use layered notices. This is because the obligation is to either notify them upfront, or ensure they are aware. We recommend that APP 5 is amended to make it explicit that providing a link to information would satisfy the obligation to ensure the individual has been made aware of the relevant matters even though the individual may choose not to access it.

Standardised privacy language and framework for notices

21. ANZ would support the development of a standardised privacy language and framework for notices. This could be standardised wording for collection purposes such as 'product

[10] Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, June 2019), p. 404

[11] Privacy Act, Schedule 1 – Australian Privacy Principles, Part 2 – Collection of personal information, Australian Privacy Principle 5 – notification of the collection of personal information, 5.1

development' and 'personalised services'.[12] This would have the dual benefits of making notices more intelligible for consumers and providing more certainty for business regarding notice requirements, both in terms of wording and structure of required notices. Educating consumers about a standardised privacy language could make them more confident with privacy concepts and aid their understanding and trust of organisations' use of data. Broad consumer experience testing should inform the development of any standardisation.

Harmonisation with Part IIIA

22. While we understand Part IIIA of the Privacy Act is outside the scope of this Review, we would recommend that any revision of the notice requirements for collection of personal information include the corresponding provisions of Part IIIA and the Privacy (Credit Reporting) Code. These require credit providers to provide notice of information about credit reporting when collecting personal information which the credit provider is likely to disclose to a credit reporting body.[13]

23. It is important these Part IIIA provisions are harmonised with notice requirements in APP 5 because, for credit providers, disclosures complying with these two sets of notification requirements are usually contained within the one collection statement or framework.

Strengthen requirements for obtaining valid consent

Questions responded to:

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

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?

General

24. The use of meaningful consent as a basis for handling personal information can empower consumers. Consumer consent is fundamental to building trust in the operation of the Consumer Data Right.

[12] This is explored further in the Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, June 2019), p. 463

[13] Privacy Act, section 21C

25. We support the strengthening of the requirements for consent where it is needed to permit the collection, use or disclosure of personal information which would not otherwise be allowed.

Avoid over reliance on consent

26. We are mindful that the control consumers have should be meaningful. We are concerned that a privacy model which requires consent to collect, use and disclose information for each primary purpose necessary for the functions or activities of the organisation and each related secondary purpose diminishes its value. The control that a consumer has in relation to these purposes is whether or not to engage with the organisation. Seeking consent to the use and disclosure of information in situations where an organisation will not engage with the consumer in the absence of the consent makes it meaningless. If a consumer has no genuine opportunity to withhold consent, any consent provided will not be voluntary: This would make it invalid.

27. Where use and disclosure goes beyond primary and related secondary purposes, consent can be an effective way of providing consumers genuine control over the handling of their data.

28. We recognise valid concerns that:

- organisations may interpret the primary purpose of collection broadly to avoid the need to obtain consent for purposes that go beyond what is reasonably necessary (1) to perform a contract or (2) for the functions or activities of the organisation; and
- consent bundled into the terms and conditions for supply of the core consumer facing service can be used as a safety mechanism to protect organisations where it is unclear whether their use or disclosure is a 'related secondary purpose within the reasonable expectation of the individual'. Consumers cannot freely consent when consent is bundled in this way.

29. We consider that these concerns could be addressed by providing further specific guidance or standards:

- on information that may be considered 'reasonably necessary for one or more of the entity's functions or activities' under APP 3; and
- on 'related secondary purposes within reasonable expectation' of the consumer under APP 6 to assist organisations to determine when consent is genuinely required rather than using it as a safety net.

Valid and meaningful consent

30. The *Australian Privacy Principles Guidelines*[14] require that consent should be informed, voluntary, current and specific and the individual should have capacity to understand and communicate their consent. We agree with the ACCC's recommendation that consent requirements be strengthened in line with the GDPR to require:

    - 'a clear affirmative act that is freely given, specific, unambiguous and informed (including about the consequences of providing or withholding consent);'[15]
    - de-bundling consents; and
    - any settings for data practices relying on consent to be pre-selected to 'off'.[16]

31. Any reform to the requirements for valid consent may need to recognise particular situations. For example, the requirement to obtain consent to collect sensitive information from employees would need particular consideration if the employee records exemption were repealed. Employers regularly collect sensitive information (such as sick leave) from employees in the course of their employment. Given logical concerns about the ability of an employee to freely consent to their employer collecting sensitive information, it may be appropriate to consider limited exceptions to the requirement for consent.

32. With regard to de-bundling consents, requirements should allow for innovative measures which could help to minimise consent fatigue. For instance, consumers should be able to consent to multiple purposes with a single affirmative act provided they also have the option to consent (or not) to each purpose individually if they prefer.

Enable the utility of data

Question responded to:

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

General

33. Under the Privacy Act, personal information can only be used and disclosed for certain purposes.[17] As de-identified information is no longer associated with an individual, it is

[14] OAIC, *Australian Privacy Principles Guidelines* (Combined July 2019), Chapter B: Key Concepts, p. 10

[15] Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, June 2019) Recommendation 16(c), p. 35

[16] Ibid

[17] Privacy Act, Schedule 1 – Australian Privacy Principles, Part 2 – Collection of personal information, Australian Privacy Principle 6 – use or disclosure of personal information

not subject to the Privacy Act.[18] When de-identification is done effectively, it can enable information to be shared and used while protecting individual privacy.

34. Regulating de-identified information would likely constrain its use and disclosure compromising its utility. The current scope of regulating personal information is appropriate and existing constraints in the law are sufficient to achieve the right level of protection for personal information. Where de-identification techniques applied to personal information are inadequate and individuals continue to be reasonably identifiable, the Privacy Act will apply.

35. We recognise that the process of applying appropriate de-identification techniques is complex. To promote consumer trust in the process of de-identification, measures could be considered to further reduce the risk of re-identification of information. In particular, consideration could be given to strengthening de-identification techniques and introducing an offence (with appropriate defences) of knowing or reckless re-identification without authorisation.

Avoid over-regulating de-identified information

36. De-identification is a risk management '…process involving the removal or replacing of direct identifiers in a dataset, followed by the application of any additional techniques or controls required to remove, obscure, aggregate, alter and/or protect data in some way so that it is no longer about an identifiable or reasonably identifiable individual.'[19]

37. To be considered de-identified, the risk of re-identification in the data access environment must be very low with no reasonable likelihood of re-identification of the information.[20] The OAIC and Data61 recognise that it is not possible to eliminate all risk of re-identification.[21] Any revision to the Privacy Act definition of 'de-identified' requiring that the risk of re-identification be reduced to zero would, in practice, make it impossible for personal information to be considered 'de-identified'. Even if robust de-identification techniques are applied, the Privacy Act would continue to regulate the information as 'personal information' limiting its use and disclosure. This would have a chilling effect on the utility of de-identified information and should be avoided.

38. To properly de-identify information, organisations must assess (1) the level of data modification required and (2) any environment the data will be released into, to ensure that the risk of re-identification is very low. Organisations disclosing information that has

[18] Privacy Act, section 6
[19] OAIC and Data 61, *The De-Identification Decision-Making Framework*, 18 September 2017, p. 67
[20] OAIC, *De-identification and the Privacy Act* March 2018, p. 3
[21] OAIC and Data 61, *The De-Identification Decision-Making Framework*, 18 September 2017, p. 10

been stripped of identifiers must consider whether the information would still be de-identified in the hands of the specific prospective recipient. If the prospective recipient has tools and other data assets that could reasonably enable them to re-identify the information, it would be a disclosure of personal information and regulated by the Privacy Act. Under existing constraints, in cases where de-identified information may switch to personal information in different contexts, APPs 6, 8 and 11 will continue to be relevant to the handling of that information.[22]

39. Any requirement to obtain consent to de-identify personal information is likely to significantly inhibit the utility of this data and the societal and economic benefits it could provide with little to no material benefit to individual privacy. Where de-identified information is to be used with data analytics, questions also arise about the ability of consumers to give properly informed consent. It may not be possible to understand the potential implications of consent to the use of de-identified information with technologies like AI because insights that may be revealed cannot be foreseen in advance.

40. Applying all of the APPs to de-identified information would present practical difficulties. For example, many of the APP requirements, such as notification of collection under APP 5, ensuring information collected is accurate, up-to-date and complete under APP 10 and providing access to and correction of information under APP 12, could not be satisfied where the information no longer relates to an identified individual. If de-identified information was regulated, it would likely need its own regime of rules and constraints.

Strengthening de-identification

41. While we caution against applying consent and other APP requirements to de-identified information, we recognise that the practice of applying de-identification techniques can be inconsistent and lack the appropriate rigour.

42. Consideration could be given to strengthening de-identification practices through legal standards, perhaps by drawing on the de-identification decision making framework issued by the OAIC and CSIRO's Data 61.[23]

43. Further, the Data Protection Act 2018 (UK) has a re-identification offence with various defences including a public interest defence. The introduction of a similar offence in Australia could be considered. The UK offence provides that:

---

[22] Ibid, p. 12

[23] OAIC and Data61, *De-identification Decision-Making Framework*, 18 September 2017

It is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data [24]

OTHER POINTS

Emergency declarations

Question responded to:

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?

44. Where an organisation receives a request from a State or Territory authority to provide personal information to assist with a public health situation (for example COVID-19 contact tracing efforts), we believe:

- Part VIA (Dealing with personal information in emergencies and disasters) does not permit disclosure of personal information to a State or Territory authority for public health reasons.
    - Where there is a declaration of emergency under section 80J, personal information can only be disclosed to a Commonwealth agency.
- The 'permitted health situations' set out in section 16B are not broad enough to permit disclosure of personal information on request to assist a State or Territory authority for a public health reason.
- The organisation may only respond where we are required to do so by State or Territory law.
    - A requirement to disclose pursuant to law would make the disclosure permissible under APP 6.

45. Consideration could be given to expanding:

- Section 80P to enable disclosure by an organisation to a State or Territory authority; or
- The 'permitted health situations' set out in the Act.

[24] Section 171 and 172

Security

Question responded to:

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

46. The requirement in APP 11 to take 'reasonable steps' to protect personal information continues to be appropriate. It enables security risk assessments and technical and operational responses calibrated to the nature of the personal information and the different risks arising from handling of personal information across a range of circumstances.

47. It would be difficult to effectively prescribe security requirements appropriate to all of the ways that personal information is collected, stored, used and disclosed. Even if it were possible to effectively do so, ensuring such prescribed standards respond to the rapidly changing risk and threat landscape (and equally rapidly changing range of security measures being developed in response) would be a significant burden on Government and could slow innovation.

Right to Erasure

Question responded to:

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?

48. To assist consideration of this issue we note that any right to erasure would need to include an exception for legal retention and risk management requirements. As these requirements can be broad, it will be important to clearly define the types of information that fall within the exception.

Overseas data flows

Question responded to:

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?

International Money Transfers

49. We request that APP 8 be reviewed to accommodate the issues addressed in the Public Interest Determinations sought by ANZ in 2014 and 2019. This could be achieved through incorporating an additional exception for international money transfers (IMT) in APP 8.2 or through introducing a new permitted general situation in section 16A of the Privacy Act.

50. Prior to the repeal of the National Privacy Principles, remitting banks could transfer account and other identifying information of the sender or the beneficiary to a foreign financial institution (as needed in order to process the IMT). APP 8 (which replaced National Privacy Principle 9) requires that before a remitter discloses personal information to an overseas recipient, the remitter must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs.

51. ANZ sought relief under Part VI of the Privacy Act from a contravention of APP 8, section 15 and section 16C(2) where there is a cross-border disclosure of a beneficiary's personal information for the process of an IMT. The OAIC recognised that it is impracticable and difficult for a remitting bank to meet the exceptions set out in APP 8.2 and on 14 February 2020, issued the most recent Public Interest Determination to provide ANZ (the RBA and other financial institutions) with relief that remitting banks would not be in breach of the APPs in processing IMTs.

Recognising 'reasonable steps'

52. By making an APP entity responsible for the acts or practices of overseas recipients regardless of 'reasonable steps' taken to ensure overseas recipients comply with the APPs, the Privacy Act arguably favours retention of personal information onshore which is not always optimal. Data offshoring has many advantages and ideally would not be prejudiced by this aspect of the Privacy Act. This is particularly so when regard is had to:

- the fact that any additional or heightened risks posed by offshoring can be taken account of in determining what are 'reasonable steps';
- the benefits of geographic diversity in management of data including:
  - improved system resilience through stronger Business Continuity and Disaster Recovery arrangements; and
  - 24x7 managed operations with follow the sun support; and
- the advantages of dealing with third party service providers in their home jurisdictions in preference to fourth party subcontractors in Australia.

For these reasons, we think there would be benefit in amending section 16C to better recognise "reasonable steps" taken by an entity under APP 8.

'Whitelist'

53. Consideration could be given to the OAIC maintaining a white list of the jurisdictions with laws or binding schemes that 'overall, [are] at least substantially similar to the way in which the APPs protect the information'. This would give organisations clarity about which jurisdictions information can be sent to in compliance with APP 8.2(a)(i).

54. This would reduce red tape and potentially significant costs for organisations that have to undertake their own assessment, often using the services of global law firms to assist in attempting to determine the adequacy of foreign privacy laws.

Notifiable Data Breaches Scheme – impact and effectiveness

Questions responded to:

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

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?

55. The NDB Scheme has resulted in improved security standards and increased awareness about the importance of effective data security. This is confirmed by notifiable data breach statistics reported by the OAIC including a large number of 'voluntary notifications'.[25]

56. We consider that the timeframes for assessment ('expeditious assessment'), statement ('as soon as practicable') and notification ('as soon as practicable') are appropriate and permit adequate time to ensure each is meaningful, helpful and not premature or unnecessarily alarming to potentially impacted individuals.

57. While harmonisation is generally desirable, we consider it is probably not possible in relation to statutory, privacy or security breach notification timeframes. This is because of the number of different notifications potentially required and the different, underlying motivations for each. For example:

- NDB Scheme – protection of individuals;
- Australian Prudential Regulation Authority Prudential Standard CPS 234 Information Security – mitigation of impact on the bank/finance sector; and
- ASX Limited Listing Rule 3.1 Continuous Disclosure – protection of investors.

58. We agree with the OAIC that multi-party data breaches are an area for improvement for the NDB scheme and suggest there may be a greater role for the OAIC in navigating these.

[25] Issues Paper, p. 78

59. There can also be challenges for an organisation where a third party suffers a breach in respect of information of the organisation provided by others. For ANZ, this could be ANZ account information provided to a third party by mutual customers. The organisation may want the customer to be notified of a breach but the third party fails or refuses to do so. In these situations, it isn't always clear that the organisation has the ability to use customer personal information which it obtains following the third party's data breach pursuant to a "permitted general situation". In particular, arguing that the unlawful activity or serious misconduct "relates to [the organisation's] functions or activities" requires a broad reading of section 16A(1) Item 2 Column 3(a) of the Privacy Act.

60. One way to improve the ability to respond in the interests of customers in such circumstances would be to extend the scope of the Item 2 Column 3(a) to "… the entity's functions, activities, products, services or customers …".

ENDS