NEW ZEALAND BANKERS ASSOCIATION

Submission

to the

Justice Committee

on the

Privacy Bill

7 June 2018

NEW ZEALAND BANKERS ASSOCIATION
Level 15, 80 The Terrace, PO Box 3043, Wellington 6140, New Zealand
TELEPHONE +64 4 802 3358 EMAIL nzba@nzba.org.nz WEB www.nzba.org.nz

About NZBA

1. NZBA works on behalf of the New Zealand banking industry in conjunction with its member banks. NZBA develops and promotes policy outcomes that contribute to a strong and stable banking system that benefits New Zealanders and the New Zealand economy.

2. The following seventeen registered banks in New Zealand are members of NZBA:

- ANZ Bank New Zealand Limited
- ASB Bank Limited
- Bank of China (NZ) Limited
- Bank of New Zealand
- MUFG Bank, Ltd
- China Construction Bank
- Citibank, N.A.
- The Co-operative Bank Limited
- Heartland Bank Limited
- The Hongkong and Shanghai Banking Corporation Limited
- Industrial and Commercial Bank of China (New Zealand) Limited
- JPMorgan Chase Bank, N.A.
- Kiwibank Limited
- Rabobank New Zealand Limited
- SBS Bank
- TSB Bank Limited
- Westpac New Zealand Limited

Background

3. NZBA welcomes the opportunity to provide feedback to the Justice Committee on the Privacy Bill (**Bill**) and commends the work that has gone into developing the Bill.

4. If you would like to discuss any aspect of the submission further, please contact:

Antony Buick-Constable
Deputy Chief Executive & General Counsel
04 802 3351 / 021 255 4043
antony.buick-constable@nzba.org.nz

Introduction

5. NZBA supports a refresh of New Zealand's privacy legislation, and notes that international privacy laws have significantly evolved since the drafting of the Bill. In particular, there has been a trend towards more robust regulation of personal information, for example Australia's recent amendment to its Privacy Act and the implementation of European Union's General Data Protection Regulation (**GDPR**). Given those international trends, and the importance of legislation that is future-

proof and consistent with international legislation and regulation, NZBA encourages the Committee to consider substantive changes to the Bill and further public consultation on any such changes.

Clause 19

6. NZBA has the following general comments in relation to the Information Privacy Principles (**IPP**):

IPP 4

7. IPP 4 sets out the method of collection of personal information.

8. Section 6 of the Privacy Act 1993 (**Act**) states IPP 4 in the following terms:

> Personal information shall not be collected by an agency – by unlawful means, or by means that, in the circumstances of the case, are unfair or intrude to an unreasonable extent upon the personal affairs of the individual concerned.

9. Whereas, cl 19 of the Bill states IPP 4 in the following terms:

> An agency may collect personal information only by a lawful means, and by a means that, in the circumstances of the case (having regard particularly to the age of the individual concerned), is fair and does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

10. This change introduces a different, and potentially higher, standard with respect to IPP 4.

11. NZBA considers this change may cause confusion and undermine existing precedent in this area. We note that neither the Law Commission review, nor the previous Government's response to that review, made any recommendation for changes to this principle. Accordingly, in the absence of any clear justification for the change in wording, we submit that the status quo ought to be retained.

IPP 9

12. As currently worded, IPP9 is extremely onerous. NZBA considers that the obligation could instead be aligned with the Australian approach; where an entity no longer needs personal information for any purpose for which the information may be used or disclosed under the APPs, the entity must take reasonable steps to destroy the information or ensure that it is de-identified.

Clause 27

13. NZBA considers that cl 27(6) of the Bill should provide that the Privacy Commissioner (**Commissioner**) is permitted to grant an authorisation to deviate from IPPs on the grounds that the burden to the agency of compliance is disproportionate to the detriment to the public of non-compliance.

Clause 58

14. Clause 58 introduces an explicit ability to impose conditions on the use/disclosure of information provided in response to a request for personal information (previously

only indicated as a possibility under s 66(2)(iii) of the Act). However, it is unclear what the anticipated remedy would be for any breach of the conditions imposed and further clarity as to how this ability is intended to function would be of assistance.

Clause 62

15. Clause 62 sets out the ways in which information may be made available, including the ways in which an individual may request information, and the obligation on agencies to provide the information in the way requested unless an exception applies.

16. NZBA queries why only two of the three exceptions contained in s 42(2) of the Act have been replicated in cl 62 of the Bill (s 42(2)(c) has been omitted – providing the information in the format requested would prejudice the interests protected by ss 27-29 and there is no countervailing public interest).

17. NZBA seeks clarification as to why this exception has been removed as the change does not appear to have been contemplated by the Law Commission in its review, or the previous Government in its response to that review.

Clauses 84 and 87

18. Clauses 84 and 87 enable the Privacy Commissioner to refer a matter to the Director of Human Rights Proceedings (**DHRP**) prior to investigating a complaint or prior to the completion of an investigation where:

    (a) the Commissioner is unable to secure a settlement or satisfactory assurance;

    (b) it appears that a term of settlement previously secured between the agency and the complainant has not been complied with; or

    (c) it appears that the action that is the subject of the complaint was done in contravention of any term of settlement or an assurance previously secured under the Privacy Act.

19. NZBA consider that (b) and (c) are reasonable as they provide a path for enforcing an undertaking previously made by an agency. However, we are concerned about (a) as we consider that it could result in a complaint being referred to the DHRP for action in circumstances where the agency has not had an opportunity to go through the proper investigation process.

20. We also query how cls 84 and 87 operate in the context of cl 102, which provides that the DHRP may take proceedings on behalf of a complainant on referral from the Privacy Commissioner *after the completion of an investigation*.

Clause 92

21. Clause 92(2)(a) of the Bill provides that the Commissioner may impose a time limit for a person to provide information, documents, or things within that person's possession or control that the Commissioner considers may be relevant to an investigation. If no date is specified in the notice, a 20 working day period applies under clause 92(2)(b).

22. NZBA considers that the default position should be that organisations have a timeframe of no less than 20 working days within which to provide the information required under clause 92(2)(a). That is because it may not be operationally feasible for organisations to provide this information in shorter timeframes. However, the Commissioner should also have the ability to request information in a shorter period where there is an appropriate reason for this (in line with the way urgent requests are dealt with under the Act).

Part 6, subpart 1

23. NZBA considers that it is important that affected individuals properly consider notifications of data breach. As such, setting the right threshold for notification is important. Impacts of the data breach should be material to the individual and easily understandable in the notification.

24. Part 6, subpart 1 of the Bill contains provisions relating to notifiable privacy breaches. The current drafting of those provisions takes a single tier approach to notification – requiring notification of privacy breaches to both the Privacy Commissioner and affected individuals (apart from certain limited exclusions). It also sets a relatively low threshold for breaches which are required to be notified (there must have been a breach which has caused harm or which may cause harm).

25. We note that the Bill creates a different threshold to the current Australian data breach notification scheme which requires notification to the regulator where there has been a privacy breach resulting in a serious risk of harm, and to affected individuals when the agency has not been able to prevent the risk of harm with remedial actions. It also sets a different threshold to GDPR, which requires notification to the regulator where there has been a privacy breach resulting in a real risk to an individual's rights and freedoms, and notification to the individual where there is a high risk to the individual's rights and freedoms.

26. NZBA considers the Bill should be more closely aligned with the Australian framework for notifiable breaches. We believe that would minimise the costs of compliance and will be likely to minimise confusion arising from having multiple differing thresholds for breach notification across different jurisdictions.

27. Additionally, as with the Australian regime, we believe that there should be an exception to the reporting of privacy breaches where the organisation takes action to remedy the breach and prevent serious harm from occurring to the affected individuals. If the organisation is comfortable that the breach is unlikely to result in serious harm to any of those individuals, then reporting should not be required. If adopted, this may require amendment to cl 122.

28. If our submissions above are not accepted, NZBA seeks guidance on how 'notifiable privacy breaches' may be identified as this may be difficult to determine in practice. The proposed process for identifying a 'notifiable breach' is based on the definition for 'harm' (cl 75(2)(b)). That definition, especially the matters set out at cl 75(2)(b)(iii), is wide and terms like 'may cause' and 'significant humiliation' are subjective.

29. Finally, to enable agencies to develop appropriate compliance processes, we consider that there should be a 12-month implementation period for Part 6 of the Bill (similar to the Australian legislation).

Clause 118

30. Clause 118 provides that '[a]n agency must notify the Commissioner as soon as practicable after becoming aware that a notifiable privacy breach has occurred'.

31. Other jurisdictions, such as Australia, provide a period of time within which agencies can assess whether the potential breach is notifiable. We suggest the following approach be adopted:

    (a) an assessment period of up to 30 days from the day the agency first becomes aware of a suspected breach; and

    (b) where the agency determines that the breach is eligible for reporting, then the agency must notify the relevant parties within the required time frame (ie as soon as practicable to affected individuals/no later than 72 hours to the Commissioner).

Clauses 109, 122 and 133

32. Clauses 109, 122 and 133 set out the Commissioner's power to enforce when an agency has failed to comply with an order 'without reasonable excuse'.

33. NZBA seeks guidance as to what constitutes 'reasonable excuse'. We note the Commissioner's s 26 report dated 3 February 2017 which states:[1]

> Current experience of agencies obstructing statutory investigation processes has shown that the "reasonable excuse" defence means that the offences are not operating satisfactorily. A person or agency who fails to comply with the Commissioner's lawful requirements can employ various excuses including a mistaken belief that they need not comply with the requirement

    Given the potential for misuse or confusion, clearer language and/or guidance is required.

34. In addition, to the extent that the submission in paragraph 27 is accepted, this will have implications for the Commissioner's power to enforce when an agency has failed to comply with an order 'without reasonable excuse'.

Clause 210

35. Clause 210 is limited to adverse comments contained in a 'statement or report'. NZBA considers that this should be amended to apply to 'any communications made' to take into account the range of different communication methods available.

[1] Report to the Minister of Justice under s 26 of the Privacy Act, 3 February 2017, para 101