NEW ZEALAND BANKERS ASSOCIATION

Submission

to the

Ministry of Justice

on the

Engagement Document: Possible changes to notification rules under the Privacy Act 2020

30 September 2022

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. The New Zealand Bankers' Association (**NZBA**) is the voice of the banking industry. We work with our member banks on non-competitive issues to tell the industry's story and develop and promote policy outcomes that deliver for New Zealanders.

2. The following eighteen 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
   - 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.
   - KB Kookmin Bank Auckland Branch
   - Kiwibank Limited
   - MUFG Bank Ltd
   - Rabobank New Zealand Limited
   - SBS Bank
   - TSB Bank Limited
   - Westpac New Zealand Limited

Introduction

NZBA welcomes the opportunity to provide feedback to the Ministry of Justice (**MoJ**) on the Engagement Document: Possible changes to notification rules under the Privacy Act 2020 (**Engagement Document**). NZBA commends the work that has gone into developing the Engagement Document.

Contact details

3. If you would like to discuss any aspect of this submission, please contact:

Antony Buick-Constable
Deputy Chief Executive & General Counsel
antony.buick-constable@nzba.org.nz

Brittany Reddington
Associate Director, Policy & Legal Counsel
brittany.reddington@nzba.org.nz

Summary

NZBA generally supports developments to bolster an individual's right to privacy. However, we also consider that legislative changes should typically occur in response to a clear problem or need.

These changes are likely to have a number of adverse impacts on both consumers and businesses. Therefore, any problem definition and resulting benefits that might flow from the proposed changes should be identified at the outset. In our view, the current notification regime under the Privacy Act sufficiently covers indirect collection of personal information, and is broadly aligned with overseas jurisdictions.

If MoJ decides to go ahead with these changes, we recommend a further consultation clearly outlining the problem definition and proposed changes, with further information on the detail and granularity of the requirements. Any changes should be narrow and directly respond to the problems identified, with clear exceptions to avoid any adverse consequences.

We are happy to discuss any aspects of this submission further if helpful.

Factors most important when it comes to considering changes to indirect collection of personal information

Problem definition

Any proposal of legislative change should always include careful consideration of the problem such change is trying to address. In this instance, we query whether there is in fact a material gap in the current notification regime that warrants legislative change.

Under the Privacy Act's IPP 2, agencies must generally collect information directly from an individual unless an exception applies. In practice, these exceptions are only invoked on a limited basis and where applicable; it may not be appropriate to notify the individual in each instance for legitimate reasons. For example, if the information is already publicly available then a disclosure is not necessary (and could just result in notification fatigue) and if the information was collected for law enforcement purposes, then a disclosure to the individual concerned could interfere with legal proceedings. In any event, under IPP3, an agency is required to tell an individual when it intends to share their information with any third parties – so an individual should be informed from the outset about where their information is, or may be, held. Accordingly, banks, as agencies under the Privacy Act, already have lengthy IPP3 privacy collection notices given their complex business models.

Further, we consider that the status quo is broadly in alignment with overseas regulatory frameworks. Broadly, both the GDPR and the Australian Privacy Act have materially similar outcomes to that of the New Zealand Privacy Act, with the end result being that all individuals are currently entitled to notification of where their personal information is being collected, used and disclosed, unless an exception applies.

Impact of the possible changes

The impact of any proposed changes will need careful consideration. These proposed changes will impact both consumers/individuals and businesses/agencies who collect information from, or share information with, a third-party source. For consumers/individuals, these changes could result in an overload of information, undue anxiety, and confusion. This would likely lead to increased complaints and disputes and an overall worse customer experience.

For businesses/agencies, there may be a number of issues arising depending on the framework. These could include:

- In the banking context, customers are already provided with lengthy privacy collection notices setting out how information collected directly may be used or shared. To overlay a separate obligation may generate overly complicated disclosures.
- Interference with reasonable and required embedded business processes may arise as a result of this change, such as credit checks, identity verification checks or mortgage broker arrangements.
- There may be adverse consequences in some instances e.g. where notification discloses debt collection activity or law enforcement activity that may jeopardise collection or the integrity of the personal information collected.
- Notification may often be impractical as the collector will not necessarily have a relationship with the individual concerned. Legislation should not force more personal information to be collected (address, contact details etc.) in order to comply with legislative requirements.
- There is likely to be an increased compliance burden with no clear corresponding benefit. We believe existing processes are transparent and more than sufficient to ensure that individuals understand how banks are handling and protecting their information. Any further disclosures made to individuals on top of those existing processes, in each and every instance that information is shared, may just result in compliance burden and notification fatigue (as already identified in the Engagement Document). It is important that banks strike the right balance between being transparent and clearly explaining to individuals what information they hold about them, without overloading them with information and draining organisational resource unnecessarily.
- There are likely to be increased compliance costs in keeping disclosures current and up-to date (these would need constant updating for each new agency or supplier). It will be difficult to deal with the frequency of the changing status of vendors/third parties.

Form the proposed changes should take

If the Ministry decides these changes are necessary, any amendments to the existing IPPs, or creation of a new IPP, should be narrowed so that they address only the particular concern at issue.

There should also be carve outs/exceptions for instances where notification would be unnecessary (e.g. where the information is already publicly available or where the individual

has already authorised the collection of such information) or where notification would be inappropriate (e.g. where the information is being collected for law enforcement purposes or where disclosure would undermine the purpose for which the information was being collected). We note that in Australia, there are exceptions available under APP5 for third party collection of information in certain instances.

We also note that some global firms comply with the GDPR requirements by placing the notification onus on the third party providing the information to the firm (in contract). For example, if Party A has a direct relationship with an individual and provides information to Party B, the parties have an agreement that Party A will notify the individual rather than Party B. This may be a way to avoid some of the issues we refer to above.