Submission by

BusinessNZ

GROWING PROSPERITY AND POTENTIAL

to the

Justice Select Committee

on the

Privacy Bill

24 May 2018

PO Box 1925
Wellington
Ph: 04 496 6553

PRIVACY BILL - SUBMISSION BY BUSINESSNZ[1]

1. Introduction

1.1 BusinessNZ welcomes the opportunity to make a submission to the Select Committee on the Privacy Bill (the Bill). It does not wish to appear before the Committee to speak to the submission.

2. Overview

2.1 BusinessNZ recognises the need for revised privacy law and is not opposed to the Bill as such but considers aspects of the proposed legislation are at the same time both potentially confusing and unduly prescriptive.

2.2 In particular, the requirement to notify an individual or give public notice as well as to notify the Commissioner should there be a risk of harm (Cls 117, 118 and 119) leaves open the question of how the likelihood of risk is to be determined. Agencies do not necessarily want to acknowledge privacy breaches 'as soon as practicable' because they do not want to be unnecessarily alarmist.

2.3 But if an agency determines a particular privacy breach is notifiable, it will then need to follow the Bill's reasonably complex notification requirements. These are set out in cl 121 (a new provision) and while they might not be too onerous for a larger agency (though that too is questionable) could prove more than a little daunting for New Zealand's many SMEs.

2.4 As with notification, other provisions of the Bill similarly demonstrate an element of uncertainty. For example, the new compliance notice provisions (subpart 2 of Part 6) allow the Commissioner to issue a compliance notice if he or she considers there 'may have been' a breach of the Act. Before doing so the Commissioner may (but doesn't have to) assess whether any person has suffered harm. It would seem more logical to require evidence of harm rather than allow a compliance notice to be issued on the basis of a possibility.

2.5 Then there is the matter of disclosure of personal information to someone overseas. How readily will a New Zealand agency be able to determine the overseas jurisdiction requires that person to protect the information in a way that provides safeguards comparable to those in the Bill (or Act, as it would then be). Uncertainty of that kind could cause considerable difficulty for agencies not fully aware of where their data might be stored (which could be something of a moveable feast).

2.6 There must also be concern about the increased powers the Bill bestows on the Privacy Commissioner. If these are to be retained, some form of oversight or control will be essential.

[1] Background information on BusinessNZ is attached as Appendix One.

3. Recommendations

- Clause 19 - Clarify the basis for determining whether an overseas country has privacy safeguards comparable to those of New Zealand
- Clause 27 - Provide examples of when privacy information may be retained for longer than the purposes for which it can be lawfully used
- Clause 51 - Give examples of when an information privacy request might raise issues of such complexity a response cannot be provided within the original time limit
- Clause 63(2)(b) - Delete this clause and provide for internal employees to have the same protection that applies to others providing evaluative material
- Clause 96 - Remove the Commissioner's right to make an access direction where, following an investigation, a complaint is unresolved
- Clause 103 - Retain the current section 83 grounds on which an aggrieved individual can commence Tribunal proceedings and delete this clause's additional grounds
- Clarify the distinction between a complainant and an aggrieved individual
- Clause 105 - Provide for agencies to present evidence that an apology has been given as part of their defence to a privacy complaint rather than merely admissible for assessing remedies
- Clause 109 – Retain an aggrieved individual's right to appeal the outcome of an access investigation directly to the Tribunal
- Clauses 110 – 114 – Delete this new appeals process
- Clause 117 – Delete the words 'risk of harm from the definition of 'notifiable privacy breach'
- Clause 118 – Insert *'having tried and failed to remedy a privacy breach'* after 'as soon as practicable' and remove 'after becoming aware'.
- Clause 122 – Make that an attempt to remedy a privacy breach has been tried and has failed a 'reasonable excuse' for non-notification when a breach occurs
- Clause 123 – Provide for the Commissioner to publish an agency's identity only in exceptional circumstances
- Clauses 124 – 126 Remove the Commissioner's right to issues a compliance notice without first receiving a complaint and clarify when a compliance notice can be issued
- Clause 127 – Reword *'as soon as practicable after a stated date'*
- Clause 130 – Extend the grounds for appeal against enforcement as for, example, that an agency has had insufficient time to comply with a compliance notice and ,make enforcement appeal decisions appealable to the High Court
- Clause 131 – Provide the Tribunal with the ability to cancel or modify a compliance notice because the breach was unintentional or without negligence

4. Discussion

4.1 Clause 19: Information privacy principles

Information privacy principle 11: Limits on disclosure of personal information

While there is a need to protect the privacy of personal information disclosed to persons overseas, there is likely, as noted above, to be difficulty in determining

whether or not a country has safeguards comparable to New Zealand's. For example, privacy protection in the USA differs from that in the EU and the Australia's current Privacy Act applies only to larger private sector entities. Would all or any of these be taken to protect local personal information as the Bill requires? Greater clarification is required.

4.2 Clause 27: Commissioner may authorise collection, use, storage, or disclosure of personal information otherwise in breach of IPP 2, 8, 10 0r 11

This clause re-enacts section 54 of the current Act but also authorises the Privacy Commissioner (the Commissioner) to allow personal information to be kept for a longer time than IPP 9 would otherwise permit (IPP 9 – *not longer than is required for the purposes for which the information may lawfully be used).* That begs the question why an agency might want to keep personal information for longer than the purposes for which it might lawfully be used and in the absence of reasonable examples, such as for archival purposes, could seem to be an unnecessary addition to the Commissioner's powers of authorisation. Examples should be provided.

4.3 Clause 51: Extension of time limits

Clause 51 essentially restates section 41 of the current Act but adds as a reason for seeking an extension of time that the '*processing of the request raises issues of such complexity that a response to the request cannot reasonably be given within the original time limit'.* Although agencies are likely to welcome a further reason for seeking an extension of time, it is unclear how *'processing of such complexity'* differs from the existing extension provisions - the need to consult before making a decision on a request and to search through large quantities of information. What 'complexity' might involve needs some clarification.

4.4 Clause 53: Evaluative material as reason for refusing request under IPP6(1)(b)

It is noted that anyone employed or engaged by an agency in the ordinary course of that person's employment or duties has now no reason to withhold requested evaluative or opinion material. This appears to mean an employee whose application for an internal appointment was unsuccessful would be entitled to see any personal information used in the selection process, something that would not be in the best interests of either the employee or the person or persons who provided the material in issue. Internal employees should have the same protection applying to others who provide information of this kind (clause 53(1)).

Clause 53(2)(b) should be deleted.

4.5 Clause 96: Procedure after completion of investigation relating to IPP 6

Whereas previously, the Commissioner was required to refer unresolved complaints to the Director of Human Rights Proceedings (the Director - and can still do so), he or she can now direct an agency to provide an individual with access to his or her personal information. However, as under clause 110 access decisions can be appealed to the Human Rights Review Tribunal (the Tribunal) there seems little advantage in further complicating matters by introducing a two-stage process.

4.6 Clause 103: Aggrieved individual may commence proceedings in Tribunal

This clause considerably expands the current section 83 grounds on which an aggrieved individual, dissatisfied with the result of a Commissioner/Director investigation, can make application to the Tribunal. Whereas at present, applications can be made only if the Director or Commissioner is satisfied a complaint does not have substance or the matter ought not to be proceeded with, the Director agrees to the individual taking proceedings or declines to take proceedings, though otherwise entitled to, the new clause adds numerous further grounds: the Commissioner decides not to investigate the complaint or matter or does not determine them, or determines a complaint has substance or a matter should be proceeded with but does not refer them to the Director, or does not make a direction requiring an agency to provide access to the individual's personal information, or makes such a direction but the aggrieved individual is not satisfied with it, or determines a complaint has substance but the respondent fails to comply with an assurance of no repetition, or determines on an appropriate agency charge which the agency does not accept. (This latter is referred to as an interference with an individual's privacy by breaching IPP6.)

These additional grounds are likely to encourage unnecessary extensions of privacy wrangling particularly as all are essentially covered under the simple ground *'if the Director agrees to the aggrieved individual commencing proceedings'* (clause 103(1)(i)). Spelling them out as the Bill does, merely limits the Director's ability to exercise what may be needed discretion.

There is also the potential for confusion over who is covered by the word 'complainant' and who by 'aggrieved individual'. Both terms are used in clause 86(1) where an aggrieved individual is someone other than the complainant. Clause 103, however, refers only to an 'aggrieved individual' although obviously, here, the term covers a complainant as well. (Similarly clause 77, *Who may make a complaint.)* Some clarification would seem necessary.

4.7 Clause 105: Apology not admissible except for assessment of remedies

The reasoning behind this new clause is difficult to follow. If an apology is admissible for the purpose of assessing remedies (where it could be the only remedy required), might not its admissibility at an earlier stage of proceedings simply help to achieve an earlier outcome? An agency should be entitled to present evidence that an apology has been given as part of its defence.

4.8 Clause 109: Enforcement of direction made by Commissioner under section 96(5)(a) after investigation of IPP 6 breach.

Where an agency fails to comply with or appeal an access direction (after the Commissioner has completed an access investigation), this new provision provides an aggrieved individual with the right to apply to the Tribunal for an access order, adding yet a further complication to the access issue. As noted under clause 96, the current situation where non-compliance with the outcome of an access investigation is taken directly to the Tribunal, is preferable and should be retained. This is particularly so as an agency that unwittingly omits to appeal an access decision can face a maximum $10,000 fine.

4.9 Appeals against direction made after investigation of IPP 6 breach

Clauses 110 to 114 are also new and set out an appeal process to be followed if an agency wants to appeal a direction from the Commissioner regarding personal information access. If the Commissioner is to have the right to make access directions, providing agencies with an appeal process is not unwelcome. But as noted, it helps to further complicate the decision-making process. So, too, does the fact that the Tribunal's chairperson will be able to make an interim order suspending a personal information access direction (clause 112), an order which in turn can be varied or rescinded by the High Court on appeal. Rescinding an interim order would leave in place the Commissioner's original direction even though this might ultimately be reversed, unduly complicating an already complicated process.

Subclauses (2)(3) and (4) of clause 112 should be deleted.

4.10 Notifiable privacy breaches

Clauses 117, 118 and 119 are all essentially new provisions requiring privacy breaches to be notified to any individual (or individuals) affected by a breach not only, as previously noted, where the breach has caused harm but also where *'there is a risk it will do so'* (clause 117 'notifiable privacy breach' definition).

Clause 118, also as previously noted, requires notification *'as soon as practicable'* but being in a position to notify (which might be seen as the stage at which notification is practicable) is rather different from determining the stage at which notification will do the least harm to all parties. Given a media tendency to run with scare stories, it would be better to require notification only after an agency has tried and failed to correct an actual privacy breach.

The reference to *'or risk it will do so'* should be deleted from clause 117 as should the words *'after becoming aware'* from clause 118. In clause 118 *'having tried and failed to correct a privacy breach'* should be inserted after *as soon as practicable'.*

Re clauses 118 and 119, it should be noted that these require notification – to the Commissioner and affected individuals (including public notice) – if *'a notifiable privacy breach has occurred'.* As a *'risk'* (clause 117, notifiable breach definition) is not something that has occurred, clauses 118 and 119 are somewhat contradictory.

4.11 Clause 122: Offence to fail to notify Commissioner

As noted above, *'as soon as practicable'* is not a realistic test. Notification should not be required until measures to remedy a breach have been tried and have failed and the attempt to remedy should be a *'reasonable excuse'* for not notifying a breach when it is occurs (or when there is an apparent risk). And a penalty should not apply. (And certainly not the rather larger penalty the current Privacy Commissioner appears to have in mind.)

4.12 Clause 123: Publication of agencies in certain circumstances

As there are generally at least two sides to any allegation, the Commissioner should be able to publish an agency's identity only in exceptional circumstances.

4.13 Compliance notices

Clauses 124 to 126 are new provisions allowing the Commissioner to issue compliance notices if he or she considers an IPP has been breached or there has been interference with an individual's privacy under some other Act. Allowing the Commissioner to issue a notice without first receiving a complaint greatly enlarges the Commissioner's powers and opens the whole privacy issue up to fishing expeditions. The Commissioner should be entitled to issue a compliance notice only on receipt of a complaint as under clause 77.

As an example of a compliance notice issued concurrently *'with the use of any other means for dealing with the breach'* (clause 124(3)) the Bill indicates it can be issued while dealing with the same breach under Part 5 (clause 77) but the process under that Part of the Bill (relating to an interference with privacy complaint) does not appear to lead to the issuing of a compliance notice. The stage at which a notice can be issued is therefore unclear; it should be stated that this can happen only once an investigation has been carried out.

4.14 Clause 127: Agency response to compliance notice

Section 127 requires steps to comply to be taken *'as soon as practicable'* but also provides for compliance by a stated date. *'As soon as practicable'* may not be the same as the stated date. It would be better to provide for compliance *'as soon as practicable after a stated date'.*

4.15: Clause 130: Enforcement of compliance notice

Failure to comply with a compliance notice can result in the Commissioner taking enforcement proceedings in the Tribunal. Under clause 131 agencies have the right to appeal a compliance notice or any variation the Commissioner might decide on (and in the latter case, clause 128, which provides for variation, requires them to be informed of that right). But once enforcement proceedings are in train agencies can object only on the ground they believe the notice has been fully complied with – which could, at times, be a matter of opinion. Other grounds for appeal against enforcement, as, for example, that the agency has had insufficient time to comply with the notice, should be available. And enforcement appeal decisions should themselves be appealable to the High Court.

4.16 Clause 131: Appeal against compliance notice or Commissioner's decision under section128

Agencies can appeal to the Tribunal against compliance notices but must do so within 15 working days from the day on which the notice was issued or notice of the decision under clause 128 is given to the agency. As in the case of enforcement, the grounds for appeal are limited – the notice or decision was not in accordance with the law, an exercise of discretion was involved and should have been exercised differently, or the agency has fully complied. The Tribunal cannot cancel or modify a compliance notice because the breach was unintentional or without negligence but arguably should be able to cancel on those grounds if the breach is currently being dealt with. Given compliance notices can lead on to enforcement proceedings, in the case of unintentional or non-negligent breaches, agencies should be able to deal with them free from any third party intervention.

4.17 Clause 132 Interim order suspending compliance notice pending appeal

The same difficulties apparent in respect to directions given after a breach has been investigated are also raised by this clause.

4.18 Comment

As it stands, the Bill provides for appeals on a number of grounds – in respect to complaint investigations, access directions, interim orders, variation and cancellation decisions and enforcement decisions. In some cases the appeal grounds are limited but it would nevertheless make the proposed legislation more navigable if all appeal provisions were placed together with any variations in process/grounds for appeal stated under each appeal heading. Having the various appeal procedures spread throughout the Bill, as currently, inevitably results in confusion.

Background information on BusinessNZ

BusinessNZ is New Zealand's largest business advocacy body, representing:

- Regional business groups EMA, Business Central, Canterbury Employers' Chamber of Commerce, and Employers Otago Southland
- Major Companies Group of New Zealand's largest businesses
- Gold Group of medium sized businesses
- Affiliated Industries Group of national industry associations
- ExportNZ representing New Zealand exporting enterprises
- ManufacturingNZ representing New Zealand manufacturing enterprises
- Sustainable Business Council of enterprises leading sustainable business practice
- BusinessNZ Energy Council of enterprises leading sustainable energy production and use
- Buy NZ Made representing producers, retailers and consumers of New Zealand-made goods

BusinessNZ is able to tap into the views of over 76,000 employers and businesses, ranging from the smallest to the largest and reflecting the make-up of the New Zealand economy.

In addition to advocacy and services for enterprise, BusinessNZ contributes to Government, tripartite working parties and international bodies including the International Labour Organisation (ILO), the International Organisation of Employers (IOE) and the Business and Industry Advisory Council (BIAC) to the Organisation for Economic Cooperation and Development (OECD).