IAG submission

to the

Privacy Bill Select Committee

on the

Privacy Bill

24 May 2018

1. INTRODUCTION

1.1 This submission is a response by IAG New Zealand Ltd (IAG) to the Justice Select Committee (the Committee) on the Privacy Bill (the Bill).

1.2 We are supportive of the broad purpose and intent of the changes proposed by the Bill and limit our specific comments to clarifying when breaches are to be reported and strengthening due process in publishing the names of organisations.

1.3 IAG is New Zealand's leading general insurer. We insure more than 1.5 million New Zealanders and protect over $650 billion of commercial and domestic assets across New Zealand.

1.4 IAG's contacts for matters relating to this submission are:

James Fong, Privacy Officer

T: 09 969 6197

E: james.fong@iag.co.nz

Bryce Davies, General Manager Corporate Relations

T: 09 969 6901

E: bryce.davies@iag.co.nz

2. GENERAL COMMENTS

2.1 IAG supports the proposed legislative changes contained in the Bill and welcomes the intent to modernise New Zealand's 25-year-old Privacy laws and strengthen privacy protections. We believe the proposed modernisation and broader alignment with international privacy developments align with our company purpose; to make your world a safer place.

Further modernisation of the Bill to be considered

2.1 The Bill in its current form is predominantly based on recommendations made to the Government by the Privacy Commissioner in 2011. Accordingly, the Bill in its essence is at best fit for purpose for the world as we knew it in 2013.

2.2 The world we operate in and the way New Zealand shares and utilises personal information has moved on considerably since 2011. One need only consider the way and the rate at which New Zealand has adopted cloud computing in the years since 2011 to illustrate this.

2.3 It is inevitable then, that for New Zealand's Privacy laws to remain relevant both now and in years to come, the Act will need further and regular amendment to reflect current information practices as well as being future proofed to the greatest extent that is practicable.

2.4 We recommend that the Bill be amended to include a provision that requires periodic review of the Privacy Act.

2.5 On the point of modernisation it is noted that the Privacy Commissioner's February 2017 recommendations to the Minister of Justice go beyond the current provisions of the Bill. We support the Insurance Council of New Zealand's (ICNZ) submission where if the Bill is to change based on the submission from the Privacy Commissioner, a proper consultation process needs to be followed and for there to be ample opportunity to provide further feedback to the Committee.

Considerations outside of the specific Bill provisions

Ensuring appropriate resourcing for the Office of the Privacy Commissioner

2.6 To ensure that individuals have appropriate access to justice, and that the Office of the Privacy Commissioner (the OPC) can successfully carry out its functions, it will be important that the OPC receives resourcing sufficient to fulfil its expanded obligations and powers.

2.7 The introduction of mandatory breach reporting in Australia is illustrative. The Office of the Australian Information Commissioner received 63 reports in the first six

weeks of the regime, compared to 114 voluntary reports for the entire year prior to its introduction.

2.8 The broad and subjective Mandatory Data Breach Notification provisions in the Bill (see further comments below) may well encourage an organisation to err on the side of reporting and, as such, brings the issue of OPC resourcing into sharper focus.

3. SPECIFIC COMMENTS

Mandatory Breach Notification provisions

Definition of harms that would require breach notification

3.1 Section 75(2)(b) of the Bill prescribes the harms that have occurred or *may* occur for a privacy breach to be notifiable, being:

- loss, detriment, damage, or injury to the individual; or
- adverse effects to the rights, benefits, privileges, obligations, or interests of the individual; or
- significant humiliation, significant loss of dignity, or significant injury to the feelings of the individual.

3.2 We believe that in its current form this provision is too broad and subjective for agencies to understand when to notify and that, out of an abundance of caution, it will lead to over reporting. This goes against the Privacy Commissioner's stated desire to avoid over-reporting and creates unintended consequences, including:

- increased compliance costs for agencies;
- increased strain on the resources of the OPC;
- misalignment with the general principles-based approach of the Bill; and
- misalignment with the desire to place the responsibility in the hands of the agency to make proactive and informed analysis (and where required, notification) of privacy breaches.

3.3 A possible approach to eliminate subjectivity in the Mandatory Breach Notification provisions is to consider a reasonableness standard not currently reflected in the Bill. This could follow the example set in Australia where an "eligible data breach" must be reported when a reasonable person concludes that the unauthorised action is likely to result in serious harm to the individual. The term "Serious harm" is not defined in Australian legislation and the assessment required therefore becomes objective based on reasonableness from an agency's perspective.

3.4 We recommend that section 117(1) of the Bill be amended to update the definition of *notifiable privacy breach* to include a reasonable person test.

Notification process

3.5 Section 118 to 121 of the Bill detail the requirements for notification. The notification process in its drafted form is complex and potentially confusing for agencies. The ICNZ has provided a submission on these provisions. We support and adopt the ICNZ's submission on the notification process.

Publishing the identity of agencies in certain circumstances

3.6 Section 123 of the Bill allows the Commissioner to publish the identity of an agency that has reported a notifiable privacy breach if the Commissioner is satisfied that it is in the public interest to do so.

3.7 We believe that the concept of 'the public interest' is extremely broad and does not fit or align with the heading description of "certain circumstances". The 'public interest' could, for example, encompass 'punitive action', 'creating a deterrent effect' and 'educational purposes' (refer Section 14(1)(c) and (d)).

3.8 The grounds for publication should be precisely articulated, or in the alternative the same factors as in Section 125 related to compliance notices could be utilised.

3.9 As a general concept, regulators should not exercise a punitive power, without first hearing the views of the party affected. Accordingly, an agency, having notified a breach should have the right to be heard before the Commissioner decides whether to publish the agency's identity. Further, given the irreversible detriments to an agency from publication, an agency should have the ability to challenge a decision to publish to the Human Rights Tribunal. Such an approach would align with the purpose of modernising the Act where publication in a modern digital environment would further magnify any adverse or negative impacts of publication.

3.10 **We recommend that section 123 is removed and folded into the current sections 124 to 132 related to Compliance Notices**. This would create consistency of process and would see that *publication* is subject to appropriate provisions including:

- Factors the Commissioner must consider before publishing (section 125);
- A right to request cancelation of the decision to publish (section 127);
- A right of appeal to the Human Rights Tribunal against a decision to publish (section 131); and
- Interim suspension of a decision to publish (section 132).