ICNZ Insurance Council of New Zealand

Insurance Council of New Zealand
P.O. Box 474 Wellington 6140
Level 2, 139 The Terrace
Tel 64 4 472 5230
email icnz@icnz.org.nz
Fax 64 4 473 3011
www.icnz.org.nz

24 May 2018

Committee Secretariat
Justice Committee
Parliament Buildings
Wellington

Dear Committee Members,

ICNZ submission on the Privacy Bill

Thank you for the opportunity to submit on the Privacy Bill ('**the Bill'**). ICNZ represents general insurers that insure about 95 percent of the New Zealand general insurance market, including over half a trillion dollars' worth of New Zealand property and liabilities.

We wish to appear before the Committee to speak to our submission.

Please contact Jane Brown (jane@icnz.org.nz or 04 495 8008) if you have any questions on our submission or require further information.

Please note that with their permission, this submission echoes parts of the submission by the Financial Services Federation, whose view on certain sections of the Bill we support.

Individual members may take differing views to ICNZ on some issues and may submit to you separately.

Submission

Overall, ICNZ supports the legislative change proposed in the Bill. We are however aware that the Privacy Commissioner has called for legislation to go beyond what is currently included in the Bill. If the Bill is to change materially based on submissions from the Privacy Commissioner or other parties, we believe that a proper consultation process needs to be followed and for there to be ample opportunity to provide further feedback to the Committee.

Notifiable privacy breaches

A privacy breach is notifiable if it has caused any of the harm listed in section 75(2)(b). We consider the harms listed in section 75(2)(b) to be very broad and subjective (noting that if the harm is anticipatory and "may" be caused it will also be covered). It is difficult to conceive of a potential issue that would fall outside of this section. The uncertainty created by section 75(2)(b) may mean agencies feel compelled to notify *any* personal information-related issue with the potential to affect an individual. Notification might then occur where adverse effects are unclear or unknown to the agency and real harm does not actually exist. That is likely to result in increased compliance costs for agencies,

as well as resourcing issues for the Office of the Privacy Commissioner (**OPC**). ICNZ notes that when comparative laws were introduced in Australia, the Office of the Australian Information Commissioner (**OAIC**) received 63 notifications in the first six weeks of the Australian Notifiable Data Breaches Scheme's implementation. The OPC can expect similar demands on its resources, with those resources best used to address genuine misconduct and/or harm to individuals.

In addition to the impact on agencies and the OPC, the unnecessary or excessive notification of minor issues creates the risk of the following negative impacts on individuals:

- causing undue concern if individuals believe they are the victim of a serious hack or breach but in fact the likely impact on them is minimal to non-existent; and
- creating a "boy who cried wolf" scenario, where individuals eventually stop paying attention if they receive frequent notification of low-risk and/or low-impact "privacy breaches".

ICNZ draws the Committee's attention to the approach adopted to harm in the Notifiable Data Breaches Scheme in Australia. Notification is required where there is an "eligible data breach", which is a data breach likely to result in serious harm to any of the affected individuals. "Serious harm" is not defined in Australian privacy law and therefore requires an objective assessment from the viewpoint of a reasonable person in the entity's position.[1] Guidance from the OAIC notes "*not all data breaches are eligible. For example, if an entity acts quickly to remediate a data breach, and as a result of this action the data breach is not likely to result in serious harm, there is no requirement to notify any individuals or the Commissioner*."

In summary, the broad definition of harm in section 75(2)(b) lacks sufficient clarity to be useful and practical for agencies, creating uncertainty, risk and additional costs for both agencies and the OPC, as well as the potential for negative impacts on individuals and the public at large. We question whether this is the intention and whether it could lead to over-reporting of potential breaches. An alternative might be to have an objective test for harm and for reporting to be required where there has been actual harm (and not just anticipated harm). Further, to assist in dealing with the amount of subjectivity in the phrases "significant humiliation" and "significant injury" to the feelings of the individual in section 75(2)(b)(iii), it would be useful to include definitions in the Bill. Having these terms defined would increase the objectivity of the test and therefore be easier to apply.

Reporting of privacy breach data

ICNZ strongly supports the availability of aggregated and anonymised data on breaches of privacy reported to the Privacy Commissioner. Provision of such data plays a general but important role in meeting transparency about breaches, understanding about the scale of any problems and information to inform if any additional interventions are required.

In addition, the insurance sector has a specific need for such data. The increasing pace of digitalisation brings with it increased accumulation of cyber risks. Almost all risks to individuals and society are capable of being managed through the transfer of some or all risks to insurers. Cyber insurance is therefore available globally to enable such risks to be transferred.

The availability of cyber insurance and the pricing of such cover is severely hamstrung by limitations on the access to data about the severity and frequency of these risks. Data on severity and frequency of risk is fundamental to the provision of any insurance cover because this is the raw material to enable informed underwriting and pricing of cover.

[1] https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches

For many lines of insurance, such as motor vehicle accidents, house fires, floods and earthquakes, there is a lot of historical data available. This enables these risks to be underwritten and priced efficiently. However, on best estimates, less than 10% of businesses in New Zealand have cyber insurance and a negligible number of consumers have such cover. This means that little data is available to individual insurers and consequently greater uncertainty exists which will be reflected in the pricing of cover. This in turn may contribute to lower levels of risk transfer.

Greater uptake of cyber insurance has additional advantages for society beyond the ability to transfer risk. Engagement with insurers inevitably involves insurers wanting to understand the risks that prospective insureds present. This prompts the insured, often a SME in New Zealand with limited in-house technical expertise, to take steps to reduce their vulnerability.

So, the provision of data on the frequency and severity of breaches will help develop better risk transfer options, reduce the retention of risk to businesses (largely small and medium enterprises) and lead to engagement with insurers to lower levels of overall vulnerability.

Finally, it is noteworthy that the OECD's Directorate for Financial and Enterprise Affairs Insurance and Private Pension Committee recommended on 23 May 2018:

> *Governments should facilitate information sharing on cyber threats and incidents by sharing the threat information available to them and encouraging greater disclosure and/or information sharing on incidents by affected businesses (including by addressing any legal impediments to information sharing). The needs of the risk management and insurance sectors should be taken into account when defining the information that needs to be submitted for regulatory notification.*

The notification process

A further concern for some of ICNZ's members is the dual notification regime set out in the Bill, namely the requirement to notify both the Commissioner (section 118) and the affected individual(s) (section 119). That approach could be onerous and impractical for certain agencies. ICNZ would instead support a two-step mandatory data breach process. There are two options for a two-step process, the first option being notification initially to the Commissioner only. If the Commissioner was then of the view that there was a real risk of harm to affected individuals, either the OPC or the agency would notify those individuals.

This approach aligns with the position previously proposed by the OPC. In ICNZ's view, a two-step notification process would ensure only breaches likely to have a real impact would be brought to the attention of individuals. This would still provide the OPC with visibility of the full range of breaches but would minimise the risks to individuals identified in the section above.

The second option, particularly if the threshold for harm is not raised as submitted in the section on notifiable breaches above, would be for notification to only be to the affected individual or individuals, who could then decide for themselves whether to also notify the OPC. This approach would both prevent the OPC being flooded with low level notifications, and the risk of delayed notification to the individual that all notifications first being required to be notified to the OPC could cause.

ICNZ's believes that either of these alternatives to the proposed dual notification regime have merit in terms of timeliness and resource efficiency, and the Committee should reconsider how the notification process would best be carried out. Further, this consideration should include whether, as in the Australian regime, the Bill should also include an ability not to notify the OPC or the individual where effective remedial action has been taken.

Informants in insurance

We consider there should be a specific provision that allows an agency to refuse a request under IPP 6(1)(b) where the personal information has been obtained from an informant reporting suspected fraudulent activity by an insured in relation to an insurance claim.

Under the Bill an insured is entitled to access his or her personal information held by an agency and this includes any information an informant provides to the insurer. This means the identity of the informant may be disclosed directly or indirectly to the insured. We note the Privacy Commissioner's Case Notes numbers 17375[2] and 207459[3] where insurers have been able to rely on section 27(1)(c) and/or section 29(1)(a) of the Privacy Act 1993 to withhold such personal information. These subsections have been re-enacted in sections 57(a) and (b) of the Bill.

We submit that it would be practical and beneficial to have a specific ground on which to refuse a request under IPP 6(1)(b) on the basis that the personal information was received from an informant regarding suspected fraudulent activity in an insurance claim. This would provide more clarity than having to address this matter within the limitations of sections 57(a) and (b). More importantly, this would provide certainty to informants that their identity will be protected and will be more likely to encourage the reporting of such information to insurers. This would in turn potentially reduce incidences of fraud which is in the public interest, particularly when such fraudulent activity could harm other persons and property, for example, where a fire is deliberately lit for the purposes of making an insurance claim or illegal activity such as illicit drug manufacture is being carried out at a property.

We suggest that a specific ground of refusal could be incorporated into sections 52(1)(a), 53(2)(a) or 57 of the Bill.

Fraudulent activity

Fraudulent activity is an ongoing issue for ICNZ members. Examples of fraud within the general insurance sector include purposefully causing damage in order to make an insurance claim for financial gain and claiming for items with a higher value than the actual item lost or damaged. ICNZ estimates that insurance fraud costs the sector about $350 million per annum. This cost is ultimately passed on via premiums charged to those consumers who do not commit fraud. To manage the risks and costs associated with fraud, ICNZ members would like to be able to share information about people committing, or attempting to commit, fraud amongst the ICNZ membership base to minimise the risk of further fraud.

As it currently stands, the sharing of personal information relating to fraudulent activity is likely to constitute a breach of both the Privacy Act 1993 and the Bill. Information Privacy Principle 11 ("IPP 11") of the Bill sets out certain limited circumstances in which the disclosure of personal information is permitted. Those circumstances do not include the ability to disclose personal information for the purposes of preventing fraud or for any other reasons that might be in the public interest.

In ICNZ's view, the Bill presents an opportunity to re-visit and expand the exceptions to the general rule prohibiting disclosure of personal information. Fraud is a persistent problem with wide ranging

[2] https://www.privacy.org.nz/news-and-publications/case-notes-and-court-decisions/case-note-17375-1997-nzprivcmr-6-couple-complain-insurance-company-refused-to-disclose-informant-s-identity/
[3] https://www.privacy.org.nz/news-and-publications/case-notes-and-court-decisions/case-note-207459-2009-nzprivcmr-17-woman-s-request-for-information-from-insurance-company-refused/

impacts across society. The ability to tackle that problem through acceptable information sharing practices would therefore be strongly welcomed by ICNZ members and many other agencies.

Further, ICNZ considers that the prevention and/or reduction of fraud is a genuine public policy justification for the sharing of information about those attempting to commit fraud. ICNZ is already committed to the detection and prevention of fraud through its Insurance Claims Register[4] (**ICR**), where information is only collected and shared with the consent of the customer. Expanding the ability to share information in certain circumstances as proposed below would be another step in the right direction towards a reduction in the incidents of fraud.

ICNZ recommends that IPP 11 of the Bill be amended from its current form so that disclosure of personal information is permitted in circumstances where there is a public interest in allowing the disclosure, including where fraud has occurred or is suspected on reasonable grounds. We recommend that the following new subsection (1)(j) be inserted into IPP 11:

> ***Limits on disclosure of personal information***
>
> *(1) An agency that holds personal information must not disclose the information to any other agency or to any person unless the agency believes, on reasonable grounds,—*
>
> *……*
>
> *(j) that there is a public interest reason for disclosing the information to another agency, including where disclosure is necessary for the prevention of fraud, or reducing the potential risk of fraud occurring where fraud is suspected on reasonable grounds.*

For the purposes of subsection (j) we propose the following definition of "fraud"[5] be included in subsection (6):

> *(6) In this principle,—*
>
> *fraud means any act, expression, omission, or concealment calculated to deceive another to his or her disadvantage…..*

Fines

While ICNZ does not specifically take a view as to what the appropriate level for penalties under the Bill should be, we believe it is important to note that there is also significant reputational harm in non-compliance with privacy law, particularly if that non-compliance results in harm to consumers through a privacy breach. Reputation harm is also a powerful incentive for compliance with the legislation.

Commissioner's ability to make binding decisions on access requests

ICNZ supports the Privacy Commissioner being able to make binding decisions on access requests. There are currently very long waiting periods at the Human Rights Review Tribunal. Allowing the Commissioner to make binding decisions on access requests will improve the efficiency of complaints and will go some way towards easing the workflow for the Tribunal.

---

[4] https://www.icnz.org.nz/industry-leadership/fraud/

[5] Merriam Webster Legal Dictionary, s.v. "fraud," accessed May 18, 2018 https://www.merriam-webster.com/dictionary/fraud#legalDictionary.

Cross-border data flow protections

ICNZ supports the requirement for New Zealand agencies to take reasonable steps to ensure that personal information disclosed overseas will be subject to acceptable privacy standards, as long as this requirement is workable and does not constrain good business practices. For example, storage of data in the cloud is now commonplace and there will likely be future developments, not only in border-less storage options, but in other areas. There is a need to ensure that the Bill is future-proofed and does not prevent any technological advances in the safe storage, sharing and access of data.

Protection, etc, of individual as reason for refusing request under IPP 6(1)(b) (sections 52(1)(a)(i) and (ii))

ICNZ supports the inclusion of sections 52(1)(a)(i) and (ii). Given the importance of these provisions in protecting individuals from harm:

- we submit that the words "the disclosure of information *would*" should be amended to "the disclosure of information *may*"; and
- we question what the intended difference is between the thresholds of "be likely to" and "a significant likelihood of".

Evaluative material as reason for refusing request under IPP 6(1)(b) (section 53(2))

ICNZ submits that section 53(2) should also include material for insurers prepared as part of the process in deciding whether to accept or decline a claim. Examples of this type of material include:

- an assessment by a claims handler to their manager
- an investigation report that include a third-party interview
- internal emails between staff on the progress of a claim
- internal process forms for appointment of assessors, investigators and suppliers.

In order to achieve this, we recommend that making decisions about claims is added to the definition of **evaluative material** as follows:

> *(iii) for the purpose of deciding whether to insure any individual or property or to continue or renew the insurance of any individual or property or to accept or decline any claim made on insurance; but…*

Agency may impose conditions instead of refusing access to information (section 58)

ICNZ considers that for this section to be effective it should be clarified that it is a breach of the legislation (and therefore an offence) if the recipient uses or discloses the information in breach of the conditions imposed by the agency.

We also submit that section 58 should specify that it is at the discretion of the agency to grant any conditional access to the information, that is, it is not mandatory to do so.

Publication of identity of agencies in certain circumstances (section 123)

Section 123(1)(a) currently says that the Commissioner may publish the identity of an agency that has notified the Commissioner of a notifiable privacy breach if the Commissioner is satisfied that it is in the public interest to do so. ICNZ is concerned that the concept of "*public interest*" is incredibly broad and does not fit within the section heading of publication in "*certain circumstances*". We believe it would be more appropriate to either precisely articulate the grounds for publication, or

alternately for similar criteria to those in section 125(1) to be used when deciding whether or not to identify an agency. ICNZ believes that the law should recognise that publication of the identity of an offending agency is inherently damaging to the commercial goodwill and reputation of the agency, and this type of publication is inherently and irreversibly punitive.

As a general concept, regulators should not exercise a punitive power without first hearing the views of the affected party. Accordingly, an agency, having notified a breach, should have the right to be heard before the Commissioner decides whether or not to publish the agency's identity. Further, an agency should have the ability to challenge a decision to publish before the Human Rights Review Tribunal.

ICNZ submits that it would be most appropriate for section 123 to be removed and incorporated into the current sections 124 to 132 relating to compliance notices. This would include factors the Commissioner must consider before publishing the identity of an agency (section 125), a right for an agency to request cancellation of the decision to publish (section 127), a right for the agency to appeal to the Tribunal against a decision to publish (section 131), and interim suspension of a decision to publish the identity of an agency (section 132).

Conclusion

Thank you again for the opportunity to submit on the Bill. If you have any questions, please contact our Legal Counsel on 04 495 8008 or by emailing jane@icnz.org.nz.

Yours sincerely,

Jane Brown
Legal Counsel