FinancialServicesCouncil.
growing and protecting the wealth of New Zealanders

Financial Services Council
of New Zealand
Level 33, ANZ Centre,
23-29 Albert St, Auckland 1010
P: +64 9 985 5762
E: fsc@fsc.org.nz
www.fsc.org.nz

25 May 2018
To the Justice Committee

Submission: Privacy Bill

This submission is from the Financial Services Council of New Zealand Incorporated (**FSC**).

We wish to appear before the committee to speak to our submission, being represented by:

- Richard Klipin, FSC Chief Executive Officer
- and colleagues, based on availability

The FSC represents New Zealand's financial services industry having 33 members at 30 April 2018. Companies represented in the FSC include the major insurers in life, disability, income, and trauma insurance, and some fund managers and KiwiSaver providers plus law firms, audit firms, and other providers to the financial services sector.

Our submission has been developed through consultation, and represents the views of our members and our industry. We acknowledge the time and input of all our members in contributing to this submission.

The FSC's guiding vision is to be the voice of New Zealand's financial services industry and we strongly support initiatives that are designed to deliver:

1. Strong and sustainable consumer outcomes;
2. Sustainability of the financial services sector; and
3. Increasing professionalism and trust of the industry.

The key purpose of the Privacy Bill is to promote people's confidence that their personal information is secure and will be treated properly. We support changes that are intended to achieve this purpose, in particular, increasing the accountability and transparency of agencies who deal with personal information.

We understand that the aim of the Privacy Bill is to remain technology neutral, and that the changes in the Privacy Bill are based on the Law Commission's 2011 review of the Act. Due to ever changing technologies regarding the way agencies collect, use, and store personal information, and the development of international standards, it is important the Bill is reviewed to ensure that legislation is sufficiently modernised and is fit for purpose for 2019 and beyond.

We have five recommendations that we believe will strengthen the final form of the Bill and we expand on these recommendations below.

We note that the Privacy Commissioner will be recommending further changes to the Bill. When we verbally present to the Select Committee we would like to respond to his written submission, once we have had a chance to consider it.

I can be contacted on 021 0233 5414 or richard.klipin@fsc.org.nz to discuss any element of our submission.

Yours sincerely

Richard Klipin
Chief Executive Officer, Financial Services Council

Recommendations

1. Mandatory Reporting – guidance on 'harm', consistency with the Australian regime

We support the mandatory reporting requirement that notifiable privacy breaches that pose a risk of harm to people must be notified to the Privacy Commissioner and to affected individuals.

We believe that aspects of mandatory reporting of privacy breaches could benefit from alignment with the Australian regime.

For example, the threshold for reporting privacy breaches provided in the Bill is too low and unclear, and may lead to a significant compliance burden for organisations. We believe that the threshold should at least correspond with the Australian regime, where the test includes a 'serious harm' element. There may also be tests applied in other jurisdictions that could be considered in this regard.

In addition, as with the Australian regime, we believe that there should be:

a) No mandatory reporting for privacy breaches that result in non-serious harm. If the organisation is comfortable that the access or disclosure would not be likely to result in serious harm to any of those individuals then no reporting should need to be undertaken.
b) Reporting of privacy breaches should take into account the mitigating factor of acting to prevent serious harm.

If alignment to the Australian regime is not desired, then we submit that further guidance on what 'harm' means would be practical for agencies, to avoid uncertainty about what should be reported, or over reporting of privacy breaches to the Privacy Commissioner.

2. Personal Information – consistency with the Australian regime

We note that the broad definition of 'personal information' is retained in the Bill. We suggest that now is the time to consider amending it to be consistent with the Australian approach, which generally requires the individual to be a subject matter of the information before it is 'personal information' and covered by the legislation. Much information (including information relating to property) is arguably currently caught by the Act and should not necessarily be caught.

3. Modernising the Privacy Principles

We note the existing 12 Privacy Principles have been carried through into the Privacy Bill, without modification. This is positive because the Principles are currently well-understood by individuals and agencies.

However, the Privacy Principles need to be extended and modernised to account for changing technology, specifically:

a) Consent/authorisation should be defined so that agencies know what is required in this regard. Does it require positive acknowledgement from the individual or is implicit consent acceptable? Ideally, we recommend the latter.
b) The Principles should not require the contact details of the agency collecting and holding personal information to be provided to an individual before personal information is collected, where it is clear in the circumstances who the agency is. This information should be publicly available anyway if it is clear who the agency collecting and holding the information is. This requirement is often honoured in the breach by agencies currently.

4. Retaining current timeframes

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, the 20 working day period applies under clause 92(2)(b).

We believe that organisations should have a timeframe of no less than 20 working days within which to provide the information required under clause 92(2)(a). However, it may not be operationally feasible at all times for organisations to provide this information in this or shorter timeframes. We recommend a mechanism be put in place to enable an ability to extend the 20 working day deadline provided certain criteria are met, for example a demonstrable challenge in retrieving all of the information from archive services.

5. Specific examples in relation to financial services

In our submission to the Financial Advice Code Working Group on the Code of Professional Conduct for Financial Advice Services, we highlighted the importance of consumer access to their own data, and two potential areas that may need exploring further in the review of the Privacy Bill:

a) Access to advice, and in particular, cost-effective advice, will mean increasing use of systems to deliver good advice experiences. Machine learning and artificial intelligence are likely to be used extensively in automated advice, and they require access to a large body of data. This should be permitted where no identification of individuals is possible.

b) In many other online services, consumers may opt out of specific privacy provisions in order to receive a free or discounted service. For example, consumers may allow insurers access to wearable health device data to receive discounts and benefits. Permitting a limited opt-out may therefore allow greater access to such benefits where consumers would otherwise be unable to afford them.