FINANCIAL SERVICES FEDERATION

PRIVACY BILL 2018 (GOVERNMENT BILL 34-1)

1. Introduction

1.1 The Financial Services Federation Incorporated ("FSF") welcomes the opportunity to comment on the Privacy Bill (the "Bill").

1.2 This submission comments on the proposed ramifications of:

1.2.1 new mandatory data breach reporting obligations;

1.2.2 the inability to share information about fraudulent activity; and

1.2.3 the disclosure of personal information overseas, particularly in relation to storage in the "cloud".

1.3 We understand the policy intent behind the Bill is to promote people's confidence that their personal information is secure and will be treated properly. The FSF agrees with and is supportive of that rationale. The focus of these submissions is ensuring that any unintended consequences of legislative change are identified and addressed. We also wish to ensure new legislation is easy for our members to understand and follow.

2. Financial Services Federation Incorporated – Background Information

2.1 The FSF is a non-profit organisation which represents a number of New Zealand's responsible, non-bank financial institutions. FSF's work includes setting industry standards for responsible lending, compliance, consumer awareness, and consulting with Government with a view to achieving fair and balanced legislation.

2.2 FSF is selective with its membership to ensure its reputational integrity. FSF's members include well established finance, leasing, and credit-related insurance companies, credit reporting agencies, and affiliate members that provide professional services to the industry. A list of the FSF's members is attached as Appendix A.

3. Mandatory data breach reporting

3.1 As a general principle, the FSF supports the mandatory reporting of privacy breaches as set out in the Bill. FSF also supports the Bill's requirement for notice to be given to both the Privacy Commissioner ("Commissioner") and affected individuals (or that public notice be given as the case may be).

3.2 FSF notes that it is an offence to fail to notify the Commissioner of a notifiable privacy breach, with agencies liable on conviction to a fine of up to $10,000[1].

Harm threshold

3.3 In its current form, the Bill requires notification to both the Commissioner and an affected individual "as soon as practicable after becoming aware that a notifiable privacy breach has occurred". A "privacy breach" refers to various types of unauthorised access or disclosure, or an action preventing an agency from accessing the relevant information. A privacy breach becomes "notifiable" if it has caused any of the types of harm listed in clause 75(2)(b) to an affected individual or individuals, or there is a risk it will do so[2].

3.4 Clause 75(2)(b) details the nature of this harm. It provides that an action of an agency is an interference with the privacy of an individual if the action:

3.4.1 has caused, or may cause, loss, detriment, damage, or injury to the individual; or

3.4.2 has adversely affected, or may adversely affect, the rights, benefits, privileges, obligations, or interests of the individual; or

3.4.3 has resulted in, or may result in, significant humiliation, significant loss of dignity, or significant injury to the feelings of the individual.

3.5 The FSF acknowledges the need for drafting to have sufficient scope to encompass a range of activities and results. However, in its current form the Bill defines the harm necessary to trigger notification of a privacy breach in an overly broad way. FSF's concern, and one which is shared by its members, is that the Bill is unclear as to the relevant threshold for reporting breaches to the Commissioner and to individuals in accordance with clauses 118 and 119 of the Bill.

3.6 The FSF notes in particular clause 75(2)(b)(ii), which includes any action that has "adversely affected, or may adversely affect, the rights, benefits, privileges, obligations, or interests of the individual". This wording is so broad that it will be difficult for agencies to understand exactly what adverse effects will require notification under that sub-clause. By way of illustration from an FSF perspective, if a mobile credit manager temporarily misplaces a single credit application form containing the personal information of a potential client, would that constitute a "notifiable privacy breach" on the grounds that the loss of the form could adversely affect the applicant's ability to obtain credit, even though there is no risk of, for example, identify fraud? The FSF's reading of clause 75(2)(b)(ii) is that this scenario is likely to constitute a notifiable privacy breach, which in the FSF's view is excessive.

[1] Privacy Bill 2018 (34-1), cl 122

[2] Privacy Bill 2018 (34-1), cl 117

3.7 The uncertainty created by clause 75(2)(b)(ii) means agencies may feel compelled to "cast the net wide" and 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"). The FSF 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. The OPC can expect similar demands on its resources, with those resources best used to address genuine misconduct and/or harm to individuals.

3.8 The FSF has significant concerns that the OPC and the Human Rights Tribunal ("HRT") will have the resources to handle the workload arising out of what is likely to be a significant increase in both notifications and resulting prosecutions and suggests that this is an issue that needs careful consideration as to the resources required particularly to ensure that the time to judgment of a prosecution is not unreasonable.

3.9 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:

3.9.1 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

3.9.2 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".

3.10 The FSF 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.[3] Guidance from the Office of the Australian Information Commissioner 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."

3.11 The FSF makes one final point in relation to the definition of a "privacy breach" and that is that clarification is required in s117(a)(ii) that this should be limited to a "malicious action" that prevents the agency from accessing the information on either a temporary or permanent basis. This is to ensure that actions such as the agency's system being

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

hacked by an outside party is captured as a privacy breach but situations where the agency's system is unavailable due to schedule outages for maintenance or upgrade are not.

3.12 In summary, the broad definition of harm in clause 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.

Two-step notification process

3.13 A further concern is the dual notification regime set out in the Bill, namely the requirement to notify both the Commissioner and the affected individual(s). That approach is likely to be onerous and impractical for agencies. The FSF supports a two-step mandatory data breach process, with 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.

3.14 The FSF notes that approach aligns with the position previously proposed by the OPC. In the FSF'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 identified in paragraph 3.9 above.

Recommendations

3.15 We recommend the Committee:

3.15.1 provides greater clarity as to the meaning of "harm" and/or an applicable threshold for the degree of harm necessary for notification, by the inclusion of:

(a) a formal and more expansive definition of "harm"; or

(b) a reference to "serious harm" as seen in the equivalent Australian legislation to introduce some form of objective threshold.

3.15.2 Considers the action required in s117(a)(ii) be limited to "malicious action"

3.15.3 introduces a two-step notification process where agencies are required to notify the Commissioner in the first instance under clause 118, with notification to affected individuals pursuant to clause 119 of the Bill then being conditional on the Commissioner's decision as to whether or not they should be notified. We have provided draft wording below (proposed changes to the draft Bill are in red):

118 Agency to notify Commissioner of notifiable privacy breach

An agency must notify the Commissioner as soon as practicable after becoming aware that a notifiable privacy breach has occurred. Within a reasonable time of such notification, the Commissioner will determine whether there is sufficient risk of harm to the affected individual(s) to require notification pursuant to section 119.

119 Agency to notify affected individual or give public notice of notifiable privacy breach

(1) If the Commissioner determines that an affected individual should be notified of a privacy breach, then the agency must notify an affected individual as soon as practicable after ~~becoming aware that a notifiable privacy breach has occurred~~ receipt of confirmation from the Commissioner of the agency's obligation to so notify, unless subsection (2) or an exception in section 120 applies.

(2) If, after the Commissioner deems notification to the affected individual must be made, it is not reasonably practicable to notify an affected individual or each member of a group of affected individuals, the agency must instead give public notice of the privacy breach.

(3) Public notice must be given—

(a) in a form in which no affected individual is identified; and

(b) in accordance with any regulations made under section 213.

(4) If subsection (2) or an exception in section 120 is relied on, the agency must notify the affected individual or individuals at a later time if—

(a) circumstances change so that subsection (2) or the exception no longer applies; and

(b) at that later time, there is or remains a risk that the privacy breach will cause any of the types of harm listed in section 75(2)(b) to the affected individual or individuals.

(5) A failure to notify an affected individual under this section may be an interference with privacy under this Act (see section 75(2)(a)(iv)).

4. Fraudulent activity

4.1 Fraudulent activity is an ongoing and growing issue for FSF members. In the lending industry, it is not uncommon for customers to provide fraudulent information in their loan applications or to use fraudulent identification to obtain finance in a name other than their own. It is also not uncommon for them to approach several different lenders (who are often members of FSF) to obtain multiple loans and financial products. The fraudulent information provided can include the following types of personal information:

4.1.1 incorrect names, residential addresses and dates of birth;

4.1.2 incorrect employment details; and

4.1.3 details of other loans.

4.2 A number of FSF's members also provide credit related insurance services. It is not uncommon for information provided by applicants for those services to be misleading and/or potentially fraudulent or for information provided when making a claim to be fraudulent in order to inflate the claim amount. There are also certain auto repairers that consistently provide quotes at above-market rates for the repair of vehicles on the basis that the work is an "insurance job".

4.3 There are many other ways in which fraudulent activity takes place in the financial services industry (including a higher than average incidence of internal fraud because of the nature of the business). The above issues raised in 4.1 and 4.2 are some examples of the way in which FSF member businesses are affected by fraud.

4.4 The incidence of fraud-related activity and loss to FSF member businesses and others in the financial services industry, are increasing. On 21 May 2018 Stuff Business Day reported that ASB bank is seeing an "unprecedented rise in credit card fraud". The article also reported that the Banking Ombudsman has become so concerned about the rising tide of complaints that she has got credit card companies and banks together to discuss what can be done to better protect the public. The article further reported that the Australian Payments Fraud Report shows that fraud has risen from 55cents per $1000 spent in 2014 to over 65cents in just 2 years to 2016.

4.5 The FSF believes that the ability for financial services providers to share information about fraudulent activity will both provide further protection to the public against fraud and also reduce the cost to industry that occurs from fraud which is a cost of business passed on to consumers who do not behave fraudulently.

4.6 Because of this lack of sharing of information, it is difficult to determine in real dollar terms the actual cost of fraud to the financial services industry. FSF members report that on average .023% of their total loan book at any one time is fraudulent (i.e. the

loan has been set up to commit fraud and no repayments are likely to result so the money is effectively lost. This might seem an insignificant amount until it is considered across a loan book valued at 10's or 100's of millions of dollars. This also relates to the fraud the credit provider is able to detect or which has actually been able to happen – it does not take into account the fraud that is thwarted at loan origination and which does not take place with one lender but might be able to with another one if there is no ability to share the information about the type of fraud being attempted. The cost of fraud is ultimately passed on via the interest rate charged to those consumers who do not commit fraud as part of the cost to FSF members and other lenders of providing access to credit. To manage the risk and costs associated with fraud, FSF members would like to be able to share information about people committing, or attempting to commit, fraud amongst the FSF membership base to minimise the risk of further fraud.

4.7 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 (Limits on disclosure of personal information) ("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.

4.8 The FSF points out that a precedent exists for the allowance of sharing of personal information relating to fraudulent activity Under Rule 11 of the Credit Reporting Privacy Code *Limits on Disclosure of Credit Information* which allows under 11(2)(C)(ii)that a Credit Reporter that holds credit information may disclose the information, if the Credit Reporter believes on reasonable grounds that disclosure is necessary:

"to enable an insurer to investigate a case of suspected insurance fraud".

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

4.10 Further, the FSF considers that the prevention and/or reduction of fraud is a genuine public policy justification for the sharing of information about those attempting to or actually committing fraud.

Recommendation

4.11 The FSF 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 have provided draft proposed changes to the Bill below, including a proposed definition for "fraud"(in red)[4]:

Information privacy principle 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,—

(a) that the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or

(b) that the disclosure is to the individual concerned; or

(c) that the disclosure is authorised by the individual concerned; or

(d) that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to disclose the information; or

(e) that the disclosure of the information is necessary—

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) or the enforcement of a law that imposes a pecuniary penalty; or

(iii) for the protection of public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(f) that the disclosure of the information is necessary to prevent or lessen a serious threat to—

[4] Merriam Webster Legal Dictionary, s.v. "fraud," accessed May 9, 2018 https://www.merriam-webster.com/dictionary/fraud#legalDictionary

(i) public health or public safety; or

(ii) the life or health of the individual concerned or another individual; or

(g) that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions; or

(h) that the information—

(i) is to be used in a form in which the individual concerned is not identified; or

(ii) is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(i) that the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern; or

(j) there is a genuine public interest reason for disclosing the information to another agency, including where disclosure is reasonably necessary for the prevention of fraud, or reducing the potential risk of fraud occurring where fraud is suspected on reasonable grounds.

(2) Without limiting the generality of subclause (1)(e)(i), an example of disclosure under that subclause is reporting to the New Zealand Police a reasonably held belief that an offence has been, or may be, committed.

(3) An agency (A) may not disclose personal information to an overseas person (B) in reliance on subclause (1)(a), (c), (e), (f), (h), or (i) unless—

(a) section 8 applies to A and B; or

(b) the individual concerned authorises the disclosure of the information to B; or

(c) B is in a prescribed country or State; or

(d) A believes on reasonable grounds that B is required to protect the information in a way that, overall, provides comparable safeguards to those in this Act.

(4) However, subclause (3) does not apply if the personal information is to be disclosed to an overseas person in reliance on subclause (1)(e) or (f) and it

is not reasonably practicable in the circumstances for A to comply with the requirements of subclause (3).

(5) Without limiting the generality of subclause (3)(d), an example of A having the necessary belief on reasonable grounds is A having entered into an agreement with B that provides comparable safeguards to those in this Act.

(6) In this principle,—

fraud means any act, expression, omission, or concealment calculated to deceive another to his or her disadvantage

overseas person means a person outside New Zealand who is not subject to this Act

prescribed country or State means a country or State that is specified in regulations as having privacy laws comparable to those of New Zealand.

5. Disclosure of personal information overseas, particularly in relation to storage of data in the "cloud"

5.1 The Bill amends IPP 11 in relation to the disclosure of personal information to "an overseas person". An "overseas person" is defined as "a person outside New Zealand who is not subject to this Act". In the absence of a definition of "person" in the Bill, we assume this is a reference to a "legal person" and includes business and other organisations with legal capacity. We suggest this is clarified in the Bill to aid interpretation and understanding, particularly by non-lawyers.

5.2 Clause 3 of IPP 11 (Part 3, Subpart 1) prohibits New Zealand agencies from disclosing personal information to an overseas person unless the following exceptions apply:

5.2.1 Clause 8 applies to A and B, namely the overseas person ("B") holds the personal information on behalf of the agency ("A");

5.2.2 the individual concerned authorises the disclosure of his or her information to B;

5.2.3 B is in a country that is prescribed in the regulations as having privacy laws comparable to those in New Zealand (a "prescribed country or State"); or

5.2.4 A believes on reasonable grounds that B is required to protect the information in a way that, overall, provides comparable safeguards to those in the Bill.

5.3 The FSF has concerns about the impact of these new obligations on its members. The obligations are likely to introduce additional complexity for agencies, particularly in relation to the growing use of cloud storage platforms. Many agencies, including FSF

members, store data (including personal information) in offshore data centres ("the cloud") because of numerous latency, cost and efficiency benefits. However, the new requirements are likely to compromise many of those benefits.

5.4 The exception in sub-clause 3(b) of the Bill in relation to personal information being "held" by a cloud service provider ("CSP") pursuant to clause 8 provides some assistance. However, many CSPs do more than simply holding personal information "for the purpose of safe custody" (clause 8(1)(b) or for the "purpose of processing the information on behalf of Agency A" (clause 8(1)(c). Indeed many cloud service agreements purport to give additional rights and access to CSPs that could well remove the opportunity for organisations to rely on that exception. The FSF is concerned that not only will its members have to determine whether their existing cloud service agreements enable them to rely on this exception (which is likely to require legal advice and associated costs), but where they do determine a CSP is doing more than "holding" the personal information, they will have to enter difficult negotiations with the CSP to restrict its access to the data in order to rely on the exception. That is likely to be difficult given that many CSPs are large US technology companies with considerably stronger bargaining power than FSF members.

5.5 It will also generally be extremely onerous for FSF members and other agencies to obtain authorisation from individuals for storage of their personal information in "the cloud" pursuant to sub-clause 3(b) of the Bill. That is particularly so for data that was collected prior to the enactment of the Bill, as such authorisation is unlikely to have been obtained previously.

5.6 This provision also raises questions as to the nature of the "authorisation" required, which we note is referred to as "consent" in the Explanatory Note to the Bill, introducing some confusion between the two terms. What does "authorisation" mean in this context? Does it equate to notions of consent under the General Data Protection Regulation (where consent must be a freely given, specific, informed and unambiguous indication of agreement)? Or will it suffice to obtain this "authorisation" via a website privacy policy? This lack of clarity creates uncertainty and therefore increased risk and cost for agencies.

5.7 Sub-clause 3(c) allows overseas disclosure if the overseas person is in a prescribed country or State. The FSF is not aware of any regulations currently in force that specify a country or State as having comparable privacy laws to New Zealand, so for the time being this is of little assistance. Even when enacted, such regulations are only likely to apply to a limited range of countries.

5.8 Sub-clause 3(d) allows overseas disclosure if there are reasonable grounds to believe that the overseas person is required to protect the information in a way that, overall, provides comparable safeguards to those in the Bill. Sub-clause 5 clarifies that this will include by contract. Where authorisation is not practical (and unclear as to what that

involves) and no prescribed countries or States have yet been confirmed, this will be the only available option to agencies.

5.9 For FSF members, and many other agencies, reliance on this exception to the general non-disclosure rule will require extensive contractual re-negotiation. Moreover, data stored in offshore clouds typically involves contracts with very large US technology companies likely to have considerably greater bargaining power. The cost in terms of time, effort and money to try and re-negotiate cloud storage contracts to meet New Zealand privacy law standards could be significant.

5.10 The FSF acknowledges that many of its members are already ensuring safeguards are built into contracts to protect the personal information that will be stored in cloud environments to a comparable standard to New Zealand privacy law. We note, however, that what is "comparable" is currently unclear, creating further uncertainty.

Recommendation

5.11 FSF submits to the Committee that the Bill be amended to:

5.11.1 clarify the meaning of "authorisation", including that such authorisation may be obtained via a statement in an agency's privacy policy; and

5.11.2 clarify the key aspects of the Bill that will be the benchmark against which "comparable safeguards" will be measured for inclusion in contracts pursuant to sub-clause 3(d).

Once again the FSF is grateful for the opportunity to make this submission and would be pleased to appear before the Select Committee to answer any questions.

Lyn McMorran
EXECUTIVE DIRECTOR

Appendix A
FSF Membership List as at 1 April 2018

<u>Rated</u> Asset Finance (B) <u>Non-Rated</u> Mutual Credit Finance Gold Band Finance ➢ Loan Co	BMW Financial Services ➢ Mini ➢ Alphera Financial Services Branded Financial Services Community Financial Services European Financial Services Go Car Finance Ltd Honda Financial Services Mercedes-Benz Financial Motor Trade Finance Nissan Financial Services NZ Ltd ➢ Mitsubishi Motors Financial Services ➢ Skyline Car Finance Onyx Finance Limited Toyota Finance NZ Yamaha Motor Finance <u>Leasing Providers</u> Custom Fleet Fleet Partners NZ Ltd ORIX NZ SG Fleet Lease Plan	L & F Ltd ➢ Speirs Finance ➢ YooGo Avanti Finance Caterpillar Financial Services NZ Ltd CentraCorp Finance 2000 Finance Now ➢ The Warehouse Financial Services Flexi Cards Future Finance Geneva Finance Home Direct Instant Finance ➢ Fair City ➢ My Finance John Deere Financial Latitude Financial Pioneer Finance ➢ Personal Finance South Pacific Loans Thorn Group Financial Services Ltd Turners Automotive Group	Equifax (prev Veda) Centrix <u>Debt Collection Agencies</u> Baycorp (NZ) Dun & Bradstreet (NZ) Limited	Autosure Protecta Insurance Provident Insurance Corporation Ltd Southsure Assurance	American Express International (NZ) Ltd AML Solutions Buddle Findlay Chapman Tripp EY Finzsoft KPMG Paul Davies Law Ltd PWC Simpson Western FinTech NZ HPD Software Ltd Total : 56 members