23 May 2018

Justice Committee
Parliament Buildings
Wellington

**SUBMISSION on**
**Privacy Bill**

## 1. Introduction

Thank you for the opportunity to make a submission on the Privacy Bill. This submission is from Consumer NZ, New Zealand's leading consumer organisation. It has an acknowledged and respected reputation for independence and fairness as a provider of impartial and comprehensive consumer information and advice.

Contact: Aneleise Gawn
Consumer NZ
Private Bag 6996
Wellington 6141
Phone: 04 384 7963
Email: aneleise@consumer.org.nz

## 2. Select Committee

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

## 3. Comments on the Bill

Consumer NZ supports the introduction of the Privacy Bill (the bill). In our view, law reform in this area is long overdue so we welcome the changes being proposed.

However, we consider there are gaps in the bill which need to be addressed. Our reasons are set out below.

### *3.1 Alignment with General Data Protection Regulation (GDPR)*

Although the bill will bring our legislation more into line with many of our trading partners, we don't think it goes far enough.

In our view, the bill needs to be better aligned with the General Data Protection Regulation for the following reasons:

(a) The protections provided by the GDPR are more extensive than those in the bill. In our view, New Zealanders should be entitled to the same protections afforded to consumers in the EU.

(b) New Zealand will have to match the protections delivered under the GDPR in order to retain EU adequacy or be deemed by the EU to have "an adequate level of protection".

(c) The scope of the GDPR means many New Zealand businesses will have to comply with its "gold standards". These businesses will need to ensure their practices comply with the GDPR and the bill. This is likely to create confusion and operational duplication.

Examples of how the bill could be better aligned with the GDPR are discussed below.

### *3.2 Consent*

Under articles 6 and 7 of the GDPR, collecting and using personal data is generally prohibited unless the individual's consent has been obtained or it is permitted by law. The individual has the right to withdraw his or her consent at any time.

Also, if the individual gives written consent, the request for consent must be presented in a manner which is "clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language".

This differs greatly from the situation in New Zealand, where consent to the collection and use of personal information is often buried in the agency's terms and conditions and is not brought to the attention of the individual.

We recommend consent provisions similar to the GDPR be included in the bill. We also recommend agencies should be required to obtain "opt-in" consent before sending marketing emails or on-selling consumers' data, as is required under the GDPR.

### *3.3 Right to be forgotten*

Article 17 of the GDPR gives individuals the right to have their data deleted without undue delay in certain circumstances. This is known as the "right to be forgotten" or the "right of erasure".

We would like to see a similar right included in the bill.

This is particularly important in the digital world we live in where people are uploading photos and information without realising the impact this information might have on the individual in years to come.

Under the GDPR, consumers in the EU will, for example, be able to request social media sites delete any data they've collected about them. We think similar protections should apply in New Zealand.

### *3.4 Mandatory reporting of privacy breaches*

We welcome the introduction of mandatory reporting of privacy breaches under the bill. However, we are concerned the commissioner has no power to penalise agencies that report a privacy breach.

That is, as the bill is currently drafted, the Privacy Commissioner only has the power to penalise agencies that don't report breaches. In our view, this is problematic.

Agencies should not receive a "get out of jail free" card just because they report breaches.

We therefore agree with the Privacy Commissioner's recommendations that the commissioner should have the ability to apply to the High Court, in the case of serious

breaches, for a civil penalty of $100,000 for individuals and $1 million for bodies corporate. These fines would provide a much better deterrent and also provide a more comparable regime to that of the EU.

Under the GDPR, the most serious breaches can result in fines of up to E$20million or 4% of global annual turnover. For less serious breaches, fines are up to E$10 million or 2% of global annual turnover.

### *3.5 Timing of notification of privacy breaches*

Under clauses 118 and 119 of the bill, an agency must notify the commissioner and an affected individual "as soon as practicable after becoming aware that a notifiable privacy breach has occurred." Under article 33 of the GDPR, agencies are required to "without undue delay and, where feasible, not later than 72 hours after becoming aware of it, notify the personal data breach."

We suggest a similar timeframe be adopted in New Zealand to ensure agencies provide notification of the breach within a reasonable timeframe. If they don't meet the timeframe, they should have to justify why this hasn't occurred.

### *3.6 Data portability*

The right to data portability (article 20) is one of the fundamental data rights in the GDPR. This right essentially allows an individual to move their personal information from one agency to another.

In our view, the right to data portability is an important one for consumers as it gives consumers greater power over their own data. A consumer who cannot easily transfer their data from one provider to another may feel "locked in" to their existing provider, particularly if they would prefer to be using another provider.

We therefore suggest the right to data portability be included in the bill.

### *3.7 Controls on re-identification*

We are disappointed to see the bill does not include protections against the risk of re-identification. Overseas, individuals have been identified from anonymised datasets that have been publicly released for research purposes. For example, in August 2016, Australia's federal Department of Health published online medical billing records of about three million Australians. The records were de-identified but patients could be re-identified, through linking the records with known information about the individuals.

As a result of overseas breaches and developments in overseas privacy laws, the Privacy Commissioner recommended new provisions be included in the bill to ensure the "opportunities and benefits of greater data use can be optimised, without undue risk to individual privacy, and public trust and confidence."[1]

We agree such provisions should be included in the bill.

[1] Report to the Minister of Justice under section 26 of the Privacy Act, "Six recommendations for privacy reform", retrieved on 21 May 2018 from: https://www.privacy.org.nz/assets/Files/Reports-to-ParlGovt/OPC-report-to-the-Minister-of-Justice-under-Section-26-of-the-Privacy-Act.pdf

### *3.8 Penalties*

We welcome the introduction of the new offences under the bill for misleading an agency in a way that affects someone else's information and knowingly destroying documents containing personal information if the documents have been requested.

However, we are concerned penalties of $10,000 for offences under the bill (including for failure to report a breach) are too low and will be insufficient to deter bad behaviour. The penalties are low by international standards.

In our view, it's possible some businesses will choose to risk a $10,000 fine rather than complying with their obligations under the bill.

Thank you for the opportunity to make a submission on the bill. If you require any further information, please do not hesitate to contact me.

Yours sincerely

Sue Chetwin
Chief Executive