Institute of Directors
Mezzanine Floor, 50 Customhouse Quay
PO Box 25253, Wellington 6146, New Zealand
telephone: 04 499 0076 *email:* mail@iod.org.nz **iod.org.nz**

23 May 2018

Committee Secretariat
Justice Committee
Parliament Buildings
Wellington

Email: justice@parliament.govt.nz

Submission on the Privacy Bill

The Institute of Directors (IoD) appreciates the opportunity to comment on the Privacy Bill (the Bill) which will replace the Privacy Act 1993 (the Act). Privacy law reform in New Zealand is well overdue and we welcome the Bill.

A lot has changed since the Act came into effect 25 years ago. The growth of the internet and the digital economy, and the emergence of new technologies have changed the way organisations operate and how personal information is used. Globally, developed countries have been reforming their privacy regimes to ensure they are appropriate for the modern world. The importance of privacy and data protection has been highlighted in a number of recent, high profile, harmful breaches and incidents.

About the Institute of Directors

The IoD is a non-partisan voluntary membership organisation committed to driving excellence in governance. We represent a diverse membership of over 8,600 members drawn from NZX-listed issuers, large private companies, small to medium enterprises, state sector organisations, not-for-profits and charities.

Our chartered membership pathway aims to raise the bar for director professionalism in New Zealand, including through continuing professional development to support good corporate governance.

Summary

The IoD generally supports the Bill and its purpose to promote people's confidence that their personal information will be secure and used appropriately. It is essential that the Bill is fit for purpose, flexible for the future, comparable with the privacy regimes of our key trading partners, and meets international best practice standards. It is also important that any reforms in the Bill will help retain New Zealand's *adequacy* status under the European Union's General Data Protection Regulation.

The Bill provides the Privacy Commissioner (the Commissioner) with considerable discretion in carrying out statutory functions and we encourage the Committee to ensure there are sufficient accountability mechanisms in the Bill. We also encourage the Committee to consider whether the privacy regime (and especially the complaints process) will function efficiently and effectively in practice.

We request that the proposed commencement date of the Bill be extended by at least six months to give organisations sufficient time to prepare for the changes in the Bill. We also request that the Commissioner provide guidance on the reforms in the Bill.

The IoD generally supports introducing mandatory notification of privacy breaches for serious breaches in New Zealand. The threshold for notification should be set at an appropriate level and we believe a threshold similar to that in the Australian notifiable data breach scheme around *serious harm* is necessary in New Zealand to strike the right balance between protecting privacy without unduly impacting organisations and the Office of the Privacy Commissioner.

There are remedies in the Bill for interference with privacy and the Human Rights Review Tribunal has considerable powers to grant appropriate remedies including damages. We understand that the Privacy Commissioner is advocating for fines up to $1 million for organisations, and $100,000 for individuals, who seriously breach their privacy obligations. This would fundamentally change the privacy landscape in New Zealand and we would not support this level of fines.

Background

The Privacy Act 1993

The Act regulates how personal information should be collected, used, disclosed, and stored in New Zealand and is based around the following information privacy principles:

1. Purpose of collection of personal information
2. Source of personal information
3. Collection of information from subject
4. Manner of collection of personal information
5. Storage and security of personal information
6. Access to personal information
7. Correction of personal information
8. Accuracy etc of personal information to be checked before use
9. Agency not to keep personal information longer than necessary
10. Limits on use of personal information
11. Limits on disclosure of personal information
12. Unique identifiers.

Most organisations (referred to as *agencies*) are subject to the Act including companies and government departments.

The functions of the Privacy Commissioner are set out in the Act and include providing advice and education on privacy matters, investigating complaints and evaluating bills that may interfere with an individual's rights.

The complaints process under the Act is summarised below:

- the Commissioner can investigate and form an opinion that there has been a privacy breach

- if the complaint has substance, the Commissioner will attempt to settle the matter through mediation. Currently, the Commissioner does not have powers to make binding rulings on investigations or to provide remedies.
- where a complaint is not settled, the Commissioner can refer it to the Director of Human Rights Proceedings (which is an independent office in the Human Rights Commission)
- the Director of Human Rights Proceedings can then choose whether to bring the case before the Human Rights Review Tribunal (on behalf of a plaintiff). The Tribunal can award damages of up to $350,000
- if the Director doesn't take the case, an individual can still bring proceedings in the Tribunal
- there is also a general right of appeal from the Tribunal to the High Court.

The Privacy Bill

The Bill has been a long time in the making. In 2011, the Law Commission completed a review of the Act and made a number of recommended changes. Many of these have been included in the Bill together with recommendations from the Commissioner's Necessary and Desirable reports.

The core framework of the Act has been retained in the Bill, including the 12 information privacy principles (although some of these have been updated to ensure they are fit for purpose).

A number of key changes are proposed in the Bill including:

- *mandatory notification of privacy breaches*: agencies will be required to notify the Commissioner and affected individuals of harmful privacy breaches
- *compliance notices*: the Commissioner will be able to issue compliance notices to agencies to remedy a privacy breach. The Human Rights Review Tribunal will be able to enforce these notices and also hear appeals
- *binding decisions on access requests*: the Commissioner will be able to make binding decisions on complaints relating to an individual's access to information (or refer the complaint to the Human Rights Review Tribunal as is currently the case). The Commissioner's decision can be appealed to the Tribunal
- *information gathering powers*: the Commissioner's existing investigation power is strengthened by allowing him or her to reduce the timeframe in which an agency must comply, and the penalty for non-compliance has been increased (ie fines up to $10,000)
- *cross-border data flow protections*: agencies will be required to take reasonable steps to ensure that personal information disclosed overseas will be subject to acceptable privacy standards
- *criminal offences*: there are new offences for misleading an agency in a way that affects someone else's information and knowingly destroying documents containing personal information where a request has been made for it (with fines up to $10,000).

IoD comments on the Bill

The IoD generally supports the Bill and its purpose to promote people's confidence that their personal information will be secure and used appropriately. Trust and transparency

are critical in today's operating environment, and the 2018 Acumen Edelman Trust Barometer (NZ) provides a strong mandate for organisations (and particularly business) to protect privacy and personal information.

Information governance is an important responsibility of boards. This includes overseeing and monitoring risks (eg privacy, ethics and cybersecurity), ensuring effective compliance, and holding management to account for having appropriate practices and processes in place.

International developments

There is a global trend towards a unified standard of data protection and regulatory environments are evolving to meet the challenges of the modern digital world. In reforming New Zealand's privacy laws, it is essential that the Bill is fit for purpose, flexible for the future, comparable with the privacy regimes of our key trading partners, and meets international best practice standards.

The European Union's General Data Protection Regulation (GDPR) comes into force on 25 May 2018. This applies to all organisations processing the personal data of European Union citizens, regardless of where they are living. Many New Zealand organisations will need to ensure they are GDPR compliant. New Zealand has *adequacy* status under the GDPR. This means that personal information can be transferred freely between European Union countries and New Zealand on the basis that New Zealand has sufficient levels of personal data protection. The Committee should ensure that any reforms in the Bill will help retain New Zealand's adequacy status.

General comments

The Bill appears to strike the right balance between improving privacy standards in New Zealand without unduly burdening agencies, subject to our comments below. The Bill provides an opportunity for agencies to revisit their privacy practices and processes to ensure compliance and best practice.

The Commissioner's powers have been strengthened and this should help improve privacy standards and ensure compliance in New Zealand. The Bill provides the Commissioner with considerable discretion in carrying out statutory functions. With greater power, comes greater responsibility, and we encourage the Committee to ensure there are sufficient accountability mechanisms in the Bill.

We also encourage the Committee to consider whether the privacy regime (and especially the complaints process) will function efficiently and effectively in practice. We understand that there is a wait time of approximately two years for cases before the Human Rights Review Tribunal. The introduction of compliance notices under the Bill may exacerbate this issue. This is a significant concern from an access to justice perspective.

Agencies will need sufficient time to prepare for the changes in the Bill, which is currently proposed to come into force on 1 July 2019. Preparation will involve assessing and updating systems and agreements with third parties, and training staff to ensure effective compliance. This may be a complex exercise for larger agencies and a challenge for small and medium sized businesses and not-for-profit organisations. Given this, we request that the commencement date be extended by at least six months.

We also request that the Commissioner provide guidance on the reforms in the Bill.

Mandatory privacy breach notification

In 2017, the Office of the Privacy Commissioner received 132 data breach notifications, 79 related to public sector organisations and 53 related to private sector organisations. Breach notification is currently *voluntary* and the actual number of data breaches that occur in New Zealand is unknown.

The Bill introduces *mandatory* privacy breach notification, which was recommended by the Law Commission in 2011. Mandatory privacy breach notification (in different forms) is increasingly common globally. Australia, for instance, enacted a notifiable data breach scheme earlier this year.

How will the notification regime work?

Agencies will be required to notify the Commissioner and *affected individuals* of a *notifiable privacy breach* as soon as practicable after becoming aware of it:

- *affected individual*, under the Bill, means the individual to whom the information relates, whether they are inside or outside New Zealand
- *notifiable privacy breach* means a *privacy breach* (which is in turn defined to include unauthorised or accidental access to, or disclosure, alteration, loss or destruction of, personal information) that causes or poses a risk of harm to an individual
- *harm* includes situations where the action of an agency:
    - has caused or may cause loss, detriment, damage or injury to the individual
    - has adversely affected, or may adversely affect, the rights, benefits, privileges, obligations or interests of the individual or
    - has resulted in, or may result in significant humiliation, significant loss of dignity or significant injury to the feelings of the individual.

Agencies must notify the Commissioner and affected individuals in accordance with a specified form (which is different for the Commissioner and affected individuals). If it is not reasonably practicable to notify affected individuals, then the agency must give public notice of the breach in a specified form.

There are exceptions to the obligations to notify affected individuals and give public notice of a notifiable privacy breach including if the notification or notice would be likely to:

- prejudice the security or defence of New Zealand
- endanger the safety of a person or
- reveal a trade secret.

It is an offence for an agency, without reasonable excuse, to *not* notify the Commissioner (with fines up to $10,000). The Commissioner will also be able to publish the name of an agency that has disclosed a notifiable privacy breach with consent or where it is in the public interest.

IoD comments

The current voluntary privacy breach notification regime may act as a disincentive for agencies to notify individuals of a privacy breach, given the potential economic and reputational costs involved in disclosing a breach. However, some organisations will

voluntarily report breaches (irrespective of legal requirements) as it will be the right thing to do.

There are benefits of mandatory privacy breach notification. A key policy reason for mandatory notification is that it allows people whose information has been compromised to take steps to mitigate any adverse consequences such as identity fraud or financial loss. For example, it gives those people the chance to change their online passwords or cancel their credit cards. Another policy reason is that people should have a right to know that their information has or may be compromised. Mandatory notification may also encourage agencies to improve their privacy practices and processes, and bring New Zealand into line with best practice, international standards.

Mandatory notification will likely impose costs on agencies. However, the advantages should outweigh the disadvantages for serious privacy breaches. Accordingly, we generally support introducing mandatory notification of privacy breaches for serious breaches in New Zealand.

There are no proposed exemptions to the notification regime for agencies already subject to the Bill and this is appropriate in the context of New Zealand's privacy law landscape.

Our main concern is that the threshold for notification be set at an appropriate level. A low threshold may lead to large volumes of reporting which could:

- be excessive, significantly reducing the effectiveness of the regime (where individuals take reports less seriously)
- be overly burdensome on agencies seeking to ensure effective compliance (and disproportionate to the harm sought to be prevented/remedied)
- unintentionally dominate the time and resources of the Office of the Privacy Commissioner.

Australia's notifiable data breach scheme has a higher threshold than that proposed in the Bill. Organisations in Australia must notify the Information Commissioner of a breach:

- when a reasonable person would conclude that the access or disclosure of information would be likely to result in *serious harm* to any individuals to whom the information relates and
- the entity has not been able to prevent the risk of serious harm.

We believe a higher threshold similar to that in the Australian scheme is necessary in New Zealand to strike the right balance between protecting privacy without unduly impacting agencies and the Office of the Privacy Commissioner. This would also make it simpler for agencies operating in New Zealand and Australia to comply with both notification regimes.

Remedies

The Act provides remedies for interference with privacy, and the Human Rights Review Tribunal has considerable powers to grant appropriate remedies including damages up to $350,000. In recent years, the Tribunal has made significant awards in privacy cases.

Outside of what is proposed in the Bill, we understand that the Commissioner is advocating for fines of up to $1 million for organisations, and $100,000 for individuals, who seriously breach their obligations.

This would fundamentally change the privacy landscape in New Zealand and we would not support this level of fines. The 2014 Regulatory Impact Statement: Supplementary Government Response to the Law Commission's 2011 report states that New Zealand should not consider imposing fines for privacy breaches given the nature of our legal framework and notes the "need for and usefulness of fines could be considered, if need be, once the impacts of the privacy reforms have been determined. If it becomes clear that guidance and early intervention is not effective, the use of sanctions may be appropriate". We agree and note that it is essential for there to be extensive consultation on such matters. It is also important to bear in mind that the actual costs for agencies of privacy breaches can be considerable, including the costs involved in determining the cause of a breach, corrective and remedial costs, legal costs, and damage to an agency's reputation and brand.

We look forward to the proposed privacy law reforms coming into effect in New Zealand and appreciate the opportunity to comment on the Bill on behalf of our members.

Yours sincerely

Felicity Caird
General Manager, Governance Leadership Centre
Institute of Directors