KensingtonSwan

AKL. 18 Viaduct Harbour Ave
Private Bag 92101
Auckland 1142
New Zealand
DX CP22001
P +64 9 379 4196
F +64 9 309 4276

WLG. 89 The Terrace
PO Box 10246
Wellington 6143
New Zealand
DX SP26517
P +64 4 472 7877
F +64 4 472 2291

24 May 2018

Committee Secretariat
Justice Committee
Parliament Buildings
Wellington

By email: ju@parliament.govt.nz

Submission on the Privacy Bill

1 About Kensington Swan

1.1 This is a submission by Kensington Swan on the Privacy Bill. We would like the opportunity to appear before the Committee to speak to this submission.

1.2 Kensington Swan is one of New Zealand's premier law firms with a legal team comprising over 100 lawyers who act on technology, government, corporate, commercial, litigation, property, and financial markets projects from our offices in Wellington and Auckland.

1.3 We have extensive experience advising a range of agencies, in various industries, who collect, hold and process personal information. We act for consumer-facing organisations, government departments, software developers, users of cloud technology, and a wide variety of other agencies who use personal information in the course of their business.

1.4 We assist our clients with their regulatory compliance obligations, and initiatives aimed at pro-actively addressing risk to our clients and their customers and employees in respect of the treatment of personal information.

1.5 Our lawyers have also advised clients, in New Zealand and overseas, in relation to their compliance obligations under the European Union's General Data Protection Regulation ('GDPR').

1.6 This submission is made on behalf of the firm and not on behalf of any client of the firm.

2 General comments

2.1 We are generally supportive of the legislative changes proposed by the Privacy Bill.

2.2 We agree that the time is right for New Zealand to update and modernise its privacy laws. It is clear that in the 25 years since the introduction of the Privacy Act in 1993, technological change has had a significant impact on the manner in which personal information can be collected and exploited. While the 1993 Act has stood up well to the test of time, in our view it is imperative that New Zealand's privacy laws are subject to thorough scrutiny and revision to ensure that they are fit for purpose in the current climate, and in particular to take into account global trends in data protection and privacy.

2.3 We are particularly cognisant of the desirability of ensuring that New Zealand privacy law continues to be considered by the European Commission as ensuring an 'adequate level of

protection' for personal data, such that New Zealand can remain on the 'white list' of countries to which EU-based organisations may freely transfer personal data. New Zealand's status as a white list country affords New Zealand-based organisations – especially those who offer cloud-based services where personal data may be hosted or otherwise processed in New Zealand – a competitive advantage when compared to organisations based in non-white list countries (which includes both Australia and the United States).

2.4 The Committee will no doubt be aware that the introduction of the GDPR represents a game-changer insofar as the implications of a breach of privacy is concerned. It also reflects a European view that places the rights of individuals with respect to their personal information at least on a level footing with the organisations who seek to exploit that personal information, in order to re-balance (in part) the ability of those organisations to commercialise and profit from their ability to collect, aggregate and commercialise that information. It is our view that New Zealand will require robust privacy laws in respect of which the Privacy Commissioner has a real and effective ability to enforce, in order to keep New Zealand's economy in step with that of one of New Zealand's primary targets for a growth in trade, Europe; an economy that is seen as a world-leader with respect to the regulation and protection of personal information.

2.5 We also consider that the existence of robust privacy laws is of paramount importance in the context of the creation and success of the 'digital economy' that is favoured by the New Zealand government (which we fully support). In our view, for a digital economy to succeed it is imperative that the integrity of each citizen's digital footprint is preserved and that citizens can be sure that when interacting online – whether with a government agency or otherwise – the sanctity of their personal information is preserved.

3 Specific comments

Fines

3.1 We believe that it is important for New Zealand privacy law to have 'teeth'. We support the Privacy Commissioner's recommendation that the Privacy Commissioner be empowered to apply to the High Court for a civil penalty in the case of serious breaches of privacy law.

3.2 Our clients come to us for advice because they value the importance of privacy and of compliance with the principles embodied in New Zealand privacy law. They invest significant resources into their compliance programmes and adapt their business models, sometimes in a way that would commercially disadvantage them, in order to ensure that they comply with the law.

3.3 We consider that the Privacy Commissioner should be empowered to apply to the High Court to impose commercially significant fines for non-compliance with privacy law. In the absence of an adequate financial incentive for all agencies to comply, those agencies that do comply are then disproportionately burdened and otherwise punished for their compliance through the cost of compliance. In our view, the lack of 'teeth' in respect of fines for privacy law breaches would result in an uneven playing field, whereby those participants in the market who fail to comply are effectively granted a commercial advantage over those that do.

3.4 In light of the above and the maximum levels of fines that can be imposed under the privacy laws of our major trading partners, including under the Australian Privacy Act and the GDPR, we believe that the Privacy Commissioner's calls for maximum fines of $1,000,000 for a body corporate and $100,000 for an individual are reasonable.

Appeals to the Human Rights Review Tribunal

3.5 As the Committee will know, the Human Rights Review Tribunal ('**HRRT**') is currently tasked with delivering remedies and rulings in privacy complaints, and under the Privacy Bill it will retain this function.

3.6 It is well publicised that the HRRT is currently overworked and experiencing considerable delays. Claimants in the HRRT are currently waiting approximately two years for a hearing and up to three years for a decision and the HRRT is no longer setting down cases for hearing unless they are urgent. These delays in the HRRT mean that final remedies and decisions on privacy complaints are currently taking an unacceptable amount of time to be resolved and access to justice is being impacted.

3.7 We understand that there are some options being floated to increase the capacity of the HRRT and to deal with the considerable backlog. At this stage however, there is no fixed plan to solve the issues the HRRT is experiencing and there is no definitive date at which we can expect the HRRT to be running smoothly and without delays.

3.8 We are concerned that the Privacy Bill does nothing to alleviate the current delays which privacy complaints are experiencing in the HRRT. The Privacy Bill makes no substantive changes to the procedure by which the Director of Human Rights Proceedings, or an aggrieved individual takes their complaint to the HRRT. We urge the Committee to consider whether there is another body or tribunal which could hear privacy complaints in a more timely manner.

3.9 Further we are concerned that there are some aspects of the Privacy Bill that will increase the workload of the already overworked HRRT.

3.10 As the Committee knows, the Privacy Bill will allow the Commissioner to issue compliance notices to agencies. We support this change. We are however concerned that the HRRT will be tasked with enforcing compliance notices and hearing appeals. With the current delays in the HRRT the Commissioner will face undue delays (of potential several years) to enforce a compliance notice. Equally an agency which believes that an enforcement notice has been unfairly issued will face unacceptable delays to appeal the notice.

3.11 Other changes which will increase the workload of the HRRT include:

a Individuals will be able to apply to the HRRT for an access order requiring an agency to comply with a direction of the Commissioner under clause 96.

b The Commissioner's decisions on complaints about access to information will be able to be appealed to the HRRT.

3.12 We are concerned that the additional workload will cause further delays in the HRRT which means access to justice for privacy complaints is hindered. This situation also disincentivises

agencies from taking Privacy seriously, as any decision or enforcement by the HRRT may take several years.

3.13 We would support any proposal which will streamline the processes of the HRRT so that the hearing of privacy complaints can be dealt with efficiently. For example the following options might assist in alleviating the current delays:

a Allowing the Commissioner greater powers to make binding decisions.

b Appointing a deputy HRRT chairperson who deals specifically with Privacy Act cases.

c Finding a different forum for hearing privacy complaints and enforcing the Commissioner's decisions.

Notifiable privacy breaches

3.14 The Committee will be aware that Part 6 of the Privacy Bill establishes a mechanism whereby agencies are required to notify the Privacy Commissioner and, subject to certain exceptions, affected individuals, if a 'notifiable privacy breach' occurs.

3.15 The obligation to report a notifiable privacy breach is similar to the concept of a 'mandatory data breach notification' under the GDPR and also under Australian privacy law.

3.16 Subject to our comments below, we support the introduction of this concept in the Privacy Bill. Many of our clients already self-report on a voluntary basis in the context of their management of privacy and data breaches, and they find the cooperation afforded them by the Office of the Privacy Commissioner to be invaluable when dealing with what can be quite sensitive and stressful situations.

3.17 However, we are concerned that the definition of 'notifiable privacy breach' is unduly subjective such that it is likely to either lead to over-reporting, or lead to agencies being 'caught out' by particular circumstances that a reasonable person would not have anticipated.

3.18 This is because the standard of a 'notifiable privacy breach' requires agencies to establish that actual harm has occurred to an affected individual or individuals (or that there is a risk that it will do so) from the point of view of the individual, rather than by reference to an objective standard. When determining whether a particular breach is a 'notifiable privacy breach', agencies will be required to step not into the shoes of a reasonable person, but into the actual shoes of the individual to whom the privacy breach relates. That individual may, unbeknown to the agency, be of a particular mental fragility or sensibility such that the individual will suffer harm from the privacy breach, notwithstanding that such breach would not normally have that effect on the population at large would they be in that individual's position. Accordingly, it may only be possible to identify that actual harm has been caused well after the time the breach occurs.

3.19 While we generally support the obligation to report a notifiable privacy breach, we believe that the Privacy Bill already adequately addresses the ramifications of a privacy breach on affected individuals who suffer harm from that breach such that the obligation imposed on agencies to report notifiable privacy breaches should be limited to those circumstances only where the breach is objectively of a nature that is likely to cause harm (or that there is a risk that it will do

so). Against this background, we consider that it would be useful to expressly prescribe that privacy breaches in respect of certain limited classes of inherently 'sensitive' personal information should be deemed to meet the standard of a notifiable privacy breach.

3.20 With the above in mind, we propose that the definition of '**notifiable privacy breach**' in clause 117 of the Privacy Bill is included as a standalone provision (as subsection (2), with the existing subsection (2) to be renumbered accordingly), and amended to read as follows:

> (2) For the purposes of this Act, **notifiable privacy breach** means:
>
> (a) a privacy breach that a reasonable person would consider is likely to ~~has~~ caused ~~d~~ any of the types of harm listed in **section 75(2)(b)** to an affected individual or individuals, or there is a risk it will do so, taking into account the likelihood that the privacy breach may cause any of the types of harm listed in **section 75(2)(b)** on each affected individual if the affected individual were reasonable person;
>
> (b) without limiting **subsection (2)(a)**, includes a privacy breach where personal information relating to an individual is disclosed or accessed other than in accordance with this Act, or is lost, and that personal information is personal information which:
>
> (i) relates to the physical or mental health or condition of that individual;
>
> (ii) relates to the sexual life of that individual; or
>
> (iii) relates to the commission or alleged commission by that individual of any offence.

Territorial effect

3.21 We consider that it is desirable for New Zealand privacy law to expressly state the territorial limits within which it is intended to apply and, if applicable, the scope of its application to agencies which are located outside New Zealand.

3.22 The Committee will be aware that, in general, New Zealand law does not automatically apply to activities, people or property that are not within New Zealand's territory.

3.23 The Privacy Bill contemplates its own territorial application:

a in clause 8, whereby personal information may be deemed to be held by an agency within New Zealand ('Agency A') if that personal information is held on behalf of Agency A by an agency that is outside New Zealand ('Agency B'), where Agency B is holding the personal information as agent for Agency A, for the purposes of safe custody on behalf of Agency A, or for the purposes of processing the information on behalf of Agency A;

b in IPP 11, whereby limits are placed on an agency's ability to disclose personal information to an overseas person;

c in clause 20, which prescribes the circumstances in which the IPPs will apply to personal information that is held outside New Zealand by an agency (including where the information has been transferred out of New Zealand by that agency or any other agency).

3.24 In particular, with respect to persons who collect personal information over the internet, it is arguable that the collection of that personal information through servers located outside New Zealand is an activity that takes place outside New Zealand (notwithstanding that the individual providing the information is located within New Zealand) and therefore on the face of it falls outside the scope of New Zealand privacy law. Against this background, it is noteworthy that each of clause 8, IPP 11 and clause 20 appear to contemplate that personal information must be first collected in New Zealand (and subsequently transferred out of New Zealand) before they are triggered – a notion that is inconsistent with an agency collecting personal information online, from an overseas location.

3.25 In our view, this situation creates an uneven playing field for New Zealand-based agencies who are clearly subject to New Zealand privacy law. They must comply with New Zealand law and absorb the costs of doing so. On the other hand, those overseas companies who are able to offer goods and services into New Zealand using an online platform that is hosted overseas are granted a competitive advantage through the fact that they are not required to comply with the same laws as New Zealand-based companies who otherwise operate in the same industry.

3.26 While we appreciate that from a practical perspective it will be difficult for the Privacy Commissioner to regulate the conduct of persons who are outside New Zealand, we consider that the Privacy Bill should expressly apply the high standards of New Zealand's privacy law to any person who offers goods or services to individuals based in New Zealand.

3.27 With the above in mind, we propose an amendment to the definition of 'agency' in clause 6 of the Privacy Bill, by inserting new subsection (b) (with the existing subsection (b) to be renumbered accordingly and the words 'but' removed from the existing subsection (a)), as follows:

(b) includes any such person or body of persons regardless of whether the person or body of persons is situated, established or incorporated in New Zealand, if that person or body of persons collects personal information from an individual situated in New Zealand in the course of offering goods or services to that individual; but

Data portability

3.28 We support the Privacy Commissioner's calls for the Privacy Bill to include a right of 'data portability'; that is, a right for an individual to receive their personal information in a commonly-used machine readable format.

3.29 The right to data portability has been adopted by the EU in the GDPR and is recognised as improving consumer choice by facilitating the transfer of an individual's personal information from one agency to another, at the individual's direction. It recognises the individual sovereignty that an individual has in respect of his or her personal information and enables individuals to control their 'digital footprint' by providing individuals with an avenue through which other persons may have access to their personal information.

3.30 The right to data portability that has been adopted in the GDPR applies only to personal information that the individual has provided to the agency in question; that is, it does not apply to personal information that the agency has itself created or that the agency has obtained from a third party. We consider that the right to data portability, if any, adopted by New Zealand privacy law should also be limited in scope in this manner.

3.31 IPP 6 of the Privacy Bill (which updates IPP 6 of the current Act) grants individuals the right to receive from an agency access to his or her personal information. That right is subject to Part 4 of the Privacy Bill, including clause 62.

3.32 We propose an amendment to clause 62 of the Privacy Bill, by inserting new subsections (1) and (2) as follows:

> (1) Except in respect of those agencies or classes of agencies prescribed in regulations made under this Act, to the extent that the information requested by an individual under **IPP(6)(1)(b)** is personal information that the individual has provided to the agency or which the agency has generated for the individual in the course of providing goods or services to the individual, the agency must make the information available to the individual in a structured, commonly-used and machine-readable format which the individual is free to transmit to any other person without the agency's consent.

3.33 Subsection (2) of that section should be expressly subject to subsection (1). The remainder of the subsections will require renumbering accordingly.

3.34 In addition, we consider that if this right is to be introduced, agencies will require an appropriate lead-time before individuals are entitled to exercise this right. We expect that agencies will need to consider their existing systems and how personal information is recorded in those systems, and implement changes to those systems in a manner which enables the efficient and convenient 'packaging' of an individual's personal information in a way which empowers agencies to comply with requests for data portability.

3.35 It may also be that there are certain industries in respect of which it is not appropriate for individuals to have this right, due to the nature of the personal information collected or the manner in which the personal information is collected.

3.36 With the above in mind, we propose an amendment to clause 213 of the Privacy Bill, by inserting a new subsection (e) as follows:

> (e) prescribing the agencies or classes of agencies in respect of which **section 62(1)** does not apply.

3.37 In addition, we propose an amendment to clause 2 of the Privacy Bill, as follows:

> (2) Commencement
>
> (a) Subject to **subsection (b)**, ~~T~~this Act comes into force on **1 July 2019**.
>
> (b) **Section 62(1)** comes into force on **1 July 2022**.

4 Further information

4.1 We are happy to discuss any aspect of our feedback on the Bill.

4.2 Thank you for the opportunity to submit.

Yours faithfully
Kensington Swan

Hayden Wilson
Partner

P: +64 4 915 0782
E: hayden.wilson@kensingtonswan.com

Alternative contact: **Campbell Featherstone**
Senior Associate

P: +64 4 498 0832
E: campbell.featherstone@kensingtonswan.com