NEW ZEALAND LAW SOCIETY

NZLS EST 1869

Privacy Bill

24/05/2018

Submission on the Privacy Bill

Introduction

1. The New Zealand Law Society (**Law Society**) welcomes the opportunity to comment on the Privacy Bill (**the Bill**).

2. The Law Society supports provisions in the Bill that enhance the protection of personal information in an increasingly complex information environment. Personal information plays an integral role in the digital world, with heightened risks as shown by recent examples of data breaches. The Law Society is pleased that the Bill updates the law in relation to these risks.

3. The Law Society recognises the value of the comprehensive work undertaken by the Law Commission on privacy law reform, and it is pleasing to see the Commission's recommendations take shape in the legislation that will replace the Privacy Act 1993.

4. This submission makes recommendations to ensure that the reforms proposed in the Bill are workable in practice, and will operate in a proportionate and clearly justified way. Some additional amendments are suggested, to resolve known uncertainties with interpretation of the law or to fill known gaps. The key recommendations are:

    a) To extend the definition of "news medium" to include new media publishers (such as bloggers) who meet appropriate safeguards (clause 6).

    b) To amend Information Privacy Principle 1 to include an obligation for agencies to allow individuals to transact with them anonymously, unless the nature of the transaction requires the individual to be identified (clause 19).

    c) To delete the specific reference to age in Information Privacy Principle 4 and insert instead a reference to "vulnerability" as one potential factor to take into account (clause 19).

    d) To develop clearer rules around cross-border disclosure (clause 19), and to group these provisions together in one place in the Bill.

    e) To amend clause 24(1)(b) to allow individuals to be exempt from the privacy principles only when they collect information by lawful means. In addition, individuals who cause a data breach while acting solely for their personal or domestic affairs should not be subject to the breach notification provisions in Part 6 of the Bill.

    f) The select committee should explore the possibility of creating a fifth Public Register Privacy Principle to provide a more effective mechanism for people who are seeking suppression of their details on public registers (clauses 29 – 34).

    g) In the interests of clarity, drafting should be simplified to eliminate the separate provisions for requests for information made under IPP6(1)(a) (a request for whether the agency holds personal information about the requester at all) and IPP6(1)(b) (a request for access to that information).

    h) In relation to complaints, the Bill should be amended so that "any person", rather than only "aggrieved individuals", can make a complaint to the Commissioner. This would permit organisations who advocate on behalf of the public to make complaints. Part 5 should also be amended to permit representative complaints which are complaints

brought by a representative person or body on behalf of a group of complainants (akin to a class action).[1]

i) In relation to the enhanced role of the Human Rights Review Tribunal, the Tribunal is currently facing an unprecedented backlog. We recommend that the select committee notes there is an urgent and substantial need to address the Tribunal's workload, so that the Tribunal is able to perform its role effectively.

j) In relation to notifiable privacy breaches, the current test of ""interference with privacy"" is open to widely varying interpretations. This will make the law uncertain and difficult to apply. As a result, there will likely be substantial over-notification. We recommend that the select committee consider adopting the threshold of "*serious harm*" in the Australian Privacy Act 1988.

k) Clause 173, which permits information sharing arrangements in Schedule 5 to be amended by Order in Council, should be deleted.

5. The select committee's consultation on the Bill will also, and justifiably, be seen as a chance to consider issues that have arisen since the Law Commission reported in 2011. For instance, the committee may decide that it would be useful to introduce additional provisions that would further align the Bill with comparable legislation overseas (including Europe's new General Data Protection Regulation). The Law Society would welcome the opportunity to provide a supplementary submission if any of these major issues are proposed to be added to the Bill.

6. The Law Society would appreciate the opportunity to appear before the committee.

Clause 6: Definition of "news medium"

7. Under the Privacy Act 1993 (**the Act**), news activities ("gathering of news … or dissemination to the public of an article or programme of or concerning news, observations of news, or current affairs") conducted by a news medium ("an agency whose business, or part of whose business consists of a news activity") are not governed by the Information Privacy Principles (IPPs). They are exempt from the Privacy Act.

8. In 1993 when the Act was passed, it was relatively clear what types of organisations or people met the definition of a "news medium" engaging in "news activities". However, changes to technology – particularly social media and blogging – have revolutionised the ability of ordinary people to publish information, opinion and commentary. As a result, it has become significantly less clear who can be said to be a "news medium". This has led to some contradictory court judgments (including not only bloggers, but journalists who publish books),[2] and clarity would be welcomed.

---

1 Law Commission, *Review of the Privacy Act 1993 (Stage 4)* Report 123, June 2011 at [6.52].

2 See for instance *Dotcom v Attorney General* CIV2013-404-2168 [2014] NZHC 1343 at [66]-[71]; and the Privacy Commissioner's opinions on complaints involving Cameron Slater, Nicky Hager and the *Dirty Politics* book, and John Roughan's request for discovery from then Prime Minister John Key, whom Mr Roughan was suing for defamation https://privacy.org.nz/blog/when-is-a-journalist-not-a-journalist/.

9. The Law Commission addressed the issue in its *Review of the Privacy Act* (R38, R39), but in its initial response to that report, the Government noted that those two recommendations would best be considered as part of the *News Media Meets 'New Media'* reference.[3]

10. In that subsequent report[4] the Law Commission expanded on its privacy review recommendations. It concluded that there is a need to change the statutory definitions to make it clear when a publication is exempt from the Privacy Act. Its aim was to protect freedom of expression and the democratic role of the media appropriately, but also to ensure that there was effective oversight and access to remedies when a person considered that a publisher (such as a blogger) had breached their privacy.

11. The Law Commission recommended that:

> "The various statutes which currently confer privileges or exemptions specifically on the news media should be amended to ensure that in each instance the term "news media" is consistently defined as meaning entities which meet the following statutory criteria:
>
> (a) a significant element of their publishing activities involves the generation and/or aggregation of news, information and opinion of current value;
>
> (b) they disseminate this information to a public audience;
>
> (c) publication is regular and not occasional; and
>
> (d) the publisher must be accountable to a code of ethics and to a regulatory body such as the [Media Council].[5]

12. While some aspects of the *News Media meets New Media* report were adopted as part of the Harmful Digital Communications Act 2015, the recommendation on the news media definition has not yet been enacted. The Privacy Bill presents an opportunity to address this, to ensure the law is fit for purpose in the modern publishing environment.

13. The Law Society therefore **recommends** that the Law Commission's proposed definition of "news media" be added to the Bill.

Clause 19: Information privacy principle 1

14. A major recommendation from the Law Commission in its *Review of the Privacy Act 1993* report was that Information Privacy Principle 1 should be amended to require agencies to allow individuals to transact anonymously or pseudonymously, provided that the nature of the transaction did not require the person to be identified.[6] The recommendation was accepted at the policy stage, and by Cabinet,[7] but it has not made its way into the Bill.

---

3 https://www.justice.govt.nz/assets/Documents/Publications/government-response-to-law-commission-report-on-the-review-of-the-privacy-act-1993.pdf, page 6.

4 "The news media meets 'new media': Rights, responsibilities and regulation in the digital age" (March 2013), see http://r128.publications.lawcom.govt.nz/uploads/NZLC-R128-The-news-media-meets-new-media.pdf at page 6.

5 Recommendation 10, p.198.

6 Law Commission *Review of the Privacy Act 1993* (June 2011), Recommendation 35, p. 122. See http://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20R123.pdf

7 https://treasury.govt.nz/sites/default/files/2014-08/ris-justice-sgr-aug14.pdf, page 28. [check]

15. The Law Society suggests this is an omission that needs to be rectified. The ability to transact anonymously is present in comparable legislation overseas.[8] Placing a positive obligation on agencies to consider whether they can accommodate anonymous transactions reduces the potential for over-collection of information. It provides an important up-front safeguard for individuals, particularly in the online environment. It fits well with and enhances the existing protections in principle 1, which requires agencies only to collect the personal information that are "necessary for a lawful purpose".

16. The Law Society **supports** the Law Commission's recommendation that principle 1 should be "amended by adding a new sub-clause providing that individuals should be able to interact with agencies anonymously or under a pseudonym, where it is lawful and practicable to do so in the circumstances".[9]

Clause 19: Information privacy principle 4

17. Information Privacy Principle 4 deals with the way in which personal information is collected (as distinct from the content of that personal information). The rewording largely re-enacts the effect of the existing privacy principle.

18. However, principle 4(b) now also states that the age of the individual concerned is a particularly relevant factor to consider when looking at whether the means of collection are, in the circumstances, fair and not unreasonably intrusive. This reflects a Law Commission recommendation,[10] but presents some difficulties once drafted.

19. While age – whether youth or seniority – is clearly one potential factor in considering whether the means of collection are fair and proportionate, it is not the only type of potential vulnerability that might be relevant. Singling out age and not (for instance) disability, seems unjustifiable. A more general reference to the *vulnerability* of the individual concerned would be preferable.

20. Also, vulnerability of any type is not the only (nor, often, the principal) factor affecting whether collection is unfair or unreasonably intrusive. For example, a common situation in which collection is unfair is where the agency collects information covertly, without a proper justification for doing so. The way in which the principle is currently worded risks distracting users from their more fundamental obligations to act appropriately when collecting personal information.

21. The Law Society **recommends** that principle 4(b) be amended to read:

> "(b) by a means that, in the circumstances of the case (including, where relevant, the vulnerability of the individual concerned),".

Clause 19: Information privacy principle 11

22. Information Privacy Principle 11 places limits on the disclosure of personal information. In the Bill, some new subclauses have been added to that principle, to provide greater protection when personal information is sent offshore.

23. Providing this greater protection was a key aspect of the Law Commission's recommendations (see chapter 11 of *Review of the Privacy Act*).

---

8 See, for example, APP2 in the Australian Privacy Act 1988.

9 Law Commission *Review of the Privacy Act 1993* (June 2011), Recommendation 35, p. 122.

10 Recommendation 120, p.307.

24. The Law Society makes the following comments about whether the Bill as currently drafted successfully fulfils the policy intent.

25. **First**, it may prove more useful to create a separate Part of the Act to deal with offshoring of personal information, or at least to place the existing subsections in distinct sections rather than including them as part of IPP11. This would highlight the importance of this new feature of the Act, and make it easier to locate and use.

26. It would also be valuable if all the provisions on offshoring of personal information could be grouped together, preferably early in the Act so that they are close to other relevant sections such as section 8 (which governs when an agency will be said to "hold" personal information, so as to be responsible for it). In the current Bill, the Commissioner's existing powers to issue notices prohibiting data export (where New Zealand is being used as a conduit for personal information) are located towards the end of the Act, in Part 8. The separation of these provisions is somewhat illogical and will make it harder for agencies to assess how to properly apply the law.

27. **Secondly**, subclause (1) – that is, each of the current exemptions to IPP11 – apply when an agency holds *a belief, on reasonable grounds*, that the exemption applies. Even if, factually, it transpires that the belief was misplaced, the agency will not be liable as long as the belief was reasonable at the time.

28. Subclause (3) limits when certain exceptions in subsection (1) can apply to a cross-border disclosure by requiring the overseas disclosure to meet one of four additional requirements. However, subclause (3) does not incorporate the threshold of "belief on reasonable grounds", except for (3)(d). So whether most aspects of subclause (3) apply is an objective factual question.

29. This appears appropriate in the case of (3)(a) or (3)(c) which are both strictly factual matters (either the agency is acting as agent or is not; or the overseas recipient is in a prescribed country or it is not).

30. However, it is less clear how subclause (3)(b) will work. Subclause (1)(c) allows the agency to disclose information if it has a reasonable belief that the individual has authorised the disclosure, but it appears that subclause (3)(b) will only apply if the individual has in fact authorised the disclosure. This creates the potential for confusion.

31. The intent appears to be that individuals must expressly authorise the disclosure of the information in order to take advantage of subclause (3)(b). This may well be appropriate from a policy perspective, to provide a greater level of privacy protection. However, if so, the Law Society **recommends** that the need for express authorisation is made explicit in subsection (3)(b), to prevent confusion about the interpretation of the section.

32. **Thirdly**, we note that the protections intended by subclauses (3) – (6) are likely to be undermined when the disclosure is from agency A to its agent (B) that is located overseas. A common example might be where B is a cloud service provider overseas.

33. The explanatory note to the Bill states that disclosure to an overseas person will generally only be permissible if there is consent, if the overseas agency is in a prescribed country, or if agency A reasonably believes that B has comparable privacy obligations. However, the effect of subclause (3)(a) is that none of these protections will apply if B is the agent of A.

34. It is unclear why agency A should not still be expressly required under subclause 3(a) to ensure that personal information is adequately protected when it is in the hands of B (for

example by using standard contractual clauses, by obtaining consent, or by using agents located in prescribed countries). This would complement and extend the existing (but non-specific) obligations under IPP5 to ensure that information is kept safe when it is passed to a third party.

35. We also note that prescribed countries are to be set out in regulations. Using regulations for this purpose appears appropriate. Also, having regulations that prescribe 'safe harbour' countries may substantially reduce compliance costs for agencies that are sending personal information offshore. It is therefore important that the regulations for countries that most obviously have equivalency are published by the time the new Privacy Act comes into force.

36. However, assessing which countries should be 'prescribed' is a potentially complex and time-consuming task. The Regulatory Impact Statement accompanying the supplementary government response to the Law Commission's review acknowledged this (page 20). We recommend that the select committee note this point, and obtain assurances that work on the regulations will proceed as a matter of priority.

37. Finally, new IPP11(1)(i) states that an agency may disclose information to another agency if that agency believes on reasonable grounds that "the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern". The Law Society **recommends** that this be widened to include circumstances where part of a business is being sold.

Clause 24: Exemption for personal information relating to domestic affairs

38. This exemption largely re-enacts and clarifies the existing section 56 of the Privacy Act. This provision has not always been well understood, and clause 24 is a welcome clarification. It is also beneficial that the exemption will only apply when an individual is acting solely (rather than "solely or principally") in relation to their personal or domestic affairs.

39. The Law Society has two suggested amendments to the section.

40. First, clause 24(2)(b) states that IPPs 5 to 11 do not apply if the individual is holding "personal information that was collected by a *lawful means* **…".** However, the reference to collecting by a lawful means is not reflected in clause 24(1), which provides the exemption that relates to the collection of information. This appears to be an oversight.

41. It is therefore **recommended** that clause 24(1)(b) is amended to read "is collecting personal information by a lawful means solely for the purposes of, or in connection with, his or her personal or domestic affairs."

42. Secondly, if an individual acting in relation to his or her personal affairs causes a data breach, there appears to be no exemption from the notification requirements in Part 6 of the Bill. This is problematic for a number of reasons:

    a) the notification requirements could be unduly onerous for individuals in those circumstances;

    b) the law is not likely to be well understood and applied;

    c) making individuals liable for breach notification is at odds with their exemption from IPP5 (the requirement to take reasonable steps to protect information); and

d) the severity of the penalty for failure to notify (an offence and potential fine) also appears disproportionate for individuals who make a mistake while engaging in their own personal or domestic affairs.

43. The Law Society **recommends** that a subsection be added to clause 24 to provide that an individual who is collecting, using, holding or disclosing personal information solely for the purposes of, or in connection with, his or her personal or domestic affairs is exempt from Part 6 of the Bill.

Clauses 29 – 34: Public register privacy principles

44. The public register privacy principles are not well understood and applied in the current Act. The problems with the existing public register privacy principles were canvassed in volume 2 of the Law Commission's Review of Privacy.[11] That report made various recommendations, but none of the potential changes has been enacted in this Bill. It is disappointing that the opportunity to update the legislation in this important respect appears to have been missed.

45. While it may not be possible at this stage to make more sweeping amendments, one change that it may be possible to make at the select committee stage is to adopt the Privacy Commissioner's recommendation to provide a more effective mechanism for people who are seeking suppression of their details on public registers.[12] For instance, this would usefully supplement some of the new protections for victims of family violence contained in the Family and Whānau Violence Bill, currently awaiting second reading in the House.

46. Having information publicly available (often online) on the registers can create a significant safety risk for some individuals. Most public registers provide for a suppression mechanism, where people demonstrate that they have a protection order or a harassment order in their favour. However, people need to apply separately to each public register, which is time consuming and burdensome at a time when they are already under pressure. It is also not always effective, since people may not know, or may not remember, which public registers disclose their details.

47. The Commissioner's recommendation, which the Law Society supports, is to create a single point at which people can apply for suppression of their information from all public registers. The decision whether to suppress would still be one for the individual Registrars to make, in line with their normal business rules, but having a single conduit for applications and evidence could save individuals significant time and stress.

48. One way of achieving this would be to enact a fifth Public Register Privacy Principle: that each public register must have a mechanism for individuals to apply for suppression of their details if they demonstrate that their safety is at risk; and that a named government department should be a central point through which such applications can be made.

---

11 Law Commission *Public Registers: Review of the law of privacy stage two* (January 2008), see http://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20R101.pdf, at page 41 onwards.

12 Privacy Commissioner "Report to the Minister of Justice under section 26 of the Privacy Act" (February 2017), at paras 127-132.

Part 4 – Access and correction of personal information

49. The right to access one's own personal information from an agency is probably the most fundamental of the privacy principles. It supports all the other privacy principles. It provides individuals with the ability to see what an agency knows about them and what decisions it has made, how that information is used, where it goes, and whether the information is right. Principle 6 is also the only privacy principle that is (in relation to public sector agencies) directly enforceable in a court of law.

50. It is therefore particularly important that the clauses of the Bill that deal with access to personal information should be clear. Individuals need to be able to understand what their rights are, and agencies need to be able to understand and comply with their obligations with the minimum of uncertainty.

51. There are some welcome improvements to the drafting of the exceptions to the duty to provide access (clauses 52 – 57). These provisions are now clearer overall than the provisions in the current Privacy Act, particularly the evaluative material exception in clause 53. The thematic grouping is also beneficial.

52. However, many of the provisions in Part 4 now distinguish between requests made under IPP6(1)(a) (a request for whether the agency holds personal information about the requester at all) and IPP6(1)(b) (a request for access to that information). Some provisions are duplicated, to cater for these different types of requests.

53. The Law Society appreciates that it appears logical, from a pure drafting perspective, to treat these requests differently, particularly in relation to requests for confirmation about whether information is held at all (the withholding grounds will not generally come into play). However, the practical effect is counterproductive. It is noted that:

    a) Referring separately to IPP6(1)(a) and (1)(b) adds significant complexity where there is none currently, and it is not clear that the complexity adds any value – for example, it does not enhance or clarify rights or obligations (in fact it appears to have the opposite effect).

    b) In practice individuals usually simply ask for their information rather than asking for confirmation as to whether the agency holds any information. They do not make separate requests in the way the drafting suggests. They do not – and should not have to – approach IPP6 requests in a legalistic way.

    c) The drafting makes the provisions far harder to read and to navigate. It may introduce a level of confusion for agencies and the public about how to manage access requests in a straightforward, helpful, and non-legalistic way.

    d) The change in wording may lead some agencies to believe that the access provisions have changed, where in fact the effect is intended to be the same. This could cause unnecessary changes and compliance costs.

54. It is therefore **recommended** that the drafting is simplified, to eliminate the separate references to IPP6(1)(a) and (1)(b).

55. Similarly, subpart 2 (clauses 64 – 59) treats a request for correction and a request to add a statement of correction separately. Again, there is no practical value to this exercise. They can both be treated as a 'request for correction' and dealt with in the same way.

Part 5: Complaints, investigations, and proceedings

Restricted class of complainants

56. The Act provides in section 67(1) that "any person" may make a complaint to the Commissioner about an interference with the privacy of an individual. Clause 77(1) of the Bill would restrict the class of potential complainants to "aggrieved individuals" or their representatives. Accordingly, the Bill would prevent organisations who advocate on behalf of the public, or sections of the public, to complain to the Commissioner about apparent privacy breaches unless they act as a person's "representatives". Organisations who are well-placed to make complaints about privacy breaches affecting the general public might include Privacy Foundation NZ or the Human Rights Commission.[13]

57. A comparison may be drawn with the Human Rights Act 1993, under which advocacy groups may make complaints of discrimination and appear as plaintiffs in subsequent proceedings in order to raise issues of public importance.[14] It is therefore **recommended** that the Bill is amended so that "any person", rather than only "aggrieved individuals", can make a complaint.

58. The current drafting of clause 77(1)(b) does not appear to accurately reflect the Law Commission's recommendation (R60) that the new Act should expressly provide for the ability to bring representative complaints.[15]

59. A **representative complaint** (for instance an advocacy group bringing a complaint about a potential breach of the privacy of a large number of people) is not the same as a complaint brought by a **"representative of** 1 or more aggrieved individuals" (the clause 77(1)(b) wording). People can file complaints through representatives now: the clause 77(1)(b) wording would not add anything to existing rights. While representative complaints can almost certainly already be brought under the current Act, the Law Commission saw value in making that right explicit. The Commissioner would retain the ability to refuse to investigate complaints, particularly where the aggrieved person does not want an investigation.

60. The Law Society therefore **recommends** that clause 77(1)(b) be redrafted to accommodate representative complaints, in the sense intended by the Law Commission. (Representative parties should also have access to the Tribunal, although they should not be able to claim compensation in their own right.)

Proceedings commenced in the Tribunal by an aggrieved individual

61. Clause 103 lists the circumstances in which an aggrieved individual may commence proceedings in the Human Rights Review Tribunal.

62. The Law Society **recommends** that clause 103(1)(e) is amended to clarify that it only applies when clause 96[16] applies. Otherwise, clause 103(1)(e) could, unintentionally, be

---

13 However, those organisations would still need to show evidence of an interference with the privacy of a (presumably identifiable) individual.

14 See e.g. *Child Poverty Action Group Inc v Attorney-General* (2005) 7 HRNZ 939 (HC) and related proceedings and *Adoption Action Inc v Attorney-General* [2016] NZHRRT 9.

15 Footnote 1 above: *Review of the Privacy Act,* at [6.55] onwards.

16 Cl 96*: Procedure after completion of investigation relating to breach of IPP6*.

satisfied in a large number of cases. Clause 103(1)(e) could be amended to read "section 96 applies, but the Commissioner does not make a direction under section 96(5)(a)".

63. The time limits for filing proceedings in subclauses 103(2) – (8) appear to be strict. The Bill does not provide for extensions if (for example) the aggrieved individual is under a disability or where circumstances beyond the person's control prevented proceedings from being filed. Six months is a reasonable timeframe within which people can be expected to file proceedings, but inflexibility may lead to unfair disadvantage in a small number of cases. However, providing a discretion for the Tribunal to extend that deadline, similar to clause 111(2), would be likely to lead to a number of non-meritorious applications that could put further pressure on the Tribunal's already stretched resources. Maintaining a strict limitation period therefore appears preferable on balance.

Costs against the Commissioner

64. Clause 115(3) provides that the Commissioner may not be indemnified by an aggrieved individual in respect of any costs the Commissioner is required to pay "under subsection (1)". It appears this should refer to "subsection (2)". It is therefore **recommended** that the final words of clause 115(3) are amended to read "under subsection (2)".

Proceedings in the Human Rights Review Tribunal

65. As with the Act, many matters arising under the Bill will be the subject of proceedings in the Human Rights Review Tribunal.

66. In addition, Part 6 of the Bill creates several new roles for the Tribunal. Most notably, the Tribunal will be able to enforce compliance notices made by the Commissioner, and hear appeals against compliance notices. The Chair of the Tribunal may also be called upon to issue interim orders suspending the effect of a compliance notice until the appeal can be heard.

67. The intention behind the enforcement procedure is sound, and it is a central facet of the Bill, but it is likely that it will not function as intended unless existing delays in the Tribunal are resolved by the time the new Act comes into force. The new procedure may substantially increase the Tribunal's current workload.[17]

68. The Tribunal remains under an unprecedented backlog. In most cases, even a straightforward matter will not receive a date for a teleconference for at least twelve months and will not be heard for at least two years after filing. A decision might not be delivered for at least a few months and possibly a few years after a hearing. The Chairperson of the Tribunal, Mr Rodger Haines QC, has noted that "[f]or most parties, the Tribunal has ceased to function".[18]

69. Accordingly, many parts of the Bill (including Part 6) will not operate as intended for want of an effective enforcement power.

70. The Law Society therefore **recommends** that the committee notes there is an urgent and substantial need to address the problems that the Tribunal is facing. One practical measure would be to include a consequential amendment to the Human Rights Act, allowing for the

---

17 The increased workload due to Part 6 will be offset slightly by granting the Commissioner a binding power of direction in matters involving a breach of IPP 6 (with an appeal to the Tribunal): cl 96.

18 Mr Rodger Haines QC, "Submission on the Tribunals Powers and Procedures Legislation Bill", 12 February 2018, at [3].

appointment of one or more Deputy Chairpersons of the Tribunal (a role not currently provided for by the statute) and for any Deputy to be able to fulfil any statutory functions or powers that are delegated to her or him by the Chairperson.[19]

Part 6: Notifiable privacy breaches

71. A "notifiable privacy breach" is defined in clause 117(1) as "a privacy breach that has caused 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". The types of harm specified in clause 75(2)(b) include action (i) causing loss, detriment, damage or injury to the individual, (ii) adversely affecting the rights, benefits, privileges, obligations, or interests of the individual, or (iii) resulting in significant humiliation, loss of dignity, or injury to the feelings of the individual. However, no guidance is given as to how *likely* it must be that the harm will actually materialise.

72. There is a logic to this approach, as it directly ties harm suffered by breaches to the types of harm already recognised by the Privacy Act in its definition of "interference with privacy".

73. However, in practice, that harm threshold is flexible and highly contextual. It is open to widely varying interpretation in individual circumstances (which matters less where harm forms a threshold for liability rather than triggering an obligation). This uncertainty is likely to lead to over-notification, since agencies will be likely to err on the safe side and notify even when this is not required.

74. Instead of using the 'interference with privacy' test, the Law Society **recommends** a more 'bright line' test for triggering the new statutory obligations associated with breach notification. That test, at a suitably high level, would fit with the recommendations of the Law Commission report in two ways: first, the Commission suggested that the threshold for notification should be "a reasonably high one", and that the obligation to notify should arise "in a minority of cases".

75. One option would be to adopt the threshold of "serious harm" from the new mandatory breach notification provisions in the Australian Privacy Act. It states that an "eligible data breach" is (amongst other criteria) where (a) "there is unauthorised access to, or unauthorised disclosure of, the information"; and (b) "a reasonable person would conclude that the access or disclosure would be likely to result in serious harm, to any of the individuals to whom the information relates". The Australian Act then sets out eight factors that are relevant in determining whether a reasonable person would conclude that access to, or disclosure of, information would be likely to result in serious harm.[20]

76. The Australian approach maintains a degree of flexibility, but the additional guidance reduces the level of uncertainty involved. It would also go some way to avoiding over-reporting and also assist relevant decision-makers in determining whether an agency's decision was "reasonable" so as to provide a defence to the clause 122 offence of failing to notify the Commissioner. It would also have the additional benefit of aligning the new New Zealand rules with those used by a key trading partner.

---

19 As recommended by Mr Rodger Haines QC: see footnote 18, at [4] – [5].

20 Section 26WG.

77. The clause 117 definition of "privacy breach", at (a)(ii), includes actions that prevent the agency "from accessing the information on either a temporary or permanent basis". The intention behind this clause is to capture breaches caused by ransomware attacks, or similar (usually malicious) deprivations of access to information. However, as worded, it could be read to include any situation in which an agency loses the ability to access their files, such as through a power outage. Not all such situations would jeopardise the security of personal information in the way that the provision intends.

78. The Law Society therefore **recommends** that subclause (a)(ii) should be amended to read "an action that prevents … and that causes or may cause any of the effects stated in subclause (a)(i)."

79. Clause 120 sets out exceptions to the obligations to notify an affected individual or give public notice of a notifiable privacy breach. The exceptions in this clause are all expressed objectively. Given that failure to comply is a criminal offence (cl 122(2)(a)), it would seem appropriate to make the exceptions consistent with the "believes on reasonable grounds" terminology used in the IPPs. (Strict liability would be more appropriate if liability were reduced to the civil, rather than criminal, standard.)

80. Similarly, the exception in clause 120(2)(a) includes a subjective test ("the agency is satisfied that the notification or notice would be contrary to that person's interests"), but should instead require the agency to be satisfied "on reasonable grounds" that the relevant circumstances apply. It is therefore **recommended** that the exceptions in clause 120 should all apply only if the agency believes on reasonable grounds that the relevant circumstances apply.

Clause 173: Power to amend Schedule 5 by Order in Council

81. The Bill authorises named public sector agencies to have access to specific types of law enforcement information held by other named public sector agencies. These information sharing arrangements are all recorded in Schedule 5. They are clearly defined and appear to be justified. Many are long standing arrangements and most have been added to the Schedule by primary legislation over the years. The Bill continues these information sharing arrangements, which is appropriate.

82. However, the Law Society is concerned about the power created by clause 173 to amend Schedule 5 by Order in Council. The ability to amend primary legislation through an executive order is generally known as a "Henry VIII" clause. It is usually objectionable under the principles of the rule of law, particularly where it can fundamentally affect rights or obligations.

83. Deciding which agencies can share certain types of law enforcement information – and with whom – is not a minor technical or administrative matter. Law enforcement information is often negative (such as the fact that someone is a wanted person, or is the subject of a protection order), and use of it can have serious consequences. It may fundamentally affect people's rights. While it will be appropriate to add new arrangements from time to time, each new proposal deserves proper scrutiny by Parliament.

84. Clause 173 requires the responsible Minister to consult with the Privacy Commissioner before making changes to the Schedule, which is one useful safeguard. However, the Executive will still be able to add to or otherwise change these important information sharing arrangements without Parliamentary or public scrutiny.

85. The Law Society **recommends** that clause 173 be deleted and that any changes to Schedule 5 should be made only through legislation, as is the case now.

Tiana Epati
Vice-President
24 May 2018