Privacy Commissioner's Submission on the Privacy Bill to the Justice and Electoral Select Committee

Executive Summary

1. I welcome and support the law reform package represented by the Privacy Bill. Privacy law reform has been under consideration since 1998, including the wide-ranging Law Commission review from 2006-2011.[1] These reviews and the Government response to them form the basis for the proposed modernisation of the legislation.[2]

2. The reforms in the Privacy Bill are necessary for New Zealand's regulatory framework to catch up with developments in international best practice. However, the reforms need to go further than those proposed in the Privacy Bill as introduced.

3. The Bill is based on a set of reform recommendations that are now 7 years old. It needs to be refreshed to address current issues of concern. There has been dynamic change in the global digital environment over this period with significant implications for personal information. Privacy laws in other countries have since been reformed to address the impacts. New Zealand now has the opportunity to ensure our privacy statute is up to the task of protecting the personal information of individuals from misuse and addressing serious risks to privacy.

4. Two key criteria have guided my response to the proposals and redrafting in the Bill, and my proposals for further reforms to be included:

   a) Do the provisions in the Privacy Bill enhance or retain privacy rights for New Zealanders?

   b) Is any compliance burden on agencies justified?

5. My submission is in two parts. Part A addresses the matters I consider necessary to update and enhance the Privacy Bill. This includes the need to address current gaps in the regulatory design, such as making provision for the inclusion of civil penalties in the Bill for serious non-compliance, and requiring agencies to report on steps taken or to be taken to ensure they are in compliance with the new Act.

6. In addition, I recommend in Part A that the complaints system should be rationalised by implementing the Law Commission's recommendation to discontinue the role of the Director of Human Rights Proceedings in privacy cases. My recommendations include proposed amendments to achieve these reforms.

[1] See NZLC SP 19 (2008), R101 (2008), R 113 (2010), IP17 (2010), R123 (2011); OPC *Necessary and Desirable* (1998-2008).
[2] The Government response to the Law Commission's report includes an initial response in 2011 and a detailed response in 2014.

7. I also recommend in Part A that the privacy principles need to be enhanced to take account of fundamental changes to the way in which personal information is provided, handled and used, and the potential impacts resulting for individuals. These enhancements include:

   a) Strengthening protections for individuals from the privacy risks of de-identification (when personal information is used for statistical and research purposes), and providing safeguards for the privacy risks resulting from re-identification events;

   b) Bolstering the right of individuals to access their own personal information by including a right to personal information portability;

   c) Supplementing the right of individuals to correct their personal information, and providing protection against the use of personal information that is out of date, inaccurate or misleading by including a right to erasure;

   d) Supporting the rights of the individual to the fair use of their personal information, and enhancing the transparency of decision-making affecting the individual by adding a new privacy principle to address automated decision-making and algorithmic transparency.

8. I am mindful that these enhancements (and others that may be proposed by other submitters) will need the opportunity for public consultation, and will need to be co-ordinated with the progress of the Bill. In light of the Committee's timeframe, I am available to offer assistance to officials and the Committee to develop the necessary consultation proposals, so that the necessary and practical amendments can be included in this Bill prior to enactment.

9. Part B of my submission comments on the Bill Part by Part. It addresses the implementation of the reform proposals and recommends necessary amendments. Part B includes recommendations that some of the proposed reforms should not proceed in the Privacy Bill or that they be implemented in a different way to better achieve the policy intent. Some of the Law Commission's proposed reforms have not yet been implemented in the Privacy Bill and I recommend they should be.

10. Part B also includes recommended amendments to a number of Privacy Bill provisions that continue current provisions in the Privacy Act. The recommended amendments are necessary to ensure that the scope and effect of the current provisions is properly carried over in the Privacy Bill.

11. I welcome the opportunity to speak to the Committee in support of my submission, at the Committee's convenience.

John Edwards
Privacy Commissioner

31 May 2018

Summary of Recommendations

Part A – Further reforms are needed in the Privacy Bill

RECOMMENDATION A.1

A civil penalty provision and ancillary provisions should be included in the Privacy Bill.

RECOMMENDATION A.2

Clause 201 of the Privacy Bill should be amended to enhance agency accountability for compliance by requiring agencies to report on request on the steps taken or to be taken to ensure their compliance.

RECOMMENDATION A.3

Law Commission recommendation 55 should be implemented in the Privacy Bill to discontinue the role of the Director of Human Rights Proceedings in privacy cases.

RECOMMENDATION A.4

The Privacy Bill should:

(a) strengthen protections for individuals from the privacy risks of inadequate de-identification of personal information for statistical and research purposes; and

(b) provide safeguards against the privacy risks resulting from re-identification events.

RECOMMENDATION A.5

The Privacy Bill should include a right to personal information portability.

RECOMMENDATION A.6

The Privacy Bill should include a new information privacy principle on the right to erasure of personal information.

RECOMMENDATION A.7

Additional provisions, including a new privacy principle, should be included in the Privacy Bill to limit the harms arising from automated decision-making and to require algorithmic transparency in appropriate cases.

Part B – Part by Part Recommendations

RECOMMENDATION B.1.1

The new Privacy Act should be named both in English and te reo Maori.

RECOMMENDATION B.1.2

The words “while recognising that other rights and interests may at times also need to be taken into account” should be deleted from clause 3(a).

RECOMMENDATION B.1.3

Paragraph (b)(ix) of the definition of "agency" should be deleted.

RECOMMENDATION B.1.4

The definition of "court" in clause 6 should be deleted and in clauses 171 and 172 the term "holder agency" should be replaced with "specified holder" and in clause 169 the words "specified agencies" replaced with "specified holders".

RECOMMENDATION B.1.5

The definition of "Minister" should include a Parliamentary Under-Secretary.

RECOMMENDATION B.1.6

In the definition of "publicly available publication" the term "statutory register" should be replaced with "public register".

RECOMMENDATION B.1.7

The Privacy Bill should include an additional provision in Part 1 of the Bill, to clarify the application of the Act to the activities of overseas agencies that collect, hold, use or disclose personal information about New Zealand individuals, and to the overseas activities of New Zealand-based agencies.

The provision should include the following elements:

a) the collection, holding, use and disclosure of personal information from New Zealanders within the jurisdiction (regardless of the physical location or place of business of the agency collecting the information) is a sufficient link for application of the Privacy Act;

b) carrying on business or trade in New Zealand or the offering of goods or services establishes a sufficient link for the Privacy Act to apply, but need not require any payment by the individual concerned;

c) activities that impact on the privacy rights of New Zealanders, based on their personal information, such as the monitoring of behaviour, establishes a sufficient link for the Privacy Act to apply;

d) the collection, holding, use and disclosure of personal information by New Zealand-based agencies is subject to the Privacy Act, regardless of whether the individuals concerned are New Zealand citizens or residents.

RECOMMENDATION B.2.1

Clause 15 should be incorporated into the list of discretionary functions in clause 14.

RECOMMENDATION B.3.1

Law Commission recommendation 35 should be implemented in IPP 1 or by an alternative drafting option.

RECOMMENDATION B.3.2

IPP 4 should not be amended as proposed. An alternative drafting option should be considered to address the collection practices of agencies when collecting personal information from children and young people.

RECOMMENDATION B.3.3

IPP 11(2) should be deleted.

RECOMMENDATION B.3.4

IPP 11(3) should include provisions permitting disclosure to participants in binding schemes that provides comparable safeguards to this Act.

RECOMMENDATION B.3.5

IPP11(3)(c) should be amended by adding the phrase "after being informed of risks arising in the absence of comparable safeguards".

RECOMMENDATION B.3.6

The definition of overseas person in IPP 11(6) should be amended by deleting "who is not subject to this Act."

RECOMMENDATION B.3.7

IPP 12(2) should be amended by replacing the second reference to the word 'assign' by the phrase 'adopt as its own identifier'.

RECOMMENDATION B.3.8

IPP 12(5) should be amended by extending its application to disclosures to 'any person' and to the display of a unique identifier.

RECOMMENDATION B.3.9

Clause 22 should be amended to limit future regulations prevailing over the privacy principles unless the empowering provision expressly authorises the override, as recommended by the Law Commission.

RECOMMENDATION B.3.10

Clause 23(3) should be deleted.

RECOMMENDATION B.3.11

Clause 24(3)(a) should be deleted.

The phrase "personal or domestic affairs" should be replaced with "personal, family or household affairs".

The structure of clause 24 should be simplified.

RECOMMENDATION B.3.12

Clause 26(1)(c) should be amended so that it does not apply to personal information about the Auditor-General's current, former or prospective staff.

RECOMMENDATION B.3.13

Subpart 3(2) should be repealed and replaced with new privacy safeguards to provide a practical suppression mechanism for individuals whose safety is at risk, and to provide for privacy complaints where public register access conditions are breached.

Alternatively, the Bill should provide for expiry of subpart 2 12 months after the Bill comes into force, to allow for a Privacy (Public Registers) Amendment Bill to be introduced, that includes a practical suppression mechanism and provides for privacy complaints where public register access conditions are breached.

RECOMMENDATION B.4.1

The drafting of Part 4 should be reorganised, following the outline provided.

Part 4 should reflect the nature of the IPP 6 access right as a right to request access to one's personal information, retaining the Act's procedure for responding to requests on the basis that access is sought, and the Act's flexibility to deal with the exceptional request for confirmation only.

The provisions should be organised to clearly set out the procedural pathway that represents the usual type of response, with particular provisions being available as relevant in specific circumstances.

To maintain the settled approach, Part 4 should retain the well-known provisions in the current Act in a similar form.

RECOMMENDATION B.4.2

Clause 47 and 67 should be amended to carry over the effect of section 38 of the Privacy Act 1993 by including the duty to assist an individual to make a request in accordance with the requirements of the Act and to make the request to the appropriate agency.

RECOMMENDATION B.4.3

Clause 68 (if retained) should be amended for consistency with clause 48(3) and (4).

RECOMMENDATION B.4.4

For clarity, and to reflect that it arises only in special circumstances, the "neither confirm nor deny" response option to an access request in clause 49(3) and 50(4) should be moved back to a standalone provision.

Sub clauses 59(1), (2)(a), (3) and (4) should be deleted.

RECOMMENDATION B.4.5

The limit on the reasons to refuse an access request in clause 50(3) should be moved to a standalone provision.

To carry over the effect of section 30 of the Privacy Act 1993, the scope of the limit should include the requirements of other laws that may provide good reason to refuse an access request.

RECOMMENDATION B.4.6

Clause 51 should be amended to include requests for a large quantity of information.

If retained, clause 71 should be amended for consistency with new clause 51(1)(c).

RECOMMENDATION B.4.7

Clause 52(1)(a)(i) should be amended to implement Law Commission recommendation 22.

RECOMMENDATION B.4.8

Clause 52(1)(c) should be amended to replace "requestor" with "individual" to preserve the scope of section 29(1)(d) of the Privacy Act 1993.

RECOMMENDATION B.4.9

Clause 52(1)(d) should be amended to replace "requestor" with "individual" to preserve the scope of section 29(1)(e) of the Privacy Act 1993.

RECOMMENDATION B.4.10

Clause 57(b) should be amended to implement Law Commission recommendation 93.

RECOMMENDATION B.4.11

Clause 57(h) should be deleted. To implement Law Commission recommendation 17, clause 63 should be amended.

To implement Law Commission recommendation 18, clause 75(3) of the Bill should be reviewed to ensure that it provides a ground of complaint for an agency's breach of clause 63, as amended.

RECOMMENDATION B.4.12

The title of clause 58 should be amended by deleting "under section 57".

RECOMMENDATION B.4.13

Clause 63 should be amended to expressly include options for an individual to request their personal information be made available to them electronically and in machine readable format. Clause 63 should also entitle an individual to request that their personal information be transferred, where technically feasible, to another agency.

RECOMMENDATION B.4.14

Clause 70 should be renamed "Statements of Correction."

Clause 70(2) should be amended by deleting "and in any case not later than 20 working days after the day on which the correction request made under IPP 7(2)(b) is received".

RECOMMENDATION B.4.15

Clause 72 should be redrafted to make clearer the matters for which an agency may or may not charge. An indicative provision is suggested.

RECOMMENDATION B.4.16

Clause 73 should be redrafted to carry over the proper effect of section 36 of the Privacy Act 1993.

RECOMMENDATION B.5.1

Clause 74 definition of "aggrieved individual" should be amended by adding the following text "(c) a proceeding under subpart 2 of this Part."

Clause 74 definition of "complainant" should be amended by replacing the word "individual" with the word "person".

Clause 74 definition of "parties" should be amended by deleting (a)(i) and including in (a)(ii) the words "or the representative of a complaint brought on behalf of a class of aggrieved individuals."

RECOMMENDATION B.5.2

Clause 77 should be amended by adding to (1)(b) the words "or a representative of a class of aggrieved individuals."

RECOMMENDATION B.5.3

Clause 80 should be amended to provide that the Commissioner may decide not to investigate a complaint if he or she considers in the circumstances, following preliminary inquiries, that any action is unnecessary or inappropriate.

Clause 80(a) should be amended by replacing the words "the complainant has not" with the words "there has not been".

Clause 80(b) should be amended by deleting the words "to the complainant".

Clause 80(e) should be amended by replacing the word "complainant" with "aggrieved individual".

RECOMMENDATION B.5.4

Clause 81 should be deleted. As a consequence, clause 79(1)(b) should also be deleted.

RECOMMENDATION B.5.5

Clause 82(1) should be amended to replace the words "on receiving a complaint" with the words "at any time after receiving a complaint."

RECOMMENDATION B.5.6

Clauses 84(2)(b) and 87(3)(b) should be amended by replacing the word "complainant" with "aggrieved individual".

RECOMMENDATION B.5.7

Clause 86(1) should be amended by deleting clauses 86(1)(a) and (b) and replacing the words "the following persons" with "the parties".

RECOMMENDATION B.5.8

Clauses 96(7), 96(8)(c) and 96(9) should be removed into a separate stand-alone clause - clause 96A entitled "Commissioner may make access direction", and a consequential amendment to clause 96(5)(a) so it refers to clause 96A;

The remainder of clause 96 should be amended as follows:

The title should be amended by deleting the words "completion of" so it refers to "Procedure after investigation relating to breach of IPP 6";

Clause 96(1) should by amended by replacing the words "completed an" with "made any";

Clause 96(2) should be deleted;

Clause 96(8) should be replaced with the following; "As soon as practicable, the Commissioner must inform the parties of the result of the investigation, including any action taken under (5) or (6)."

RECOMMENDATION B.5.9

There should be a new Clause 96A that provides for the making of an access direction and is entitled "Commissioner may make access direction".

Clause 96A should include the requirements for a notice of an access direction currently in clauses 96(7), 96(8)(c) and 96(9).

Clause 96A should also provide that the Commissioner may vary or cancel an access direction at any time if he or she considers (a) any of the information specified needs to be added to or amended in the direction; or (b) the particular way in which specified information

is to be made available needs to be amended; or (c) all or part of the notice is no longer needed.

Consequential amendments will need to be made to clauses 109 to 112 so these refer to new clause 96A.

RECOMMENDATION B.5.10

Clauses 97(6), 103(1)(g) and 103(6) should be deleted.

Clause 97 should be amended by deleting the words “completion of” in the title so it refers to “Procedure after investigation relating to charging”;

Clause 97(1) should by amended by replacing the words “completed an” with “made any”.

RECOMMENDATION B.5.11

Clause 98 should be amended by deleting the words “completion of” in the title so it refers to “Procedure after investigation relating to charging”’;

Clause 98(1) should by amended by replacing the words “completed an” with “made any”.

RECOMMENDATION B.5.12

Clause 99 should be amended by deleting the words “completion of” in the title so it refers to “Procedure after other investigations”.

RECOMMENDATION B.5.13

Clause 100(2) should be amended by replacing the word “completing” with “making”.

RECOMMENDATION B.5.14

Clause 102(1) should be amended to include references to clauses 84 and 87.

Clause 102(2)(b)(iii) should be amended by deleting the words “Commissioner’s investigation” and replacing these with “complaint or matter”.

RECOMMENDATION B.5.15

Clause 103 (1) should include after the words “aggrieved individual” the words “or the representative of a class of aggrieved individuals.”

Clauses 103(2)-(8) inclusive should be amended by replacing the words “An aggrieved individual” with “A person”.

Clause 103(9)(a) should be amended by including after the words “aggrieved individual” the words “or the representative of a class of aggrieved individuals.”

RECOMMENDATION B.5.16

Clause 109 should be amended by amalgamating clauses 109(1) and 109(2).

RECOMMENDATION B.5.17

Clause 110(1) should be amended by deleting “An agency” and replacing it with “A respondent”.

RECOMMENDATION B.5.18

Clause 111(2) should be amended to clarify that express permission or leave must be sought from the Tribunal to accept a late appeal.

RECOMMENDATION B.5.19

Clause 114(1)(b) should be deleted.

RECOMMENDATION B.6.1

The mandatory privacy breach notification scheme in subpart 6(1) should include an express obligation on an agency processing personal information or providing safe custody of information on behalf of another agency to notify that other agency without undue delay after becoming aware of a privacy breach affecting the information.

RECOMMENDATION B.6.2

The mandatory privacy breach notification scheme in subpart 6(1) should include an obligation on agencies to take appropriate measures to minimise the potential harm to affected individuals from a notifiable breach, including in relation to personal information that is no longer held by the agency as a result of the breach.

RECOMMENDATION B.6.3

The mandatory privacy breach notification scheme in subpart 6(1) should include discretion for the Privacy Commissioner to require that a notifying agency that has submitted a notice to the Commissioner under clause 118 must also submit a follow up notice recording the steps taken in response to the breach, by such later date as the Commissioner considers appropriate.

RECOMMENDATION B.6.4

The definition of “notifiable privacy breach” should provide more guidance and certainty for agencies about when a privacy breach is notifiable, for example by including factors to be taken into account and providing examples of privacy breaches that would, or would not, be notifiable.

RECOMMENDATION B.6.5

Clause 75 should make clear that undue delay in notification might constitute an interference with privacy.

RECOMMENDATION B.6.6

Clause 120 should include an exception to the requirement to notify affected individuals of privacy breaches where the agency is an individual and the information is limited to

information obtained lawfully and held by that individual in connection with household or personal affairs.

RECOMMENDATION B.6.7

Clause 121 should allow for the use of regulations to prescribe additional reporting requirements or specify reporting formats. A consequential amendment to clause 213 should be made to allow for regulations to be made for this purpose.

RECOMMENDATION B.6.8

Clause 122 should be replaced with a civil penalty provision where an agency fails to notify the Commissioner of a notifiable privacy breach.

RECOMMENDATION B.6.9

Clause 123 should be amended to clarify that it applies to the public release of details of a breach.

RECOMMENDATION B.6.10

Clause 20 of the Bill should clarify the circumstances in which personal information held outside New Zealand is subject to subpart 6(1).

RECOMMENDATION B.6.11

To simplify the implementation of the mandatory privacy breach notification scheme in subpart 6(1), clause 10 of Schedule 1 should be omitted so that obligations do not arise in relation to notifiable privacy breaches occurring before commencement. However, if the clause is retained, its application should be limited to notifiable privacy breaches that an agency became aware of after enactment of the Bill.

RECOMMENDATION B.6.12

Subpart 6(2) should, as recommended by the Law Commission, expressly include the Privacy Commissioner's discretion to publish the fact that a compliance notice has been issued.

RECOMMENDATION B.6.13

Clause 124 should be expanded in scope to include an agency's breach of a settlement assurance it has given to the Privacy Commissioner.

RECOMMENDATION B.6.14

Clause 124(2)(a) should be amended by adding the words "or may suffer" after the words "has suffered".

RECOMMENDATION B.6.15

Clause 125 should be amended to allow an agency's assurance to address a matter of non-compliance to be accepted by the Privacy Commissioner, at any time, at his or her discretion, including following a written notice outlining the breach in clause 125(3).

RECOMMENDATION B.6.16

In clauses 127, the reference to "served" should be amended to "issued" to ensure the terminology is consistent throughout this part.

RECOMMENDATION B.6.17

The Bill should make provision for the Privacy Commissioner to seek the imposition of a civil penalty for failure to comply with a compliance notice, as an alternative enforcement option to the prosecution of a criminal offence.

RECOMMENDATION B.7.1

Clause 142 should expressly provide that (a) agencies that are added or removed from the Schedule of Parties are to be notified, and (b) all other parties to the agreement are to be notified of a change to the Schedule of Parties.

RECOMMENDATION B.7.2

Clause 181(5) should be amended by deleting the word "even".

RECOMMENDATION B.7.3

a) The information matching provisions in Part 7(4) of the Bill should not be discontinued in relation to trans-border information matching agreements under the Social Welfare (Reciprocity Agreements, and New Zealand Artificial Limb Service) Act 1990, without a suitable replacement.
b) The consequential amendment to section 19(2A)(a) of the Social Welfare (Reciprocity Agreements, and New Zealand Artificial Limb Service) Act 1990 should be amended to (i) retain the reference to the information matching guidelines for this purpose, or (ii) replace that reference with appropriate criteria on which the Privacy Commissioner reports to Ministers, such as the criteria in clause 149(2) of the Bill.

RECOMMENDATION B.7.4

Minor and technical amendments should be made to clauses 136, 175, 177, 183 and 187.

RECOMMENDATION B.9.1

To fully implement the Law Commission's recommendation 66(a), clause 212(2)(c) should be amended as follows:

a) include as a further element of the offence that the conduct in question misleads an agency; and
b) include an offence of misrepresenting to an agency the existence or nature of an authorisation from an individual that has the effects in clause 212(2)(c)(i) or (ii).

RECOMMENDATION B.10.1

Schedule 1, clauses 7, 8 and 9 should be amended to clarify the provisions governing what was an interference with privacy under the 1993 Act, that were in force at the time of the alleged interference continue to apply.

RECOMMENDATION B.10.2

Schedule 1, clause 7 should be amended to include a savings provision that provides "Any decision made, or thing done, by the Commissioner under the Privacy Act 1993 in relation to a complaint that has not been resolved or otherwise dealt with by the Commissioner must be treated as if it had been made or done under this Act."

RECOMMENDATION B.10.3

Schedule 1, clause 11 should be amended to include a savings provision that provides "Any decision made, or thing done, under the Privacy Act 1993 in relation to a pending information sharing agreement or under the Privacy Regulations 1993 in relation to an approved information sharing agreement must be treated as if it had been done under this Act."

RECOMMENDATION B.10.4

Schedule 1, clauses 13 and 14 should be deleted.

Glossary

Terms used in the submission have the following meanings:

APEC	Asia Pacific Economic Cooperation. Significant privacy initiatives include the APEC Privacy Framework 2005 (reissued in 2015) and the APEC Cross Border Privacy Rules system (CBPRs) in 2011
EU adequacy	The process for formally recognising the laws of a non-EU state provide an adequate level of data protection to meet the EU border transfer requirements, New Zealand being formally recognised by the European Commission in 2012
GDPR	The EU General Data Protection Regulation that came into force on 25 May 2018 (replacing the Data Protection Directive 19950
Government response	Government response to the Law Commission report on Review of the Privacy Act 1993 (initial response 2011, supplementary response 2014); Cabinet Social Policy Committee: Reforming the Privacy Act 1993 (May 2014)
ICO	Information Commissioner's Office (the United Kingdom's data protection authority)
IPP	Information privacy principle (12 IPPs are set out in clause 19 of the Bill)
Necessary and Desirable	The Privacy Commissioner's 1998 first periodic review of the Privacy Act 1993, with four supplementary reports in 2000, January and December 2003, and 2008
NZLC R123	Law Commission Review of the Privacy Act Review of the Law of Privacy Stage 4 (NZLC R123, 2010)
OECD	Organisation for Economic Cooperation and Development. Significant privacy initiatives include the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data in 1980 (revised in 2013) and the OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy (2007). The Privacy Bill (clause 3) gives effect to the OECD guidelines (as set out in Schedule 9).
OPC	Office of the Privacy Commissioner (NZ)
PRPP	Public register privacy principle (4 PRPPs are set out in clause 30 of the Bill)
Section 26 report	The Privacy Commissioner's report to the Minister of Justice under section 26 of the Privacy Act 1993 (December 2016, tabled February 2017).

PART A – FURTHER REFORMS ARE NEEDED IN THE PRIVACY BILL

Introduction

1.1 In this part of my submission I recommend further amendments be made to the Privacy Bill, to ensure it meets the objective of providing a robust and comprehensive system of privacy regulation in New Zealand for the modern era, and takes account of international best practice.[3]

1.2 The Privacy Bill is not sufficiently comprehensive and there are apparent gaps and weaknesses in the Bill's enforcement framework that need to be addressed if the reforms are to be effective. A number of key developments have not yet been addressed in the Bill and are becoming increasingly urgent.

1.3 The intent of the Bill is to modernise and update New Zealand's privacy law. A lot has changed in the 7 years since the Law Commission issued its final report on the Privacy Act 1993. Important developments since 2011 that affect the operation and adequacy of privacy legislation include developments in data science and information technology, and new business models built on data-driven enterprise.

1.4 Important additional reforms need to be included in the Bill to ensure that the new legislation is fit for purpose in the dynamic data-rich world that New Zealanders embrace.

1.5 The make-up of the Privacy Bill's reforms was shaped by decisions of the former Cabinet in 2014. According to the Cabinet paper at that time, the package of reforms for New Zealand was considered to be consistent with international trends.[4] The proposals were to help ensure that New Zealand retained its EU adequacy status, a major advantage for New Zealand business.[5] This took into account the 2013 update of the OECD guidelines that form the basis of our Privacy Act.[6]

1.6 However since that time, other key international instruments on information privacy have been reviewed or reformed, including, most relevantly for New Zealand, those of APEC (2016) and the European Union (2018).[7] Privacy laws around the world have been reformed or are currently being reviewed and updated. The most influential of these is the EU General Data Protection Regulation (GDPR) that affects European nations and many of our key trading partners. It sets standards internationally in response to the challenges to consumers and data protection in today's digital economy.

1.7 In light of these significant developments, I recommend that the Committee promote amendments to the Bill. I make three specific recommendations to enhance the

[3] Privacy Commissioner, Briefing to the Incoming Minister of Justice (October 2017) https://privacy.org.nz/assets/Uploads/Briefing-for-Incoming-Minister-October-2017.pdf
[4] Cabinet Social Policy Committee paper *Reforming the Privacy Act 1993* (May 2014) at [38].
[5] For an overview, see OPC's 27 January 2017 blog on New Zealand's EU adequacy status https://privacy.org.nz/blog/providing-an-adequate-level-of-data-protection/
[6] Privacy Act 1993, long title.
[7] In May 2018, the new EU General Data Protection Regulation (GDPR) came into force and modernisation of the Council of Europe Data Protection Convention 108 was completed.

effectiveness of the framework contained in the Bill. These recommendations are in relation to:

a) Civil penalties – empowering the Privacy Commissioner to apply to the courts for a civil penalty to be imposed in cases of serious privacy breaches;

b) Enhancing agency accountability for compliance – requiring agencies to report, on request, on the steps they have taken or propose to take to ensure compliance with their privacy obligations;

c) Role of the Director of Human Rights Proceedings – implementing a Law Commission recommendation to remove the role of the Director of Human Rights Proceedings in privacy cases.[8]

1.8 These recommendations are outlined below and are accompanied by background papers attached in Appendix A (civil penalties), Appendix B (reporting on steps to compliance) and Appendix C (the role of the Director of Human Rights Proceedings).

1.9 In addition, I identify four issues of increasing importance to modern privacy frameworks and recommend the Bill be amended to address them:

a) Re-identification - strengthening protections for individuals from the privacy risks of de-identification (when personal information is used for statistical and research purposes), and providing safeguards against the risk that individuals can be unexpectedly identified from data that had been purportedly anonymised;

b) A right to personal information portability – bolstering the right of individuals to access their own personal information by including "data portability" as a right for consumers to transfer their personal information to another service provider;

c) A right to erasure (a form of the right to be forgotten) – enhancing the right of individuals to correct their personal information (IPP 7) and providing protection against the use of personal information that is out of date, inaccurate or misleading (IPP 8) by including a right to erasure; and

d) Algorithmic transparency and automated decision-making – supporting the current rights of the individual under the IPPs to the fair use of their personal information, and enhancing the transparency of decision-making affecting the individual by including a new privacy principle and new provisions as necessary to address risks to personal privacy from the use of algorithms to make decisions about individuals.

2. Civil penalties

2.1 The Bill provides an opportunity to update the design of the regulatory framework and enhance the range of available sanctions. The Bill currently lacks suitable sanctions for serious non-compliance. I recommend that the Bill should include a provision to seek the imposition of a civil penalty by the court in circumstances where there is either a serious or repeated breach of the Privacy Act.

[8] NZLC R123, R55.

2.2 The principles of responsive regulation make clear that compliance is most likely to be achieved where a regulatory regime is enforced by way of a hierarchy (or pyramid) of interventions. Internationally it is recognised that privacy and data protection regulators require a variety of potential sanctions, including the power to seek civil penalties, to be able to effectively respond to serious, persistent or egregious breaches and non-compliance with privacy law.

2.3 While the Bill includes specific criminal offences, these are limited to particular instances of non-compliance, and do not provide a power to enforce serious breaches of privacy. Criminal offences are a blunt tool that can prove resource intensive to prosecute, do not apply to public sector agencies and can be of limited practical use against large corporates, due to the complexity of criminal process rules. The maximum fine is relatively low.

2.4 Civil penalties, in comparison, offer a discretionary and flexible tool and they can be used to respond to a significant breach or non-compliance that puts personal information at risk. Civil penalties provide a means to punish serious breaches, including repeat offending. They act as an incentive to encourage agencies to cooperate and to mitigate the risk of harm. This aligns with the regulatory approach operated by the Privacy Commissioner in his complaints jurisdiction that emphasises agency engagement and negotiated resolution.

2.5 It also aligns with consumer protection regulation. Civil penalties are commonly used both by other New Zealand regulatory and consumer protection agencies such as the Commerce Commission, the Department of Internal Affairs and Inland Revenue, and internationally by a range of privacy and data protection agencies including the Australian and UK Information Commissioners and supervisory authorities subject to the EU General Data Protection Regulation.

2.6 The Commissioner suggests a penalty provision along the following lines:[9]

Pecuniary penalty for serious or repeated breaches

(1) On the application of the Privacy Commissioner, the court may order an agency to pay a pecuniary penalty to the Crown, or any other person specified by this court, if the court is satisfied that the agency has:

(a) done an act, or failed to do any act, or engaged in a practice, that is a serious breach of the Act or a code of practice; or

(b) repeatedly done an act, or failed to do any act, or engaged in a practice, that is a serious breach of the Act or a code of practice.

(2) Subject to the limits in subsections (3) and (4), the pecuniary penalty that the court orders the agency to pay must be an amount which the court considers appropriate taking into account all relevant circumstances, including -

(a) The nature and extent of the breach;

(b) The nature and extent of any loss or damage suffered that has been or may be caused by the breach;

[9] Modelled on the Unsolicited Electronic Messages Act 2007, s 45.

(c) The circumstances in which the breach took place;

(d) Whether the agency has previously been found by the Privacy Commissioner or the Human Rights Review Tribunal or the court to have engaged in any similar conduct.

(3) If the agency is an individual, the court may order the agency to pay a pecuniary penalty not exceeding $100,000 in respect of the breach that is the subject of the Commissioner's application.

(4) If the agency is not an individual the court may order the agency to pay a pecuniary penalty not exceeding $1 million in respect of the breach that is the subject of the Commissioner's application.

2.7 My Office would produce enforcement guidance and the factors that may be considered in applying to the court for imposition of a penalty, as is the practice for other regulatory agencies with civil penalty powers.[10]

2.8 Other clauses will be required to support this provision. I am available to provide supporting advice to the Ministry of Justice and Parliamentary Counsel Office in drafting these provisions.

2.9 A background paper on the recommended reform is attached in **Appendix A**.

RECOMMENDATION A.1

A civil penalty provision and ancillary provisions should be included in the Privacy Bill.

3. Enhancing agency accountability for compliance

3.1 The extent to which the Commissioner can proactively identify and address systemic compliance issues in the absence of a specific breach or incident is not clearly expressed in the Bill. The Commissioner recommends that the Bill should make provision for agencies to report to the Privacy Commissioner on request, at any time, on steps taken by the agency or proposed to be taken to ensure its compliance with the privacy legislation.

3.2 While the Bill signals a change from a primarily complaints-based or reactive system of oversight, to a system that facilitates proactive oversight of privacy risk, the Commissioner's ability to influence an agency's practices may be targeted primarily to cases where a specific breach has occurred or a complaint investigated. This may affect the extent to which systemic issues can be effectively addressed before breaches become apparent or complaints emerge.

3.3 The Bill's new compliance notice power will enable the Commissioner to respond more effectively to identified issues of non-compliance, but this proposed amendment will improve the Commissioner's effectiveness in responding to emerging systemic issues. It

[10] See for example, Commerce Commission *Enforcement Response Guidelines* (October 2013); Office of the Australian Information Commissioner *Guide to regulatory action* (updated May 2018).

will improve proactive compliance without unduly increasing agency compliance costs, aligns with international best practice, and reflects the revised 2013 OECD principles. This new power would also enhance public trust and confidence in effective regulation and the Privacy Commissioner's role to uphold individual privacy rights.

3.4 The additional provision is within the scope of the key reform in the Bill of strengthening the Commissioner's information-gathering powers, and is necessary to support the stated overall goal of the reforms in ensuring New Zealand has a privacy regime more focused on early intervention and prevention of risks, rather than ex-post remedies. It would facilitate a relatively low-level enforcement response which is intended to educate agencies and encourage them to establish and maintain their privacy management practices. This approach would be a suitable intervention prior to escalating to a more formal regulatory step as necessary.

3.5 Amending clause 201 to provide for this demonstration of compliance is the most straight-forward way of achieving this provision. The Commissioner suggests adding two short sub-clauses to clause 201:

201 ~~Privacy officers~~ Agency accountability for ongoing compliance

(1) *An agency must appoint as privacy officers for the agency 1 or more individuals whose responsibilities include –*

2.1 *The encouragement of compliance, by the agency, with the IPPs:*

2.2 *Dealing with requests made to the agency under this Act:*

2.3 *Working with the Commissioner in relation to investigations conducted under **Part 5** in relation to the agency:*

2.4 *Ensuring compliance by the agency with the provisions of this Act.*

(2) *Each agency shall take such other steps as are, in the circumstances, reasonable to ensure its on-going compliance with the Act.*

(3) *The Commissioner may, at any time, require an agency to report to the Commissioner in writing, as the Commissioner may reasonably require, on the steps the agency has taken or proposes to take to ensure its ongoing compliance with the Act.*

3.6 The proposed amendment would strengthen this provision, which requires agencies to appoint a Privacy Officer, to include an obligation on agencies to take other reasonable steps to ensure compliance, and respond to any reasonable request from the Commissioner about the agency's established or proposed compliance measures. The provision would be supported by a published Commissioner policy on regulatory enforcement responses

3.7 A background paper on the recommended reform is attached in **Appendix B**.

RECOMMENDATION A.2

Clause 201 of the Privacy Bill should be amended to enhance agency accountability for compliance by requiring agencies to report on request on the steps taken or to be taken to ensure their compliance.

4. Director of Human Rights Proceedings

4.1 In its review of the Privacy Act 1993 the Law Commission recommended:[11]

> *The role of the Director of Human Rights Proceedings should be removed in privacy cases. The Privacy Commissioner should decide which cases are to proceed to the Human Rights Review Tribunal and act as the plaintiff in those cases, and perform the other roles currently performed by the Director.*

4.2 The previous Government did not accept this recommendation and it has not been implemented in the Bill. The Bill carries over the current model in the Privacy Act 1993 that splits functions between the Privacy Commissioner and the Director of Human Rights Proceedings in relation to privacy complaints. If the Privacy Commissioner considers proceedings should be brought in the Tribunal (because it raises important issues) the complaint is referred to the Director of Human Rights Proceedings for his or her consideration. The Director considers the matter afresh and acts as the plaintiff.

4.3 I recommend that the Law Commission's recommendation should be implemented in the Bill. In summary, I agree with the Law Commission's view that the current model is "duplicative and inefficient".[12] Reform in this area would reduce unnecessary compliance costs for complainants and other parties when they access the Tribunal, and enhance individual privacy by promoting more effective resolution of complaints.

4.4 Duplication of processes will be reduced by removing the Director's role and allowing the Commissioner to take proceedings directly.

4.5 In addition to duplication, the split model is inefficient given the relative expertise of the two offices. Privacy represents a minority of the Director's workload compared to human rights issues, while the Commissioner and his Office are privacy specialists.

4.6 It is also anomalous for the Commissioner not to have control over how the proceedings are argued yet to be liable for the costs.[13]

4.7 The previous government rejected the Law Commission's recommendation based on concerns about the independence of the Commissioner's conciliation function, and litigation resourcing within the Office of the Privacy Commissioner. The Law Commission found concerns about the conciliation function were "outweighed by the speedier and more efficient arrangement which would result".[14]

4.8 Further, my being able to bring proceedings directly in the Tribunal would complement other reforms in the Bill that provide more efficient and effective enforcement powers, including binding access directions[15] and compliance notices.[16] My Office will be required

[11] NZLC R123, R55.
[12] NZLC R123 at [6.33].
[13] Privacy Bill, cl 115(2).
[14] NZLC R123 at [6.38].
[15] Privacy Bill, Part 5, cl 96.
[16] Privacy Bill, Part 6(2).

to have the litigation capability to enforce and defend compliance notices in addition to the current requirements.

4.9 The change would be fiscally neutral as any adjustments to the Director's or OPC's funding would balance each other out.

4.10 The Privacy Act 1993 is now 25 years old and is being modernised in this Bill. The Director's role may have seemed appropriate when the current Act was introduced but it is no longer necessary or appropriate. It is timely for the Law Commission's recommendation to be implemented and the role of Director to now be removed.

4.11 The Law Commission's recommendation could be implemented by:

a) amending clauses in the Bill that currently provide for the Commissioner to refer complaints to the Director,[17] and instead providing the Commissioner with discretion to consider whether proceedings should be instituted;

b) amending clause 102 of the Bill to provide the Commissioner with discretion to commence proceedings in the Tribunal; and

c) substituting further references to the Director for references to the Commissioner under various clauses.[18]

RECOMMENDATION A.3

Law Commission recommendation 55 should be implemented in the Privacy Bill to discontinue the role of the Director of Human Rights Proceedings in privacy cases.

5. Re-identification

5.1 Increasingly datasets are being released to further the objectives of the open government agenda, recognising that data as a public asset should be made publicly available. Datasets provide a trove of information and insights that inform new and improved products, processes, and applications. The potential for doing so without compromising privacy is achieved by anonymising datasets of personal information about individuals before they are interrogated for research purposes.

5.2 The Bill carries over provisions from the Privacy Act 1993 that allow for the publication and use of personal information in a form in which the information is anonymised.[19] I support the continued application of these exceptions to the use and disclosure principles. These provisions serve an important public interest in allowing the statistical use of personal information for research purposes. They provide one of the statutory underpinnings of the open government data programme that allows government-held data

[17] Privacy Bill, clauses 84, 87, 96, 98 and 99.
[18] Privacy Bill, clauses 94, 95, 103, 104, 108, 204 and 206.
[19] Privacy Bill, IPPs 10(1)(b) and 11(1)(h).

to be made increasingly available for public benefit, including private sector initiatives that utilise anonymised data to create new services.

5.3 I am mindful however that to provide greater access to personal information, datasets containing personal information must be carefully and robustly de-identified before being released for downstream uses, in order to protect the privacy of the individuals concerned. Personal information can be de-identified by applying various tools and techniques.[20] Which tools are most effective will depend on the particular context, including the nature of the particular dataset and the underlying data, and the proposed uses of the dataset.

5.4 What has come to light in recent years is the risk of harm to individuals if their identities are unmasked when de-identification techniques applied to information sets are not sufficiently robust. My 2016 report to the Minister on the operation of the Privacy Act noted that there have been a number of high profile instances overseas where individuals in anonymised datasets have been re-identified, leading to a range of privacy harms and the de-railing of public and private sector initiatives.[21]

5.5 Re-identification is the process by which anonymised personal information is linked back to the individuals the information relates to, and destroys the cloak of anonymity that protects individuals' privacy in that information. The risk of re-identification rises if the de-identification process is inadequate. Re-identification can be a deliberate act such as interrogating datasets for weak anonymisation to reveal individual identities, or it can be inadvertent, such as data research that uncovers vulnerabilities in de-identification techniques. It can also arise from combining different datasets to discover correlations between them.

5.6 A recent Australian example is the Medicare Benefits Scheme data released for public access and analysis that contained ostensibly de-identified information about services, the location of service provision and the encrypted healthcare provider and recipient numbers for each funded service. University of Melbourne researchers tested the robustness of the anonymisation and were able to decrypt service provider identifiers using publically available information. When the vulnerability was reported, the dataset was taken down, and an Australian Information Commissioner investigation found that the Department of Health had unintentionally breached the Australian privacy principles in preparing the dataset for publication.[22]

5.7 In my 2016 report to the former Minister I suggested that a new privacy principle be considered to protect against the risk of re-identification, as well as clarifying agencies'

[20] For example, removing unique identifiers, aggregating information into ranges, swapping identifying information between individuals to maintain the integrity of the information as a whole, but removing the ability to identify a particular person, generating synthetic data with similar patterns to the original dataset but without any identifying features, and suppressing data that would otherwise allow individuals to be identified.
[21] Section 26 report - six examples were set out in an appendix to the report, outlining high profile re-identification events in the United States, the United Kingdom and Australia between 1997 and 2016.
[22] https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/publication-of-mbs-pbs-data The Australian Government has since published guidance on releasing datasets of sensitive information: *Process for Publishing Sensitive Unit Record Level Public Data as Open Data*

Privacy Act obligations when anonymising and de-identifying personal information, when they rely on current exceptions.[23] Given the seriousness of this issue for maintaining the privacy of individuals, I maintain my support for new measures in the Bill to strengthen agency responsibilities in relation to effective de-identification, and to address re-identification in circumstances where it would give rise to serious privacy harms.

5.8 There are a range of approaches from other jurisdictions that provide models to inform how the issue could be addressed in the New Zealand Privacy Bill. In the United States, the Health Insurance Portability and Accountability Act (HIPAA) treats data as anonymised if 18 specific data elements are removed. The EU GDPR allows for personal data to be used for scientific, historical or statistical purposes (that would otherwise be limited) provided that "appropriate safeguards" are implemented.[24] The GDPR explicitly provides that "pseudonymisation" of the dataset (techniques to replace personal identifiers) is a safeguard that can help an agency meet this requirement, unless re-identification techniques are reasonably likely to be used, such as singling out the individual either directly or indirectly.

5.9 In the United Kingdom, the Data Protection Bill includes a new offence for intentionally re-identifying individuals from data that should have protected their identities.[25] In Australia, the Privacy Amendment (Re-identification Offence) Bill 2016 has been introduced following the Medicare Benefits Scheme re-identification event noted above.[26] The proposed new offences would prohibit intentional re-identification of Commonwealth Government data and the intentional disclosure of re-identified personal information, as well as ancillary offences, and impose notification obligations when re-identification occurs. There has been debate in Australia about whether the proposed offences in that Bill are necessary and proportionate.

5.10 I recommend that the Privacy Bill strengthen protections for individuals from the risks of inadequate de-identification of personal information for statistical and research purposes, and provide safeguards from the risks of re-identification. There is an important public interest in having the appropriate regulatory settings in place, including in the Privacy Act, to ensure that the significant advantages of anonymised data for government and business can be maximised. This issue is relevant to New Zealand's open data strategy, and further consideration could be given to the issue in that context. [27] However there is an opportunity to strengthen the Privacy Bill, before New Zealand suffers its own high profile re-identification event that leaves individuals exposed to harmful effects.

[23] Section 26 report, recommendation 2.
[24] GDPR, article 89.
[25] Clauses 167, 168.
[26] https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1047
[27] The Data Futures Partnership has carried out some preliminary work on the topic, and the Government's Chief Science Adviser has noted the issue in a June 2017 discussion paper on using evidence to inform social policy: http://www.pmcsa.org.nz/wp-content/uploads/17-06-19-Citizen-based-analytics.pdf . See also the July 2017 report http://www.pmcsa.org.nz/wp-content/uploads/17-07-07-Enhancing-evidence-informed-policy-making.pdf

RECOMMENDATION A.4

The Privacy Bill should (a) strengthen protections for individuals from the privacy risks of inadequate de-identification of personal information for statistical and research purposes; and (b) provide safeguards against the privacy risks resulting from re-identification events.

6. Proposed right to personal information portability

6.1 In my 2016 report to the former Minister I recommended, and repeat that recommendation here, that New Zealand's privacy law ought to include a right to personal information portability to strengthen individuals' control over their personal information in the digital economy.[28]

6.2 Such a right is not without precedent. The right to data portability (as it is known in Europe) is already to be found as a consumer entitlement for over 500 million residents of the European Union in the new EU GDPR (article 20). For 25 years, New Zealand has had a portability right for health information that was enacted in conjunction with the Privacy Act in 1993 (see s 22F of the Health Act) and which is enforced through complaint to the Privacy Commissioner.

6.3 Laws and regulatory schemes mandating portability rights have been found to be useful spurs to competition in various contexts such as banking, telecommunications and utilities where industry can make it difficult for consumers to switch providers.[29] The Australian Productivity Commission last year recommended that to build community trust and acceptance for information sharing, Australian consumers should have comprehensive new data rights which would include a portability right to "direct data holders to transfer data in machine-readable form, either to the individual or to a nominated third party."[30]

6.4 A portability right will allow individuals to request an agency to provide them their personal information in a suitable electronic format or to require the agency to transfer the information in electronic format directly to another agency. This will reduce the current friction in transferring services to another provider and have a range of benefits including:

a) helping to ensure existing access and use principles remain meaningful in a pervasive digital environment;
b) strengthening consumer choice in relation to information service providers in the digital environment and preventing provider lock-in;

c) ensuring NZ businesses meet rising consumer expectations internationally and legal requirements when trading in the EU and benefit from competition enabled by portability; and

[28] Section 26 report, recommendation 1.
[29] For example, the Electricity Authority's "What's my Number" initiative or the local and mobile number portability requirements under the Telecommunications Act 2001.
[30] Australian Productivity Commission Inquiry Report, *Data Availability and Use*, March 2017, recommendation 5.1.

d) preserving NZ's status, and comparative trading advantage, as a country recognised as providing a high level of data protection, including in the face of any post-GDPR review of NZ's formal 'adequacy' status;

e) ensuring NZ consumers can benefit from any service innovations arising from European businesses implementing the new data portability right in that region.

6.5 In a 2016 survey of public attitudes on behalf of the Office of the Privacy Commissioner, in response to a question about how important people considered portability of their personal information, UMR Research found a majority of the public consider the ability to transfer personal information between social network or cloud services as important.[31]

6.6 By way of example, the portability right might, where feasible, enable individuals to take their transaction histories with them or have their information transferred when they switch to a new social media service provider. The right would also be relevant in relation to online cloud services that provide storage and access to personal information such as digital photo albums whereby individuals could request a transfer of their pictures to a new provider. Where a service provider does not offer portability of information, the individual's choice is to remain locked into a service they don't want or that doesn't meet their needs or, to lose access to cherished digital memories. Where services are being used in a professional capacity, the lock-in problem can also have an impact on a person's livelihood.

6.7 The proposed right would broadly correspond to the new 'Right to Data Portability' in GDPR, article 20. The GDPR entitles the individuals concerned to receive the personal information that they have provided to an online business in a 'structured, commonly used, machine-readable and interoperable format', and to transmit the information to a competing business. Where technically feasible, the individual concerned will also have the right to insist that the first business transmit the personal information directly to the other business.

6.8 Consumer lock-in is a problem for privacy, autonomy and individual control. The ability for an individual to be able to exercise choice over who holds and uses their information is central. The proposed new portability right is an appropriate legislative measure to ensure that existing individual privacy rights regarding access and control of use of personal information remain meaningful in a pervasive digital environment. The long established and fundamental individual right of access to one's own information diminishes in usefulness in today's environment if the information obtained is not provided in a reusable digital format or if businesses hinder the efforts of individuals to make further electronic use of the information.

6.9 The issue can also be seen as a competition problem. The new right proposed will go beyond simply strengthening existing privacy rights in a digital environment. It will also empower consumers to make choices allowing market forces to respond. Individuals

[31] OPC, Privacy Survey 2016, Part E https://privacy.org.nz/news-and-publications/surveys/privacy-survey-2016/

should be able to switch services, especially in a world where service providers may change business models and privacy policies or discontinue products.

6.10 The drafting and scope of a New Zealand right may appropriately differ from portability laws in the European Union and Australia. However, the objective would be to produce a right that is interoperable with other privacy frameworks. In the case of EU provisions, for example, a New Zealand agency meeting the requirements of the proposed right should thereby be confident of meeting the GDPR requirements in the event that it was to trade into the EU. Similarly, European consumers should be able to confidently switch their information to or from a New Zealand provider just as New Zealand consumers might benefit from the new GDPR right in dealing with an EU-based business.

RECOMMENDATION A.5

The Privacy Bill should include a right to personal information portability.

7. The Right to Erasure

7.1 The Privacy Commissioner proposes that the Bill include a new information privacy principle to provide individuals with a right to erasure of personal information. The proposal will ensure that the Bill reflects new standards for the erasure of personal information, also known as the 'right to be forgotten'.

7.2 Such a right to be forgotten gained prominence following a 2014 Court of Justice of the European Union ruling[32] requiring Google to remove some specific search engine results that included personal information about the bankruptcy of Mr Gonzales, a Spanish citizen. Following the decision Google was obliged to delink certain search engine results as requested by Mr Gonzales.

7.3 New Zealand legislation already provides for limited rights to erasure of personal information. For example, IPP 7 of the Privacy Act entitles individuals to request the correction of their personal information (the definition of "correct" including deletion), and IPP 9 requires agencies to not keep personal information for longer than is required for the purposes for which the information may lawfully be used. The Harmful Digital Communications Act 2015 also provides for court orders to be issued to an online content host to take down or disable public access to harmful material. These measures do not however go far enough.

7.4 The technological improvements of the past 25 years are creating an urgent need for a right to erasure of personal information. The dramatic changes over this time period include the growth of the internet, telecommunications and mobile computing, social networking and internet search engines.

[32] *Google Spain and Google Inc v Agencia Espanol de Proteccion de Datos (AEP) and M C Gonzalez* 13 May 2014 available at http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d50cc57fb6d9ae4925aff5d9bbd76b8b00.e34KaxiLc3eQc40LaxqMbN4Ob3uSe0?text=&docid=152065&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=102488

7.5 Vast amounts of personal information have been and are continuing to be digitised and this information can be readily distributed and searched by anyone. This can include unlawfully obtained personal information (by hacking or other means) including sensitive information, offensive material such as revenge porn and numerous other types of personal information about an individual that in the passage of time they have a legitimate reason for it remaining private. For example an online search may reveal information about an individual's historic criminal convictions that is covered by the Criminal Records (Clean Slate) Act 2004 and which the individual has a right under that Act not to reveal. The inability to have that online index erased undermines individuals' rights and the policy of the Act.

7.6 The power of search engines to find information (including historical personal information) is a fundamental shift that requires addressing. The fall in search costs means an issue that historically would be forgotten can now stay with an individual for their entire life. When Mr Gonzales had his home repossessed in 1998 he was one of the first to experience the power of search engines to keep his past alive.

7.7 Emerging technologies such as advanced algorithms and artificial intelligence require vast amounts of personal information and shape the prospects of individuals. Expanding existing rights to include a right to erase personal information will provide individuals with some measure of personal control over the algorithms and automated decision making they are subject to.

7.8 In response to these same factors, the European Union and United Kingdom are expanding their rights to erasure.

The European Union right to erasure of personal information

7.9 Article 17 of the GDPR builds on the European right to be forgotten by including the right for individuals to request that personal data be erased without undue delay by a data controller (equivalent to an 'agency' in the Privacy Bill). The right forms part of the matrix of other obligations agencies have when they collect, use and delete personal data. The right is not absolute and only applies in certain circumstances.

7.10 The GDPR gives individuals the right to request their personal data be erased if:

a) the personal data is no longer necessary for the purpose which it was originally collected or processed;
b) the agency is relying on consent as the lawful basis for holding the data, and the individual withdraws their consent;
c) the individual objects to the processing of their data, and there is no overriding legitimate interest to continue processing it;
d) the agency has processed the personal data unlawfully;
e) the agency has a legal obligation to erase the data (for example an obligation arising from another Member State); or
f) the agency has processed the personal data to offer information society services to a child.

7.11 Where personal data has been made public in an online environment, reasonable steps must be taken to inform other controllers who are processing the personal data to erase links to, copies, or replication of that data.

7.12 There are several situations where the right to erasure of personal information does not apply. These include protections for exercising the right of freedom of expression and information and complying with legal obligations. The GDPR also specifies two circumstances where the right to erasure will not apply to special category data that are related to public health and preventative or occupational medicine.

The United Kingdom right to erasure of personal information

7.13 The Data Protection Bill is currently before the United Kingdom Parliament and contains a modified version of the GDPR right to erasure of personal information. Clause 45 of the Data Protection Bill provides for a right of erasure or restriction of processing where the processing of personal data would infringe certain data privacy rights or where the controller has a legal obligation to erase the data. New provisions were added to protect the preservation of evidence and to restrict processing where accuracy is contested.

7.14 In addition, the Bill provides that where an agency has disclosed the personal data to others, it must contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked to, the agency must also inform the individuals about these recipients.

New Zealanders need expanded rights to maintain privacy in the 21st century

7.15 The current rights and protections available to New Zealanders are gradually weakening as technology develops. In particular, the requirement in principle 9 for information to be kept for no longer than is necessary is rendered meaningless in the context of advanced algorithms and artificial intelligence. For example, the thirst of artificial intelligence systems for data will mean that agencies will want to keep all of the data that is available for increasing periods of time.

7.16 There are clear situations where the protection of individual privacy will be maintained through expanding existing rights to include a right to erasure. The European and United Kingdom legislation provide useful precedents for these situations, which include when the information has been unlawfully obtained (such as through a data breach) or where an individual has withdrawn their consent.

7.17 Providing individuals with a right to erase personal information is a better approach than tightening requirements for how long agencies can keep information. The decision making onus will shift from agencies (who have an incentive to collect information) to individuals so that they can maintain their own privacy. In effect, a right to erasure of personal information will establish a balancing force against agency desires to keep increasingly large amounts of information for longer.

7.18 Providing individuals with a right to erasure will empower them to resolve issues with agencies directly. As Privacy Commissioner I will provide guidance and act on any complaints and compliance issues that arise between the parties.

7.19 I recommend a new information privacy principle "Erasure or restriction of processing of personal information" be added to the Bill.

RECOMMENDATION A.6

The Privacy Bill should include a new information privacy principle on the right to erasure of personal information.

8. Algorithmic transparency and automated decision-making

Introduction

8.1 Automated tools or systems that use personal information to make a decision or assessment are increasingly used. These may include:

a) Algorithmic or automated decision-making, i.e. tools relying on algorithms, programming or artificial intelligence (AI) to assess information and make a decision on outcomes which would formerly have been made by a human.

b) Predictive analytics, sometimes referred to in New Zealand as predictive risk modelling, i.e. a statistical tool that attempts to determine future outcomes or likelihood of risk by analysing the characteristics associated with those outcomes in historical cases.

8.2 While these tools can improve services and productivity by automating manual decision-making processes, they can also give rise to privacy and other risks such as discrimination. Algorithmic transparency means having visibility over the inputs and decision-making processes of the tool, or being able to explain the rules and calculations if challenged, and is a useful response to help ensure individual control over the use of their information and in addressing other related issues.

8.3 The Bill does not expressly address the emerging privacy issues relating to automated decision-making. Automated decision-making tools are increasingly being used by agencies, and when operated non-transparently or without opportunity for affected individuals to challenge decisions, can pose significant risks for individuals' rights and freedoms.[33] Without appropriate safeguards these practices can lead to inaccurate predictions, denial of services and discrimination.

[33] See for example the report recently issued by the UK House of Commons Science and Technology Committee: *Algorithms in decision-making*, Fourth Report of Session 2017-19, issued 15 May 2018, as to the potential issues posed by algorithms and algorithmic decision-making.

8.4 While data analytics are not new, the availability of more powerful analytical tools creates a greater capacity to analyse large datasets. These tools can provide potentially significant positive impacts on a wide range of services, but there is also potential for these tools to create significant negative outcomes. Professor Roth in his 2009 report on the operation and adequacy of the Privacy Act when assessed against European standards stated that "automated decision-making is not a common phenomenon in New Zealand in either the public or private sectors" and there are a range of legislative provisions operating to discourage this work.[34] However, almost ten years on it would be harder to be so categorical with both public and private sector agencies understood to be increasingly using algorithmic or automated decision-making tools to support their work.

8.5 In recognition of the significant risks of automated decision-making, specific safeguards have been included in Europe privacy law. I recommend new measures in the Bill to better safeguard the interests of individuals with respect to automated decision-making including obligations on agencies to provide algorithmic transparency.

Privacy risks

8.6 Data analytics and automated decision-making often lack transparency and provide no meaningful accountability. Systems may appear objective and yet be subject to in-built bias leading to discrimination. Many algorithmic assessment tools operate as 'black boxes' without transparency. This lack of transparency is compounded when private commercial interests claim trade secrecy over proprietary algorithms so that even the agencies using the tools may have little understanding over how they operate.

8.7 Transparency of operation is essential in identifying and addressing inherited bias. Algorithms can have inherited bias due to poor policy inputs or unreliable or flawed data. Failures in predictive model capacity are usually not evenly distributed; these failures can perpetuate or exacerbate poor outcomes for disadvantaged communities.

8.8 These issues erode an individual's control over the use of their information.

Addressing the privacy risks in the Bill

8.9 There is currently a gap in legislation relating to the use of algorithmic or automated decision-making and related tools. The Privacy Act 1993, the Human Rights Act 1993, the New Zealand Bill of Rights Act 1990 and the Official Information Act 1982 provide the general legal human rights framework that applies to private and State actions involving the personal information of individuals in a manner that may adversely impact on their interests and rights, but these Acts do not create any general and principled high level framework protecting individuals in relation to automated decision-making.[35]

[34] *Analysis of the Adequacy of Protection of Personal Data Provided in New Zealand*, Final Report, Dr Paul Roth (2 June 2009) p 126.

[35] The above mentioned laws address some aspects of automated decision-making in an ad hoc way in relation to, for example, rights of access to internal rules affecting decisions and to reasons for decisions in the state sector (Official Information Act, ss 22 and 23); rights of challenge in relation to data matching (Privacy Act , s 103); and obligations on agencies to justify discriminatory decisions in the insurance and

8.10 The IPPs can apply to the collection and use of personal information in this context. The principles "generally function as a restraint on automated individual decisions."[36] Professor Roth notes that there is "a disincentive for automated decision-making built into the Privacy Act as any agency that breached an IPP and caused harm or loss to an individual as a result of an automated decision incurs liability under the Act."[37] However, the principles do not directly – or arguably very effectively – address the particular risks and issues created by automated decision-making processes. Nor do they require specific mitigations such as algorithmic transparency.

8.11 Part 10 of the current Privacy Act, relating to information matching, is the most comprehensive example of controls over automated decision-making. Professor Roth calls the systemic controls on data matching as "particularly relevant to the regulation of automated decision-making."[38] The statutory information matching rules provide the regulator with some oversight of the matching algorithms being used.[39] The Act also creates a process whereby the individuals concerned are told of any discrepancy produced by an automated match and given a chance to explain themselves and to challenge an adverse decision proposed to be taken as a result.[40] However, it is notable that the information matching controls do not extend to private sector activities. Further, the Bill proposes to sun-set the information matching provisions in relation to public sector activities.[41]

European laws: EU General Data Protection Regulation and Council of Europe Convention

8.12 The EU GDPR regulates automated decision-making and profiling by imposing certain restrictions and creating rights to challenge certain processes or require them to be justified to the individuals concerned. The GDPR rights and obligations are subject to certain exceptions and may in some cases be further affected by domestic law in Member States. Generally speaking, the GDPR requires agencies to provide meaningful information about the logic involved in their decision-making process, as well as the significance and envisaged consequences for the individual, obliges agencies to take steps to prevent errors, bias, and discrimination, and gives individuals rights to challenge and request a review of the decision.

8.13 Automated decision-making can, but does not always, include profiling. The GDPR's definition of 'profiling' is:

> *"the automated processing of personal data consisting of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict*

---

superannuation fields by reference to actuarial data (Human Rights Act, ss 48 and 70); a requirement on credit reporters to reveal the general methodology underpinning credit scores (Credit Reporting Privacy Code, rule 6(2A)).

[36] *Analysis of the Adequacy of Protection of Personal Data Provides in New Zealand*, above, p 125.

[37] Above.

[38] Above.

[39] Privacy Act 1993, Schedule 4.

[40] Privacy Act 1993, s 103.

[41] Privacy Bill, Schedule 8.

aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

8.14 Relevant articles of the GDPR include:

a) Article 13 includes transparency obligations for automated decision-making, including profiling. A European agency must advise the individual if it uses automated decision-making, and explain the logic, at the time an individual's information is collected.

b) Article 21 provides directly affected individuals with a right to object to certain automated decision-making (including profiling). This includes a right to object where the processing is in the public interest by a public body. The processing must stop unless the controller can demonstrate compelling legitimate grounds which override the individual's interests.

c) Article 22 is a more general right for individuals not to be subject to automated decision-making (including profiling), unless authorised by law (provided suitable safeguards apply), or subject to certain exceptions, including the individual's consent. There are safeguards for special categories of sensitive information, that generally cannot be used, and a right to seek human intervention in the decision, and to contest it.[42]

8.15 As this type of processing is considered to be high-risk, the GDPR requires agencies using automated decision-making to carry out a Data Protection Impact Assessment (known in New Zealand as a Privacy Impact Assessment or PIA) to show they have identified and assessed the risks involved and how they will be addressed.

8.16 The modernised Council of Europe Data Protection Convention has new provisions that have similar effect to a number of the GDPR provisions, including:[43]

a) The right for individuals not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration.[44]

b) The right to obtain, on request, knowledge of the reasoning underlying data processing.[45]

c) The right to object at any time, to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms.[46]

[42] The GDPR specifies the 'special categories' in article 9.
[43] The Council of Europe Data Protection Convention 108 was adopted in 1981 but finally modernised in May 2018.
[44] Modernised Convention, article 9(1)(b).
[45] Modernised Convention, article 9(1)(c).
[46] Modernised Convention, article 9(1)(d).

Recommendations for addressing automated decision-making

8.17 I recommend new measures be included in the Bill to ensure algorithmic transparency and the rights of individuals to safeguard their interests when automated decision-making is applied to them. I recommend including a new privacy principle setting the high level expectations of fair practice.

8.18 The Bill must respond to the exponential growth of personal data in the digital age over the 25 years since the 1993 Act was enacted. The precise form that such reforms should take is a matter of debate but whatever course is taken agencies should not be able to hide behind machines when decisions are taken affecting individual New Zealanders: people programme the algorithms and people must take responsibility for the decisions that result from them. Transparency, proper justification, accountability and the ability of individual challenge in appropriate cases would seem likely to be part of the appropriate regulatory mix.

RECOMMENDATION A.7

Additional provisions, including a new privacy principle, should be included in the Privacy Bill to limit the harms arising from automated decision-making and to require algorithmic transparency in appropriate cases.

PART B – PART BY PART RECOMMENDATIONS

Introduction and background

1. The Privacy Bill modernises and updates the 1993 Privacy Act and makes a number of technical changes. In Part B of my submission I recommend implementing certain Law Commission recommendations that have not yet been included in the Bill. I also recommend amendments to improve the implementation of proposed reforms, and amendments to Bill provisions to carry over the effect of current provisions in the Privacy Act 1993. I make a number of drafting suggestions to do so, including in particular in Part 4 of the Bill.

2. The Privacy Bill retains and carries over the core features of the Privacy Act 1993, including:

    a) the 12 information privacy principles (the IPPs);[47]

    b) the Privacy Commissioner's complaints system;[48]

    c) the Commissioner's own motion investigation powers;[49]

    d) the rights of individuals to bring proceedings in the Human Rights Review Tribunal following investigation of their complaint by the Privacy Commissioner.[50]

3. Some of the Law Commission's recommendations have previously been implemented in the Privacy Act and are continued in the Bill, including:

    a) Part 9A[51] added to the Privacy Act in 2013, implementing the Law Commission's recommendations on information sharing;[52]

    b) The definition of "serious threat" was also added in 2013 to provide criteria for assessing the seriousness of a threat to health or safety in order to provide an exception to the use and disclosure principles;[53]

    c) Amendments made in 2015 to qualify the domestic affairs exemption in section 56 so that actions relating to personal information are no longer exempt if reasonably considered "highly offensive";[54]

[47] Privacy Bill, clause 19.
[48] Privacy Bill, Part 5(1)-(2).
[49] Privacy Bill, Part 5(1(-(2).
[50] Privacy Bill, Part 5(3).
[51] Privacy Bill, Part 7(1).
[52] Law Commission, ministerial briefing on Information Sharing (29 March 2011), NZLC R123, Appendix 1.
[53] NZLC R123, R31.
[54] NZLC R123, R45, partially implemented by the Harmful Digital Communications Act 2015. The Privacy Bill implements other aspects of this recommendation in clause 24.

d) Amendments made in 2017 to apply most of the IPPs to the intelligence and security agencies and to amend the exemption in section 57 of the Privacy Act.[55]

4. The Privacy Bill now implements the Law Commission's other significant law reform recommendations including:

a) Mandatory breach notification - the introduction of mandatory reporting of privacy breaches to bring New Zealand into line with international best practice (subpart 6(1));[56]

b) Compliance notices - empowering the Privacy Commissioner to use a compliance notice in the event of a breach of the Act (subpart 6(2));

c) Access determinations - empowering the Privacy Commissioner to issue a determination when a person has been wrongly denied access to their personal information (Part 5); and

d) Cross border disclosure - requiring agencies to ensure there are appropriate privacy standards in place for personal information when they disclose it to someone in another country (IPP 11(3)-(6)).

5. A further change is proposed in the Bill that would curtail the use of information matching agreements beyond those already established, with the intent that new initiatives will be carried out as approved information sharing agreements.[57]

PART 1 – Preliminary Provisions

1.1 This part contains the Bill's purpose statement in subpart 1 and definitions in subpart 2.

Clause by clause comments

Title of the Act

1.2 I consider it appropriate that the new modernised Privacy Act be named both in English and te reo Maori.

RECOMMENDATION B.1.1

The new Privacy Act should be named both in English and te reo Maori.

[55] Intelligence and Security Act 2017; NZLC R123 R46. The relevant exemption is in the Privacy Bill, cl 25.
[56] OPC currently receives voluntary notification from agencies in the event of a privacy breach and provides guidance on breach responses.
[57] Privacy Bill, Sch 8.

Clause 3: Purpose

1.3 The Bill introduces a purpose clause. The Privacy Act 1993 does not have a purpose clause, and the Law Commission recommended that it should.[58]

1.4 I propose that clause 3(a) should be amended. It is not necessary in the purpose clause to recognise that other rights and interests may need to be taken into account. The recognition of other rights and interests is embedded throughout the Bill including in clause 18, the exceptions to the IPPs, the exemption clauses in Part 3(1), and the various mechanisms for information sharing, accessing and matching in Part 7.

1.5 The purpose clause should primarily affirm that the Act is to promote and protect privacy, as the long title to the Privacy Act 1993 currently affirms. This reflects the design of the legislation as rights affirming by upholding privacy rights, subject to the legislative design features that expressly allow for other interests to be taken account in the circumstances. Adding an overlay in the purpose clause, that references the need for recognition of other rights, may potentially undermine the intended interpretation of the Bill.

RECOMMENDATION B.1.2

The words "while recognising that other rights and interests may at times also need to be taken into account" should be deleted from clause 3(a).

Clause 6: Interpretation - definition of "agency" para (b)(ix): Ombudsman

1.6 An "agency" is broadly defined for purposes of the Bill,[59] and is subject to a number of exceptions in paragraph (b), including the Ombudsmen.

1.7 The Law Commission recommended removing this exception from the definition, with the intent that the Privacy Act should, as a matter of principle and for the sake of consistency, apply to the Ombudsmen.[60] Other officers of Parliament are subject to the Privacy Act and so are the courts (except in their judicial functions). Most submissions to the Law Commission on this point supported the recommendation, but the Ombudsmen opposed it. One argument made was that the Ombudsmen acts as a "last line" check on the exercise of executive power and therefore should not be subject to the oversight of the Privacy Commissioner.

1.8 The Government response to the recommendation accepted the arguments of the Ombudsman and proposed instead that the Ombudsman Act be amended to require annual reporting on the Ombudsman's handling of personal information. I have not yet been consulted on any legislative proposal to amend the Ombudsman Act to do so.

1.9 In my view, the case has not been made to exempt the Ombudsmen from the application of the Privacy Act, and there are strong and principled reasons that the

[58] NZLC R123, R3.
[59] Definition of "Agency", para (a).
[60] NZLC R123, R37.

Ombudsmen should be subject to the Privacy Act. From the citizen's perspective it is important that the system of oversight, including of our public sector and Parliamentary oversight bodies, has the necessary checks and balances. Each oversight body has a dedicated area of specialist oversight. Just as the Privacy Commissioner is subject to the Ombudsman Act, it is appropriate that the Ombudsman become subject to the Privacy Act.

1.10 Issues of workability, given the nature of the work of the Ombudsman, can be accommodated. If necessary, the Ombudsmen could be exempted from principles 6 and 7, to align with the position of the Auditor-General in clause 26 of the Bill.[61] Any such exemption should not extend to personal information about the Ombudsman's current, former and prospective staff.[62]

1.11 I recommend that the Law Commission's recommendation to remove the Ombudsmen from para (b) of the definition of an "agency" should be implemented in the Bill.

RECOMMENDATION B.1.3

Paragraph (b)(ix) of the definition of "agency" should be deleted.

Clause 6: Interpretation – definition of "court"

1.12 This definition is for the purposes of subpart 3 of Part 7. I understand it was included to ensure there was no doubt the subpart provided authority to access court records even though a court in relation to its judicial functions is not an agency for the purposes of the Bill.

1.13 In my view the inclusion of this definition is potentially confusing as well as unnecessarily complex. I recommend the simplest and most effective approach that will remove any doubt is to replace the term "holder agency" with "specified holder" in clauses 171 and 172 (no change to the substance of the definition in clause 171 is required). In addition clause 169 should be amended by replacing "specified agencies" with "specified holders". The definition of "court" in clause 6 will therefore be unnecessary and can be deleted.

RECOMMENDATION B.1.4

The definition of "court" in clause 6 should be deleted and in clauses 171 and 172 the term "holder agency" should be replaced with "specified holder" and in clause 169 the words "specified agencies" replaced with "specified holders".

[61] Cl 26(1)(c).
[62] This aligns with the scope of the Law Commission's recommendation in relation to the exemption from IPPs 6 and 7 for the Auditor-General: NZLC R123, R42.

Clause 6: Interpretation – definition of "Minister"

1.14 This clause provides the definition of "Minister" means "a Minister of the Crown in his or her official capacity." A Minister acting in his or her official capacity is subject to the Privacy Act (under the definition of "public sector agency") but a Member of Parliament acting in his or her official capacity is not (due to an exception in the definition of "agency"). There is currently no express provision in the Bill in respect of whether a Parliamentary Under-Secretary is subject to the Act.

1.15 I recommend that an amendment should be made to the definition of "Minister" in the Bill to include a Parliamentary Under-Secretary, to confirm that Under-Secretaries, acting in their official capacity are subject to the Privacy Act, consistent with the position of Ministers.[63] This would align with the clarification made to the Official Information Act 1982.[64]

RECOMMENDATION B.1.5

The definition of "Minister" should include a Parliamentary Under-Secretary.

Clause 6: Interpretation – definitions of "publicly available publication" and "statutory register"

1.16 A number of amendments have been made to definitions by the Bill. My comment relates to the definition of "publicly available publication". This term is used in IPP 10(1)(d) and IPP 11(1)(d). Currently, in the Privacy Act 1993, this includes a magazine, book, newspaper, or other publication that is or will be generally available to members of the public, and includes a public register.

1.17 I support the modernisation of the definition in the Bill, as recommended by the Law Commission.[65] The definition (para (a) will now cover a publication in printed or electronic form that is or will be available to members of the public free of charge.

1.18 However, para (b) of the definition is an expansion to include all statutory registers. This goes beyond the intent of the Law Commission recommendation. Paragraph (b) of the definition should be reserved for public registers.

1.19 The Law Commission carried out a comprehensive survey of statutory registers in 2008.[66] These registers are subject to varying degrees of availability to the public, from open by default, to accessible on request, to limited access to accredited persons or members of a particular profession or industry. Whether a statutory register should be regarded as publicly available should be assessed under paragraph (a) of the definition i.e. generally available to members of the public for free or for a payment.

[63] Constitution Act 1986, s 9 provides that a Parliamentary Under-Secretary has the functions, duties and powers of the Minister of the Crown that are assigned by the relevant Minister.
[64] Official Information (Parliamentary Under-Secretaries) Amendment Act 2016.
[65] NZLC R123, R8.
[66] Law Commission *Public Registers* (NZLC R101, 2008).

RECOMMENDATION B.1.6

In the definition of "publicly available publication" the term "statutory register" should be replaced with "public register".

Clarifying the Act's application to overseas agencies or overseas activities

1.20 I recommend an additional provision should be included in Part 1 of the Bill, in line with similar approaches in Europe, Australia and Canada, to clarify the application of the Act to the activities of overseas agencies that collect, hold, use or disclose personal information about New Zealand individuals, and to the overseas activities of New Zealand-based agencies.

1.21 This clarification is necessary for a number of reasons. Firstly, from the consumer perspective, it would align with consumer interests that New Zealanders dealing with overseas companies can expect suitable standards, regulation and enforcement.

1.22 Secondly, it is important that the Privacy Act is not out of step internationally. Other jurisdictions have recognised the necessity of coverage provisions as to the application of data protection laws to the activities of overseas entities that affect domestic consumers. It is desirable, for both individuals and entities trading across jurisdictions that New Zealand's law is interoperable with other comparable laws, and aligns with the global framework.

1.23 Thirdly, the Bill should provide certainty of its extraterritorial application through inclusion of this express provision. Our Supreme Court has affirmed the principle that an Act of Parliament should not be held to have extraterritorial effect unless that effect is signalled by express language or by necessary implication.[67] The Court emphasises that it is far better, both in principle and pragmatically, for Parliament to address the issues arising in a comprehensive way rather than for the courts to effect ad hoc additions by a process which does not accord with appropriate principles of statutory interpretation.[68]

1.24 The current position under the Privacy Act, continued in the Bill, provides scope for the principles to apply to the activities of overseas entities in particular circumstances. This depends, however, on the interpretation of a number of different definitions and provisions, in particular clauses 8 and 20. Other provisions and definitions are also relevant to the Act's extraterritorial application.[69]

1.25 Clause 8 continues the approach taken in section 3(4) of the Privacy Act. This provides that where an agency appoints an agent to carry out certain services such as safe

[67] The LAC guidelines (2018) suggest that where cross-border issues arise, legislation must provide clear guidance on whether New Zealand's rules or another country's rules will apply and which country or body will have the jurisdiction to make decisions.
[68] *Poynter v Commerce Commission* [2010] NZSC 38.
[69] Alan Toy "Cross-border and Extraterritorial Application of New Zealand Data Protection Laws to Online Activity" (December 2010) 24 NZULR 222, 224-5. See also Gehan Gunasekara ""MySpace" or Public Space: the relevance of data protection laws to online social networking" (December 2008) 23 NZULR 191, 205.

custody or the processing of personal information on behalf of the principal, the principal agency will be treated as remaining responsible for that information under the Privacy Act, regardless of where the agent holds the information to perform the required services (such as cloud storage).

1.26 Clause 20 continues the approach taken in section 10 of the Privacy Act. This provision serves to establish the Bill's application to personal information held outside New Zealand. It provides firstly that personal information is "held" by an agency, and therefore subject to IPPs 5 and 8-11, if it is transferred out of New Zealand by that agency or any other agency. Secondly, personal information held by an agency includes personal information held outside New Zealand by that agency, for purposes of IPPs 6 and 7.

Overseas approaches

1.27 The following sets out the approach taken in the GDPR, Australian privacy legislation, and New Zealand consumer protection legislation. They have commonalities, for example, all include a business or trade component.

1.28 The GDPR applies to non-EU organisations if they offer goods or services to individuals in the EU. The company does not have to be based or resident in the EU in order to fall within scope. Similarly, the GDPR does not differentiate between paid and unpaid services, these are treated the same.

1.29 Article 3 provides:

> This Regulation applies to the processing[70] of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
>
> This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
>
> i) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
>
> ii) the monitoring of their behaviour as far as their behaviour takes place within the Union.
>
> This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

1.30 The Australian Privacy Act makes clear that an act outside Australia by a government agency is subject to the Privacy Act.[71] Whether the acts outside Australia by other

[70] 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

entities are subject to the Privacy Act depends on whether they have an "Australian link". A link is established if the entity is an Australian citizen or entity created or incorporated in Australia.[72] A link is also established if the entity carries on business in Australia and collects personal information in Australia.[73]

1.31 Factors to assess whether an entity carries on business in Australia include whether: [74]

a) the entity has a place of business in Australia;

b) people who undertake business acts for the entity are located in Australia;

c) the entity has a website that offers goods or services to countries including Australia;

d) Australia is one of the countries on the drop-down menu appearing on the entity's website;

e) web content that forms part of carrying on the business, was uploaded by on behalf of the entity, in Australia;

f) business or purchase orders are assessed or acted upon in Australia; and

g) the entity is the registered proprietor of trade marks in Australia.

1.32 A somewhat similar link requirement is relevant in Canada to the interpretation of the application of the Personal Information Protection and Electronic Documents Act (PIPEDA). Whilst that Act that does not include an express provision as to its scope to companies outside Canada, the courts have confirmed that the Canadian Privacy Commissioner has jurisdiction under PIPEDA where there is a "real and substantial link" to Canada. In a recent decision, the Federal Court,[75] considered the following "connecting factors" in finding there was sufficient connection between Canada and the activities of a Romanian website that republished personal information from Canadian websites:[76]

a) The content at issue involved Canadian court and tribunal decisions containing personal information which was copied by the respondent from Canadian legal websites;

b) The website directly targeted Canadians by specifically advertising that it provided access to Canadian case-law, and the majority of the website's visitors were from Canada;

[71] Privacy Act 1988 (Cth) s 5B(1).
[72] S 5B(2).
[73] S 5B(3).
[74] OAIC APP guidelines – key concepts – Australian link (March 2015).
[75] A.T. v *Globe24H.com* 2017 FC 114.
[76] Alex Cameron and Claire Feltrin (28 February 2017) The Global Reach of Canadian Privacy Law: Federal Court Issues Landmark Ruling in Globe24h (www.lexology.com)

c) The impact of the website was felt by members of the Canadian public including distress, embarrassment and reputational harm by republishing personal information and making it accessible via third party internet search engines.

1.33 New Zealand consumer protection statutes have adopted the "carrying on business" test. The scope of the Fair Trading Act is expressed as:[77]

> This Act extends to the engaging in conduct outside New Zealand by any person resident or carrying on business in New Zealand to the extent that such conduct relates to the supply of goods or services, or the granting of interests in land, within New Zealand.

1.34 The Commerce Act extends to the engaging in conduct outside New Zealand by any person resident or carrying on business in New Zealand to the extent that such conduct affects a market in New Zealand.[78] The provision was amended in 2017 to clarify that a person engages in conduct in New Zealand if any act or omission forming part of the conduct occurs in New Zealand.[79]

1.35 Having surveyed the various approaches above, I recommend a new provision should be drafted for the Privacy Bill that is comprehensive, not unduly complicated or technical and enhances the privacy rights of New Zealanders. I recommend it include a number of necessary elements that are included in the recommendation below.

RECOMMENDATION B.1.7

The Privacy Bill should include an additional provision in Part 1 of the Bill, to clarify the application of the Act to the activities of overseas agencies that collect, hold, use or disclose personal information about New Zealand individuals, and to the overseas activities of New Zealand-based agencies.

The provision should include the following elements:

a) the collection, holding, use and disclosure of personal information from New Zealanders within the jurisdiction (regardless of the physical location or place of business of the agency collecting the information) is a sufficient link for application of the Privacy Act;

b) carrying on business or trade in New Zealand or the offering of goods or services establishes a sufficient link for the Privacy Act to apply, but need not require any payment by the individual concerned;

c) activities that impact on the privacy rights of New Zealanders, based on their personal information, such as the monitoring of behaviour, establishes a sufficient link for the Privacy Act to apply;

[77] Fair Trading Act 1986, s 3(1).
[78] Commerce Act 1986, s 4(1). The Court of Appeal in *Commerce Commission v Visy Board Pty Ltd* [2012] NZCA 383, [29] found that whether or not a person is "carrying on business in New Zealand" is a question of fact where a number of factors are relevant. The analysis is not confined to whether or not the company maintained a systematic and continuous physical presence in New Zealand; that states the test too highly and does not serve the purpose of the Commerce Act.
[79] S 4(1AA)(a).

d) the collection, holding, use and disclosure of personal information by New Zealand-based agencies is subject to the Privacy Act, regardless of whether the individuals concerned are New Zealand citizens or residents.

PART 2 – Privacy Commissioner

2.1 Part 2 continues provisions of the Privacy Act relating to the appointment and functions of the Privacy Commissioner.

Clause by clause comments

Clause 15: Commissioner must monitor the operation of Act

2.2 Clause 15 continues section 26 of the Privacy Act 1993, but removes the five yearly periodic reporting. However the requirement to report on the operation of the Act remains mandatory. There appears little reason to treat this function differently from the other Privacy Commissioner functions in clause 14.

2.3 To maximise flexibility and efficiency, this obligation should be reconfigured as a discretionary function under clause 14. This would allow for monitoring and reporting to the responsible Minister on the operation of the Act as is considered necessary (such as responding to technological and international developments), when assessed in light of the other functions, priorities and resourcing.

RECOMMENDATION B.2.1

Clause 15 should be incorporated into the list of discretionary functions in clause 14.

PART 3 – Information privacy principles, public register privacy principles and codes of practice

3.1 Part 3 continues the information privacy principles and exemptions with amendments (subpart 3(1)), the public register privacy principles without amendment (subpart 3(2)) and provisions relating to the Commissioner's power to issue Codes of Practice with some technical amendments (subpart 3(3)).

3.2 This part of the submission includes comments on the implementation of amendments to the IPPs and exemptions in subpart 3(1), and recommends the implementation of an outstanding Law Commission recommendation in IPP 1. This is followed by comments on the proposed continuation of the public register privacy principles in subpart 3(2). The technical amendments in subpart 3(3) are supported and I do not comment further on that subpart.

Clause by clause comments

SUBPART 3(1): INFORMATION PRIVACY PRINCIPLES

Information privacy principle 1 – Purpose of collection of personal information

3.3 No changes of substance have been made to IPP1. However a Law Commission recommendation accepted by Cabinet in 2014 has not yet been implemented and I submit that it should be. In its review of the Privacy Act, the Law Commission recommended that:[80]

> *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.*

3.4 The Law Commission proposed the express provision as a means to limit the over-collection of personal identifiers and promote individuals' control over their information. Principle 1 requires an agency to only collect personal information when it is necessary for a lawful purpose, connected with a function or activity of the agency. This means agencies should assess whether it is necessary to collect identifiers, including an individual's real name, and whether it is possible to offer the option of dealing with the individual under a pseudonym. Legislatively guiding agencies to consider anonymity and pseudonymity in collection practices would promote these options being incorporated into the design of systems and processes, where appropriate.

3.5 There is a precedent for this reform in the Australian privacy legislation.[81] Australian Privacy Principle 2 provides that individuals must have the option of not identifying themselves, or of using a pseudonym when dealing with an entity in relation to a particular matter, unless it is impracticable or the entity is required or authorised by law or court order to deal with individuals who have identified themselves.

3.6 Both the New Zealand and Australian Law Commissions identified a strong public policy rationale for statutory recognition of anonymity and pseudonymity as personal information collection options. People are likely to be more open, to access more services and participate to a greater level in society if they can confidently control their personal information, such as opting to use privacy protective measures to transact with agencies. For example, when individuals are seeking general information from an agency or submitting their views in response to a public consultation, it is not always necessary for the agency to collect the individual's real name or other identifying details.

---

[80] NZLC R 123, R35. See also supplementary reports to *Necessary and Desirable* raising Australian versions of an anonymity and pseudonymity principle and recommending a similar principle be considered for New Zealand: OPC first supplement, recommendation 17B; OPC fourth supplement, para 2.3.

[81] The Australian principle was first introduced to the Australian Privacy Act 1988 as a national privacy principle in 2000. Its application was expanded in 2010, implementing the Australian Law Reform Commission's 2008 recommendation that it should apply to Commonwealth government agencies as well as the private sector. See ALRC R 108, recommendation 20-1.

3.7 It is desirable for the legislation to expressly incorporate the options of anonymous and pseudonymous collection of personal information, where feasible and consistent with the agency's purpose for collection. This is a rights-enhancing measure that supports IPP 1 (the collection limitation principle) as it would allow individuals to ask if they can transact with an agency anonymously or pseudonymously.

3.8 Transacting anonymously is no guarantee that the individual is not identifiable to the agency concerned, as it is relatively easy to identify individuals based on their transactional information, even without formal identifiers being provided. Nevertheless, express reference to these options highlight practical options for individuals to exercise control about how they identify themselves to an agency and limit disclosure or use of their personal details. This is particularly important for vulnerable individuals who seek to protect their identity (for example individuals who have taken out protection orders). It would not unduly increase compliance costs for agencies, as these options must only be given effect where it is practicable to do so.

3.9 I therefore support implementing the Law Commission's recommendation in the Bill by adding a new sub-clause to IPP 1. An alternative drafting approach might be to amend IPP 3(1) to add a new requirement to ensure an individual is aware of an option to transact anonymously or pseudonymously that is offered by the agency, along the following lines:

(1) If an agency collects personal information from the individual concerned, the agency must take any steps that are, in the circumstances, reasonable to ensure that the individual concerned is aware of—
- *(a) the fact that the information is being collected; and*
- *(b) the purpose for which the information is being collected; and*
- *(c) the intended recipients of the information; and*
- *(d) the name and address of—*
  - *(i) the agency that is collecting the information; and*
  - *(ii) the agency that will hold the information; and*
- *(e) if the collection of the information is authorised or required by or under law,—*
  - *(i) the particular law by or under which the collection of the information is authorised or required; and*
  - *(ii) whether the supply of the information by that individual is voluntary or mandatory; and*
- *(f) <u>the option for the individual to supply the information without identifying themselves or under a pseudonym, if applicable;</u>*
- *(g) the consequences (if any) for that individual if all or any part of the requested information is not provided; and*
- *(h) the rights of access to, and correction of, personal information provided by the IPPs.*

RECOMMENDATION B.3.1

Law Commission recommendation 35 should be implemented in IPP 1 or by an alternative drafting option.

Information privacy principle 4 – manner of collection of personal information

3.10 Privacy principle 4 has been amended in the Bill to require an agency to have particular regard to the age of the individual concerned to ensure the means by which personal information is collected is fair and does not intrude to an unreasonable extent upon the affairs of that individual.[82]

3.11 In its review of the Privacy Act, the Law Commission identified that children and young people have particular vulnerabilities in relation to the protection of their privacy.[83] The Law Commission recommended an amendment to IPP 4 which is implemented in the Bill. IPP 4 (as proposed to be amended) reads as follows:

> An agency may collect personal information only-
>
> (a) by a lawful means; and
>
> (b) by a means that, in the circumstances of the case (*having regard particularly to the age of the individual concerned*)-
>
> (i) is fair; and
>
> (ii) does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

3.12 The problem that the Law Commission sought to address was that some agencies tend to take a blanket approach to the collection of personal information. This is not consistent with the collection principles that require agencies to ensure that collection practices are not unfair or unreasonably intrusive in the circumstances (IPP 4) and to adequately explain the implications of collection to the individual (IPP 3). The intent of the recommendation to amend IPP 4 is to remind agencies, when collecting information from children or other vulnerable individuals, whether online or otherwise, to take particular care on account of that vulnerability.

3.13 However I question whether this amendment will be effective to achieve the policy objective of better protecting the privacy interests of children and others whose age may raise special considerations, and whether it may have unintended consequences.

3.14 There is a risk that the proposed amendment to IPP 4 may incentivise agencies to routinely collect age or date of birth information about all individuals to verify the agency's obligations have been met, regardless of whether this personal information is in fact necessary for their functions or activities. This may result in the unnecessary over-collection of personal information (an issue under IPP 1). I also question whether the proposed amendment provides agencies with enough guidance about what their collection practices should take into account when collecting personal information about children.

[82] NZLC R123, R120.
[83] NZLC R123, at [12.43].

3.15 Other jurisdictions have introduced requirements for express verified parental consent for the collection of personal information from children in certain contexts.[84] I do not propose that such a model would necessarily be effective or a useful one for the Committee to consider for the New Zealand privacy legislation.

3.16 However, I suggest a new standalone provision that provides statutory guidance for agencies as an alternative drafting option for consideration. This provision could provide that for purposes of the collection principles (IPPs 1, 2, 3 and 4), when collecting personal information directly from children or young persons (or other individuals of limited agency compared to an adult with full decision-making capacity), an agency must take into account any relevant factors, including:

- the purpose of the collection;
- the nature and type of personal information being collected;
- the circumstances under which the information is being collected;
- the proposed use of the personal information by the agency and the proposed length of its retention;
- whether the proposed collection of the information and the proposed use is or could be detrimental to the interests of the individual it relates to and whether parental or representative consent is necessary in the circumstances; and
- whether the agency's IPP 3 statement is expressed in a suitable form to be understood by the individual and whether, in the circumstances, it should be provided to a parent or representative.

3.17 The advantage of this approach is that it directly addresses the particular policy problem and provides agencies with a clearer expectation that the subjective position of the individual whose personal information is being collected, is a relevant consideration to an agency's compliance with the collection principles. It is less likely to have the potential unintended consequences raised by the proposed amendment to IPP 4. A factors-based provision could be supplemented by Commissioner-released guidance as appropriate.

3.18 I recommend that IPP 4 should not be amended as proposed, given the risk of unintended consequences that could be detrimental to privacy, and that an alternative drafting option should be considered, such as a standalone provision that offers statutory guidance.

RECOMMENDATION B.3.2

IPP 4 should not be amended as proposed. An alternative drafting option should be considered to address the collection practices of agencies when collecting personal information from children and young people.

[84] United States COPPA (Children's Online Privacy Protection Act 1998); GDPR article 8.

Information privacy principle 11- Limits on disclosure of personal information

3.19 IPP11(2) implements a Law Commission recommendation[85] to add a new exception to principle 11 to expressly permit the reporting of suspected offending to a law enforcement agency. This has been implemented in subclause 11(2) of the Bill:

> 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.

3.20 I do not consider the amendment is necessary. Subclause 11(1)(e)(i) provides that an agency that holds personal information must not disclose it, unless the agency believes on reasonable grounds that the disclosure of the information is necessary to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, investigation, prosecution and punishment of offences. The reporting of a reasonably held belief that an offence has been or may be committed to the New Zealand Police falls squarely within the exception carried over from principle11(e)(i) of the current Act to the Bill.

3.21 Principle 11(e)(i) has now been expressly considered by the Supreme Court in *R v Alsford*[86], a pre-trial application to exclude Crown evidence in the trial of the defendant on criminal charges relating to cannabis cultivation, on the basis that evidence had been improperly obtained by Police from Mr Alsford's electrical suppliers. Police did not have a warrant or production order to obtain the information, and instead sought information on the basis that it was necessary to avoid prejudice to the maintenance of the law by any public sector agency, including the detection of offences. The information was disclosed by the electricity retailers on the basis of the principle 11 exception allowing disclosure to avoid prejudice to the maintenance of the law.

3.22 The Supreme Court noted that:

> "…the authorised purposes in the exception are broadly stated. They refer to avoiding "prejudice to the maintenance of the law by any public sector agency". They then go on to include within that broad principle, avoiding prejudice to "the prevention, detection, investigation, prosecution, and punishment of offences". Focussing again on principle 11(e), the references to "the maintenance of the law" and to avoiding "prejudice to", together with the breadth of the included purposes, particularly prevention, detection and investigation, are relevant to the nature of the reasonable grounds test that the holder of the information is required to meet to justify disclosure. They suggest that the test – **belief on reasonable grounds that non-compliance is necessary – is a relatively low one"** (emphasis added).[87]

3.23 The Supreme Court's decision in this case provides the necessary clarification that a disclosure to the New Zealand Police of the belief that an offence has or may be committed is clearly captured by the existing principle and corresponding subclause in the Bill. The Law Commission concluded that much of the uncertainty about the scope of

[85] NZLC R123, R97.
[86] *R v Alsford* [2017] NZSC 42.
[87] At 34. See also *Tan v New Zealand Police* [2016] NZHRRT 32 at [78].

the maintenance of the law exception could be addressed in guidance.[88] My Office has issued a range of guidance on the maintenance of the law exception and commentary on the Supreme Court decision.[89] These developments now make a legislative amendment unnecessary.

3.24 I also consider the amendment undesirable as the example provided may not create the certainty intended. IPP 11(2) refers only to Police. This may give rise to doubt about whether disclosures to other public sector agencies are permitted under this ground. IPP 11(1)(e)(i) permits disclosure to any public sector agency, which could include, for example, the Ministry of Social Development, the Ministry of Business, Innovation and Employment, the Department of Corrections, the New Zealand Parole Board, and the Ministry of Education. The Commissioner considers that it is unnecessary to include IPP 11(2) and its inclusion risks creating unintended uncertainty.

RECOMMENDATION B.3.3

IPP 11(2) should be deleted.

Information Privacy Principle 11(3) - (6)

3.25 The Bill includes a new clause (3) in information privacy principle 11 that obliges agencies when disclosing information overseas to ensure that the information is protected in one of various ways.[90] I support the imposition of this obligation as a suitable way to seek to protect individuals in today's digital economy.

3.26 This kind of border restriction has become increasingly common internationally in recent years and is the recommended approach in notable European standards. A similar approach has operated in Australia for many years. With more countries having established or being likely to establish whitelisting processes, other countries are likely to look for the existence of border controls in assessing whether other country's laws meet their standards. The border controls in IPP 11 have been drafted in a sufficiently flexible way to align with APEC and OECD guidance to be proportionate and to sufficiently take account of issues of risk, purpose and context.

Making provision for binding schemes

3.27 The first point raised is the desirability of the principle explicitly recognising that 'comparable safeguards' might be provided by binding schemes (such as the APEC

[88] NZLC R123 at [9.45].
[89] The issue of guidance fulfils the Law Commission's recommendation 96; see OPC AskUs "When can I rely on the maintenance of the law exception?"https://privacy.org.nz/further-resources/knowledge-base/view/247?t=98326_137890; OPC Releasing personal information to Police and law enforcement agencies: Guidance on health and safety and maintenance of the law exceptions (October 2017) https://privacy.org.nz/assets/Files/Reports/October-2017-Final-Guidance-on-releasing-personal-information-to-Police-and-law-enforcement-agencies-Principle-11f-and-ei.pdf ; Privacy Commissioner's blog post on Alsford decision (11 May 2018) https://privacy.org.nz/blog/supreme-courts-alsford-decision-affirms-role-of-the-privacy-act/
[90] NZLC R123, R110 - R112.

Cross Border Privacy Rules system).[91] This would add to the flexibility and interoperability of the law. Where applicable, such provision would give affected businesses (and those dealing with them) greater certainty about compliance with the standard.

3.28 The APEC Cross Border Privacy Rules system (CBPRs), and its processor counterpart APEC's Privacy Recognition for Processors (PRP) scheme, are arrangements that provide a degree of interoperability between privacy laws in the Asia Pacific in relation to cross-border transfers. Enforceability of privacy standards is extremely difficult to achieve in the context of transfers out of the jurisdiction and this is a challenge that APEC has sought directly to address through those two schemes. Europe operates a similar scheme known as 'Binding Corporate Rules'.

3.29 It would be possible to easily reference arrangements such as CBPRs, PRP and BCR by the generic label 'binding scheme' (the phrase used in the equivalent Australian principle) which could be defined as follows:

> **Binding scheme** means an arrangement that binds participants to provide, in relation to cross-border disclosures, a continuing level of protection to personal information and to provide individuals with redress and remedies in cases where privacy protections are violated.

3.30 New Zealand has not yet taken any decision to participate in the APEC schemes. However, there could be provision for the APEC schemes to be prescribed for the purpose of the clause in the event that NZ does participate. The following definition could be included:

> **Prescribed binding scheme** means a binding scheme that is specified in regulations as providing comparable safeguards to this Act.

3.31 Accordingly, in addition to IPP11(a) to (d), IPP 11(3) could allow for disclosure where A believes on reasonable grounds that:

- B participates in a prescribed binding scheme; or
- B participates in a binding scheme that provides comparable safeguards to this Act.

3.32 Both provisions would be useful. If there is a prescribed scheme, simply disclosing to a participant would suffice. However, there are other schemes that exist that are not prescribed and the agency would simply need to satisfy itself that they offer comparable safeguards to the Act. Examples might be disclosure to a CBPR-certified company prior to NZ deciding to join the scheme or disclosure to a BCR-certified company operating outside the EU. There are binding self-regulatory schemes existing in a number of countries that do not yet have applicable privacy law.

[91] NZLC R123, R115.

RECOMMENDATION B.3.4

IPP 11(3) should include provisions permitting disclosure to participants in binding schemes that provides comparable safeguards to this Act.

Information Privacy Principle 11(3)(b) – authorisation by the individual concerned

3.33 The second point raised is a recommended amendment to IPP11(3)(b).

3.34 The recently modernised Council of Europe Convention allows for the transfer of personal information with the individual's consent but explicitly provides that the individual must first be informed of the risks.[92]

3.35 I consider it necessary to make clear that the consent for this purpose must be fully informed consent, before the exception applies, and this should be clarified in the Bill by amending IPP11(3)(c) to add the phrase "after being informed of risks arising in the absence of comparable safeguards.

RECOMMENDATION B.3.5

IPP11(3)(c) should be amended by adding the phrase "after being informed of risks arising in the absence of comparable safeguards".

Information Privacy Principle 11(6) - Definition of overseas person

3.36 Thirdly, an overseas person is defined in the Bill in IPP11(6) as "a person outside New Zealand who is not subject to this Act."

3.37 The definition is used in IPP11(3) as the threshold for the new obligation on an agency when disclosing the personal information of individuals to an overseas entity. Where the personal information is disclosed beyond the jurisdiction of the New Zealand Privacy Act, there will be an onus on the discloser to ensure that the information will be subject to alternative privacy safeguards.

3.38 In my view the definition could be simplified, by deleting "who is not subject to the Act." The policy objective is that IPP 11(3) applies where personal information is disclosed beyond the jurisdiction of the New Zealand Privacy Act. Depending on its activities and the nature of its links to New Zealand, an overseas person may be subject to the New Zealand Privacy Act in relation to some activities but not others. Specifying that an overseas person is not subject to the Privacy Act could introduce confusion about the intended scope of IPP11(3) and when it applies.

[92] Council of Europe Convention for the Protection of Individuals with Regard to the Processing of Personal Data (adopted 17-18 May 2018), article 14(4)(a): Notwithstanding the provisions of the previous paragraph, each Party may provide that the transfer of personal data may take place if: a. the data subject has given explicit, specific and free consent, after being informed of risks arising in the absence of appropriate safeguards; or …

3.39 This can easily be resolved by the recommended deletion. This aligns with the comparable provision in the Australian Privacy Act.[93]

RECOMMENDATION B.3.6

The definition of overseas person in IPP 11(6) should be amended by deleting "who is not subject to this Act."

Information privacy principle 12 – unique identifiers

3.40 IPP 12 responds to the social and technical concerns associated with referring to individuals by number. The underlying social concerns are that individual dignity is undermined by a dehumanising practice of referencing individuals solely by numbers and that having multiple agencies using the same identifier would be a step towards a de facto national identification number (and raising fears of a surveillance state). The more practical technical concerns revolve around the problems for information accuracy that can be caused by unique identifiers, both in general, and when one organisation tries to use the numbering system of another.

3.41 IPP 12 addresses the issues by regulating systems that agencies use for uniquely numbering people and placing controls on what agencies can do with numbers generated by such systems.

3.42 I support the proposed drafting improvements in IPP 12. In particular I welcome both:

a) Clarifying the drafting of the IPP (although further improvement may be possible) and of the related definition of a "unique identifier";

b) The substantive changes, implementing Law Commission recommendations,[94] including:

- A statistical exception in IPP 12(2)(b);
- An obligation in IPP 12(5) to minimise risks when disclosing unique identifiers (e.g. by masking some of the digits as part of efforts to combat identity fraud).

3.43 The following comments relate to drafting issues with IPP 12(2) and IPP 12(5).

IPP 12(2) drafting issues

3.44 IPP 12(2) addresses the same issue as does IPP 12(2) in the 1993 Act: the practice of an organisation using another organisation's unique numbering system as its own. An example would be an employer that used the tax file number of all its employees as the identification number for employees within the employer's agency. The practice of agencies cross-using a unique identifier in this manner is prohibited. The prohibition

[93] Australian Privacy Principle 8.1 provides that an "overseas recipient" is a person who is not in Australia and is not the disclosing entity or the individual concerned.
[94] NZLC 123, R33 and R117.

addresses both the technical concerns in relation to accuracy created by the practice[95] and the social concerns over the creation of a de facto national identification number. However, the provision can prove difficult to read without referring to supporting information and agencies commonly raise questions about the scope of the prohibition on the assignment of unique identifiers.

3.45 The Law Commission recommended that IPP 12(2) be redrafted so that the meaning is clearer.[96] The Law Commission recommendation focused upon the meaning of 'assign' as a source of confusion as IPP 12(2) in the 1993 Act was somewhat difficult to interpret by the use of 'assign' or 'assigned' in three places (in relation to the agency that originally assigned the identifier, the second agency that was prohibited from assigning the same number, and the general definition of 'unique identifier'). IPP 12(2) has been redrafted to read more clearly than the 1993 Act, by:

a) Removing 'assign' from the definition of unique identifier;

b) Using an 'Agency A/Agency B' formulation to more easily track through the obligations;

c) Including a statistical or research exception to remove one of the more commonly arising interpretational complications to the prohibition of re-assignment;

d) Adding an example of a practice that does not amount to assignment.

3.46 While we think the drafting of IPP 12(2) (taken together with IPP 12(3)) is considerably clearer than existing IPP 12(2) in the 1993 Act, I recommend further amendment to improve the clarity of the provision The Bill presents the opportunity to improve accessibility and understanding of this privacy principle.

3.47 This recommendation builds upon our view that confusion can arise by the fact that the word 'assign' (or 'assigned') is used twice and in slightly different senses. It would be better to use the word 'assign' only once.[97]

3.48 It would simplify the clause by using a substitute phrase in place of 'assign' in IPP 12(2) in relation to Agency B. I suggest that the phrase 'has been assigned to that individual by another agency (Agency B)' be replaced with the phrase 'has already been adopted by another agency (Agency B) as its own identifier'. This phrase is derived from wording

[95] As evidenced by problems in the USA over widespread adoption of the Social Security Number outside the social security context.
[96] NZLC 123, R32.
[97] The clause uses the term "assign" once in respect of Agency A and again in respect of Agency B. Agency B's original assignment arises from a system operated to create unique identifiers in a database, associate them with a particular individual whose details are known and bring them into use for identification purposes for the administration of the agency. By contrast Agency A's use of an earlier assigned identifier might vary quite markedly. It is not obvious to staff in agencies as to what constitutes "assignment" and they wonder, for example, whether noting down a reference number on an identity document they've viewed for verification purposes amounts to assignment (it does not).

adopted in the equivalent principle in the Australian privacy law which has avoided some of the interpretational difficulties encountered with the New Zealand principle.[98]

RECOMMENDATION B.3.7

IPP 12(2) should be amended by replacing the second reference to the word 'assign' by the phrase 'adopt as its own identifier'.

IPP 12(5) drafting issues

3.49 IPP 12(5) requires an agency to take reasonable steps to minimise the risk of misuse that can result from the uncontrolled release of unique identifiers. An example of the type of reasonable steps that might be contemplated would include number truncation if the unique identifier is printed on a document or displayed on an electronic screen or the encryption of numbers in transmission. An example of the kind of misuse in contemplation would be where an identifier falls into the hands of unintended recipients, such as identity thieves who use the identifier to access an account: this misuse can be readily enabled through lax practice in the display or recording of identifiers.

3.50 This requirement applies before disclosing a unique identifier 'to another agency'. I recommend that the clause be widened because the risks arise not merely with respect to disclosures to agencies but also, for example, on receipts printed for the individual concerned or for disclosures to overseas persons. Widening the scope of IPP 12(5) would be consistent with the relevant Law Commission recommendation which proposed that the obligation extend both to disclosure 'or display' of an identifier.[99]

3.51 I recommend that the scope of the new requirement extend to "display" of a unique identifier, as well as to "disclosure". Both terms are commonly used in relation to unique identifiers as there are risks to privacy from disclosing unique identifiers between entities and from their public display and use in documentation and communications with the individual. Some of these uses will be covered by the term ""disclosure", but the provision also needs to cover the display of a unique identifier in documentation (such as a receipt) that is given to the individual or in communications with the individual, to protect the individual from the risk of identity theft in the event that the documentation or communications are intercepted or lost.

3.52 I suggest that the obligation apply to a disclosure to 'any other agency or any other person', the wider phrase used in IPP 11. This phrase should be adopted at the start of IPP 12(5) together with a small change at the end to make it clear that the obligation is to minimise risk by misuse by the person intended as the recipient but also any other person. Thus IPP5) would read:

> Before disclosing a unique identifier to another agency *or any other person*, *or before displaying a unique identifier,* Agency A must take all reasonable steps to minimise the risk of misuse of the unique identifier by that other agency *or person* or any other person.

[98] Privacy Act 1988 (Cth), Australian Privacy Principle 9.
[99] NZLC 123, R117.

RECOMMENDATION B.3.8

IPP 12(5) should be amended by extending its application to disclosures to 'any person' and to the display of a unique identifier.

Clause 22: Relationships between IPPs and other law

3.53 This clause continues section 7(1), (2) and (4) of the Privacy Act 1993. This establishes the statutory relationship between the privacy principles and other legislative provisions. The privacy principles generally defer to other law and will be overridden to the extent that another provision is inconsistent with the privacy principle.

3.54 However this clause does not implement a Law Commission recommendation to limit future regulations prevailing over the privacy principles unless the Act empowering the regulations expressly authorises the override.[100] As the Law Commission notes, it is unusual for delegated legislation to be able to modify primary legislation and it is generally undesirable:[101]

> *In an age where concerns about our privacy are increasing, the privacy principles should be seen as more robust than that.*

3.55 The Law Commission's recommendation was supported by the majority of submissions it received on the issue. I support an amendment to clause 22 to implement the recommendation. This could be implemented with a 12 month deferred commencement, to allow for any necessary consequential amendments to empowering provisions.

RECOMMENDATION B.3.9

Clause 22 should be amended to limit future regulations prevailing over the privacy principles unless the empowering provision expressly authorises the override, as recommended by the Law Commission.

Clause 23: Exemptions relating to IPPs 1 to 4 and 12

3.56 This clause carries over an existing exemption from certain IPPs for acts prior to 2 July 1993. Clause 23(2) and (3) relate to the exemption for unique identifiers before 2 July 1993.

3.57 I suggest that clause 23(3) is unnecessary and can be deleted to remove duplication in relation to IPP12(2). Clause 23(2) adequately carries over the current exemption from section 8(5) of the Privacy Act 1993.

RECOMMENDATION B.3.10

Clause 23(3) should be deleted.

[100] NZLC R123, R80.
[101] NZLC R123 at [8.6].

Clause 24: Exemption for personal information relating to personal or domestic affairs

3.58 Clause 24 re-enacts and modernises the domestic affairs exemption that exempts the application of the IPPs to personal information relating to personal or domestic affairs. Changes have been made to the scope, structure and terminology of the exemption.

3.59 Clause 24 implements a Law Commission recommendation.[102] The exemption will no longer apply if the information is being or has been collected by unlawful means (by the omission of IPP4(a) from clause 24(1)),[103] or by engaging in misleading or deceptive conduct (clause 24(3)(a)). I make recommendations about the proposed amendments to this exemption, including its new scope, and its language and structure.

3.60 Firstly, I support narrowing the exemption to exclude collection by unlawful means. This change will provide individuals with the ability to access civil remedies for serious breaches of privacy, for example where an individual has collected information by falsely representing they are another person to obtain a financial advantage.

3.61 However I do not consider it necessary or desirable to further narrow the domestic affairs exemption to exclude other misleading or deceptive conduct. The primary intent of this part of the proposed reform is to address the "pretexting" situation where an individual collects another person's information by falsely representing that person, or falsely pretending to be that person.[104]

3.62 The Privacy Act already provides for actions considered to be highly offensive to fall outside the scope of the exemption. The Bill will provide new avenues to address issues such as identity theft or false misrepresentation. The new criminal offence in clause 212(2)(c) provides that a person commits an offence under the Privacy Act if the person impersonates or falsely pretends to be an individual for the purpose of obtaining access to that individual's personal information and/or having that individual's personal information used, altered, or destroyed. The criminalisation of this activity means it will be unlawful and therefore excluded from the scope of the clause 24 exemption (as the exemption will no longer extend to IPP4(a) that limits the collection of personal information by unlawful means).

3.63 In my view, the limits on the exemption need to be set at an appropriately high level, such as unlawfulness, as proposed, or "highly offensive", an existing limit on the exemption. A limit on misleading and deceptive conduct between individuals in their personal lives does not set a sufficiently high threshold to limit the potential for regulatory intrusion into personal affairs.

3.64 I am mindful that the rationale for the domestic affairs exemption is to limit the application of the Privacy Act to people's everyday domestic affairs, and the potential for the Privacy Commissioner and Human Rights Review Tribunal being caught in the

[102] NZLC R123 R 45. Part of the recommendation was implemented by the Harmful Digital Communications Act 2015. See also OPC Necessary and Desirable (1998) recommendation 17.
[103] IPP4(a) provides that personal information may only be collected by lawful means.
[104] Necessary and Desirable, recommendation 17.

middle of domestic disputes.[105] Attempting to resolve privacy complaints about misleading conduct between individuals in their personal lives has the potential to be fraught and may undermine the overall policy objective of the overall exemption. I therefore recommend deleting clause 24(3)(a).

3.65 Secondly, I recommend that the phrase "personal, family or household affairs" from the current exemption in section 56 of the Privacy Act 1993 be retained, rather than shortening the expression to "personal and domestic affairs". The original phrase should be retained as it usefully conveys the meaning and scope of the exemption, especially to individuals.

3.66 Thirdly, I am concerned that splitting up the exemption between different principles, adds complexity. The provision should be expressed as plainly as possible, given its relevance to ordinary citizens. Clause 24 would be easier for users (particularly individuals) if structured as one exemption (as per the current structure in s 56) covering all the IPPs.

3.67 The key point is that the IPPs do not apply to individuals in a personal capacity, with two exceptions – where the personal information was collected unlawfully, and where any action by an individual in relation to another person's personal information would be considered highly offensive.

3.68 An alternative drafting option would be along the lines of the following:

(1) The Information Privacy Principles do not apply in respect of:

a. the collection of personal information by an agency that is an individual; or
b. personal information that is held by an agency that is an individual, -
where that personal information is collected or held by that individual solely for the purposes of, or in connection with, that individual's personal, family or household affairs.

(2) The exemption in subsection (1) ceases to apply once the personal information concerned is collected, disclosed, or used, if, -
a. the information is or was collected unlawfully; or
b. the collection, use or disclosure of the personal information would be highly offensive to an ordinary reasonable person.

RECOMMENDATION B.3.11

Clause 24(3)(a) should be deleted.

The phrase "personal or domestic affairs" should be replaced with "personal, family or household affairs".

The structure of clause 24 should be simplified.

[105] NZLC IP 17 at [5.44].

Clause 26: Certain personal information exempt from IPPs 6 and 7

3.69 This clause provides certain exemptions from IPPs 6 and 7 (access and correction). It implements a Law Commission recommendation in clause 26((1)(c) to exempt the work of the Auditor-General from these two principles.[106]

3.70 In my view, an amendment is desirable to clarify, as the Law Commission intended, the exemption does not extend to personal information about the Auditor-General's current, former and prospective staff. Accordingly I recommend a clarification to clause 26(1)(c).

RECOMMENDATION B.3.12

Clause 26(1)(c) should be amended so that it does not apply to personal information about the Auditor-General's current, former or prospective staff.

SUBPART 3(2) – PUBLIC REGISTER PRIVACY PRINCIPLES

3.71 The Bill does not implement any change to the public register privacy principles or supporting provisions. The four public register privacy principles have been carried over from the Privacy Act 1993, along with Schedule 2 that lists certain public register provisions these principles apply to. The Bill's Disclosure Statement notes that these reforms may be considered for a future amendment Bill.

3.72 I recommended that the public register privacy principles should be repealed,[107] noting the Law Commission's public register reform proposals in 2008.[108] I am concerned that re-enacting these provisions in the Bill detracts from the objective of updating and modernising the Privacy Act so that it is made fit for purpose and provides a robust system of privacy regulation in New Zealand for the modern era.

3.73 In its consultation, the Law Commission found little support for the continued use of the public register privacy principles. The public register privacy principles have limited utility in the modern information environment and need to be substantively overhauled by repealing Part 7 of the Privacy Act and replacing it with specific privacy safeguards such as the suppression of personal information in cases requiring the protection of personal safety. This is urgent as there is not currently any central point of contact to request suppression where an individual's details appear on multiple public registers.

3.74 I recommend:

a) repealing the public register privacy principles and associated provisions in subpart 2 as well as clauses 76(1)(b) and 98, amending clauses 82 and 83 to delete references to public registers; and

[106] NZLC R123, R42.
[107] Section 26 report, recommendation 6.
[108] Law Commission *Public Registers* (NZLC R101, 2008). See also OPC Necessary and Desirable, ch 7.

b) including new privacy safeguards in the Bill to provide for the suppression of personal information in public registers where there is a safety risk by application to the Privacy Commissioner, and for complaints to the Privacy Commissioner about breaches of public register access conditions.

3.75 An alternative option would be to make provision for subpart 2 of the Bill and associated provisions to expire 12 months after the Bill comes into force, to allow for a Privacy (Public Registers) Amendment Bill to be introduced.

RECOMMENDATION B.3.13

Subpart 3(2) should be repealed and replaced with new privacy safeguards to provide a practical suppression mechanism for individuals whose safety is at risk, and to provide for privacy complaints where public register access conditions are breached.

Alternatively, the Bill should provide for expiry of subpart 2 12 months after the Bill comes into force, to allow for a Privacy (Public Registers) Amendment Bill to be introduced, that includes a practical suppression mechanism and provides for privacy complaints where public register access conditions are breached.

PART 4 – Access to and correction of personal information

Access and correction requests

4.1 Part 4 of the Bill updates and modernises the important procedural provisions for agency handling of access and correction requests that currently sit in Part 5 of the Privacy Act 1993, and includes the grounds on which an agency can refuse an access request that currently sit in Part 4 of the Privacy Act.

4.2 These provisions support two privacy principles that have particular significance for individuals. IPP6 represents the fundamental right for individuals to seek access to their personal information, and IPP 7 provides a practical mechanism for individuals to seek to have their personal information corrected by the agency holding it, or at least to include the individual's statement of correction.

4.3 I have a fundamental concern with the overhaul of Parts 4 and 5 of the 1993 Act, by Part 4 of the Bill, particularly subpart 4(1). I note that the proposed re-organisation does not originate from a Law Commission or Privacy Commissioner recommendation, but results from the general instruction to modernise the drafting in the new Bill. While I support modernisation and clarification, this must be achieved without creating adverse consequences to individuals or users of the provisions.

4.4 In my assessment, the redraft would create unintended consequences for fundamental access rights of individuals and potentially add to the compliance burden imposed on agencies under the new legislation. There are two key problems with the drafting of subpart 4(1) in the Bill:

a) The split process for different types of access request risks does not properly reflect the way in which IPP 6 access requests are made by requesters and handled by agencies in practice. As a consequence it risks weakening the IPP 6 access right (the right to ask an agency for confirmation it holds your information and to have access to that information);

b) The overhaul of the structure in this part of the Bill creates a very different "look and feel" to the current provisions, and risks unnecessary disruption to the continuity between the old provisions and the new, with the result that agencies will likely incur compliance costs transitioning to the new process.

4.5 These risks can be avoided by reducing the disruption to the structure of current provisions, and applying a precautionary approach to the modernisation of current provisions.

4.6 The structure proposed in this part of the Bill duplicates common procedural provisions and some of this duplication could be readily removed. An alternative drafting option for Part 4 to mitigate these risks is outlined below. I favour ordering the provisions in an accessible way for users to clearly set out the procedural pathway that represents the normal type of response, while allowing for particular provisions to be used as relevant in specific circumstances.

4.7 Two new refusal grounds are introduced to protect people other than the requester where access to the information sought may create a serious risk of harassment or unduly impact on victims.[109] Amendments are made to improve the operation of the existing refusal grounds and the processing provisions.[110] I support these changes, and make recommendations about their implementation.

4.8 One Law Commission recommendation has been implemented in a different manner to that proposed.[111] I support the intent of the Law Commission recommendation (to create additional safeguards against coerced access requests) but recommend it be implemented in clause 63 to achieve the recommendation's intent.

4.9 Two Law Commission recommendations (22 and 93), accepted by Cabinet in 2014, have not yet been implemented in Part 4 of the Bill and I submit that they should be.

Carrying over of Parts 4 and 5 of the Privacy Act 1993

4.10 Part 4 of the Bill departs from a unified procedure in Parts 4 and 5 of the Act for access and correction requests ("information privacy requests") and introduces provisions to create specific processes for:

a) Access requests under IPP 6(1)(a) seeking confirmation that and agency holds personal information (Part 4(1) - clauses 43-48);

[109] NZLC R 123, R23 is implemented in clause 52(1)(a)(ii) (significant risk of serious harassment) and R25 is implemented in clause 52(1)(a)(iii) (protection for information affecting victims).
[110] Necessary and Desirable, recommendations 24, 53, 54, 55, 68; NZLC R 123, R26, R28 and R29.
[111] NZLC R123, R17.

b) Access requests under IPP6(1)(b) seeking the provision of personal information about the requester (Part 4(1) - clauses 43-47, 49-60); and

c) Correction requests (Part 4(2) - clauses 61-69).

4.11 I support the introduction of different subparts in Part 4 of the Bill for responding to access and correction requests as this usefully highlights the right of correction that is sometimes overlooked.

4.12 However, subpart 4(1) represents a significant change to procedural provisions for access requests that are used by agencies on a daily basis. I recommend Part 4 of the Bill be redrafted to mitigate the issues raised. I provide an indicative alternative structure for Part 4 in table form at the end of this section of the submission.

The nature of IPP6 access requests

4.13 Individuals have a constitutionally significant right to ask an agency for their personal information. Privacy principle 6 embodies this as an interconnected right: the IPP6(1)(b) right to seek access to one's own personal information (IPP6(1)(b) and the right to seek confirmation that one's personal information is held by the agency (IPP6(1)(a)). The right to seek access is the overwhelmingly common demonstration of the IPP6 right, with the related right to seek confirmation being relevant only in much rarer circumstances.

4.14 Access requests by individuals take various forms and need not be specific as to the type of access right being exercised. They need not refer to the Privacy Act or to a specific privacy principle. They may be expressed generically as an "access request" or as a "principle 6 request". Often requesters will ask for all information about themselves or for information within a certain time range.

4.15 In a very tiny percentage of cases, a request may specifically be limited to seeking confirmation of whether information is held (IPP6(1)(a)). This is usually in the context of requests to the intelligence and security agencies or to the law enforcement agencies. Otherwise, current standard practice is for access rights to be exercised by default as requests for both confirmation and access to information, and for agencies to process those requests accordingly. Requests for confirmation only are handled by agencies on an exceptional basis. This approach is consistent with the fundamental right of access to information.

Problems with redrafting access procedures

4.16 Part 4 of the Bill reconfigures the IPP6 right to request access and confirmation as independent rights for procedural purposes. This is potentially detrimental to the right of access and, as discussed above, does not reflect the way in which access rights are exercised. Overall, I consider that the redrafting risks an interference with a substantive human right of access to one's own personal information.

4.17 The approach may impose new obstacles and delay for individuals seeking access to their information by placing more emphasis on the form of the request made to an

agency.[112] There is potential for agencies, under a technical reading of the newly drafted procedures, to adopt a two-stage approach to responding to requests. For example, clauses 49 and 50 may be misread as requiring or allowing an access request be dealt with in two parts with two separate timeframes. While this interpretation is not intended, it introduces uncertainty and potential complexity for the complaints process, an area that is well settled under current law.

Risk of added compliance costs

4.18 I am mindful that significant redrafting of any core features of the Privacy Act can increase upfront transitional compliance costs for agencies. The substantial restructure to these fundamental and widely used provisions could result in agencies revising their internal policies and procedures in response. This adds to the overall compliance burden for agencies adjusting to substantive reforms made by the Bill, without commensurate benefit or improvement to the privacy rights of New Zealanders.

4.19 Therefore I support a precautionary approach to the carry-over of commonly used provisions (that produce the majority of the privacy complaints made to my Office) to avoid introducing unnecessary change or uncertainty for regular and frequent users of the Privacy Act. The objective must be to keep compliance costs for agencies transitioning to the new legislation to a minimum where the changes made are technical redrafting rather than substantive reforms.

4.20 An objective of my proposed drafting option below is to retain some of the familiarity of the current provisions in the Privacy Act. This is to reassure agencies that the provisions are substantively the same (apart from the specific reforms to implement recommendations). Part 4 of the Bill should retain more of the well-known sign posts in the current Act so that agencies can easily adapt to the new legislation and maintain a common approach. For example, my proposed drafting option attached would retain a separate sub-part for the refusal grounds (as Part 4 of the Act currently provides) and retain stand-alone provisions to carry over sections 30 and 32 of the Act.

Privacy Commissioner's recommended drafting option

4.21 Part 4 of the Bill should reflect the nature of the IPP6 access right as a right to request access to one's personal information. To avoid the right being read down in a technical sense, the process should continue to provide for IPP6 requests to be considered as requests for access to information by default, unless the request is explicitly limited in the circumstances to confirmation only. I recommend Part 4 retain a unified procedure for responding to access requests that is flexible enough to deal with the exceptional request for confirmation only. This can be achieved as outlined in the table at the end of this section.

[112] This potentially detracts from the objective of the Bill to facilitate greater efficiency of process and speedier access to personal information, for example, the new power in clause 96 for the Commissioner to make binding directions on access complaints.

4.22 The objectives of this proposed approach is to retain and carry-over the current provisions (as modified by substantive reforms), to minimise interference with individual rights of access, and to reduce duplication of provisions. In particular, the provisions for decisions on IPP 6 requests are re-unified.

4.23 This approach organises Part 4 as follows:

a) Subpart 4(1) Access to personal information – responding to access requests under IPP 6;

b) Subpart 4(2) Good reasons for refusing access to personal information (the refusal grounds);

c) Subpart 4(3) Correction of personal information – responding to correction requests;

d) Subpart 4(4) Procedural provisions relating to access and correction of personal information (transfers of requests to another agency, extension of time limits for responding, and charging).

4.24 The key features of the alternative drafting option are:

a) Amalgamating clauses 49 and 50 into one clause, to retain the Act's unified procedure for responding to access requests, regardless of form, while allowing for the specific type of access request where necessary;

b) Organising the provisions in four sub-parts rather than three, to allow the refusal grounds to sit in a separate subpart (as they do currently in Part 4 of the Privacy Act 1993) and as a way to simplify the procedure for access requests in subpart 4(1);

c) Adding a separate subpart for the refusal grounds on clauses 52 to 57 to simplify subpart 4(1) and for accessibility (as per Part 4 of the 1993 Act);

d) Placing two key provisions (sections 30 and 32 of the 1993 Act) in standalone provisions with appropriate cross references, to simplify the drafting of clauses 49 and 50; and

e) Shifting common procedural provisions (transfers and extension of time limits) to the end of Part 4 to sit with charging provisions, to remove duplication.

RECOMMENDATION B.4.1

The drafting of Part 4 should be reorganised, following the outline provided.

Part 4 should reflect the nature of the IPP 6 access right as a right to request access to one's personal information, retaining the Act's procedure for responding to requests on the basis that access is sought, and the Act's flexibility to deal with the exceptional request for confirmation only.

The provisions should be organised to clearly set out the procedural pathway that represents the usual type of response, with particular provisions being available as relevant in specific circumstances.

To maintain the settled approach, Part 4 should retain the well-known provisions in the current Act in a similar form.

Clause by clause comments

4.25 This part of the submission comments on provisions in Part 4 of the Bill, including the implementation of Law Commission recommendations. I note that two Law Commission recommendations that have not yet been implemented in this part,[113] and I recommend they should be. I also propose amendments to correct inadvertent changes to provisions, in order to carry over their current effect in the Privacy Act 1993.

Clauses 47 & 67: Assistance

4.26 Currently agencies are required to assist requestors.[114] This duty is continued in the Bill (clauses 47 and 67) but important features have been omitted. I consider it necessary to retain the features of the current provision as it has proved to be rights enhancing from the citizen's perspective and acts, where necessary, as a useful circuit breaker to defuse agency bureaucracy. I recommend amending the Bill to include the missing elements from section 38 of the Privacy Act including:

a) the duty to assist an individual who has not made the request in accordance with the requirements of the Act (for example a request is made on someone's behalf without the appropriate authority being in place, or one request is made by a group who each need to make individual requests); and

b) the duty to assist an individual to make their request to the appropriate agency (as it is useful and often quicker to have the flexibility of directing people to the another appropriate agency, as an alternative to the formality of the transfer provision).

RECOMMENDATION B.4.2

Clause 47 and 67 should be amended to carry over the effect of section 38 of the Privacy Act 1993 by including the duty to assist an individual to make a request in accordance with the requirements of the Act and to make the request to the appropriate agency.

Clauses 48 & 68: Transfers of access and correction requests

4.27 Clauses 48 and 68 continue the existing obligation on agencies to transfer access and correction requests respectively. Clause 48(3) and (4) implement a law reform recommendation of the first Privacy Commissioner[115] so that an agency will not have to transfer an access request if it has good reason to believe the requestor does not wish the request to be transferred.

4.28 I recommend extending this amendment to correction requests in clause 68 to align the two transfer clauses (in the event that two transfer provisions are retained). The reform proposal was not limited to access requests. There may be instances, although rarer, where an individual does not wish a correction request to be transferred to a different

[113] NZLC R123, R22, R 93.
[114] Privacy Act 1993, s 38.
[115] Necessary and Desirable, recommendation 68.

agency. The correction sought may need to be altered before it is put forward to a different agency.

RECOMMENDATION B.4.3

Clause 68 (if retained) should be amended for consistency with clause 48(3) and (4).

Clauses 49(2)(c), 49(3); 50(2)(c), 50(4), 59: Neither confirm nor deny

4.29 "Neither confirm nor deny" is an access request response option available to an agency in exceptional circumstances.[116] It is a complex provision that currently sits in section 32 of the Privacy Act 1993. In the Bill, the provision has been split across a number of provisions. I support modernisation of the provision. However, I recommend it continue to sit in a standalone provision, given the specific nature of its use, and for readability.

4.30 A standalone provision is suggested along the following lines to replace section 32 of the Privacy Act 1993:

(1) This section applies to an access request where –

(a) the agency has good reason to refuse access, in whole or in part, under sections 52(1)(a)(i) and (d), 54, 55 and 57(b); or
(b) if the agency would have had good reason to refuse access, under sections 52(1)(a)(i) and (d), 54, 55 and 57(b) if the information existed.

(2) If the agency is satisfied that an interest protected by sections 52(1)(a)(i) and (d), 54, 55 and 57(b) is likely to be prejudiced by confirming that the agency holds the personal information requested or does not hold that information, the agency may give notice to the requestor that it neither confirms nor denies the information exists.

4.31 Sub-clauses 59(1), (2)(a), (3) and (4) should be deleted. Where an agency is entitled to provide a "neither confirm nor deny" response, the obligation to provide reasons and grounds does not arise.

4.32 There is a cross reference to the "neither confirm nor deny" provision in clause 209(3) that is currently incomplete as it does not refer to clause 50(2)(c). This cross reference should be reviewed.

RECOMMENDATION B.4.4

For clarity, and to reflect that it arises only in special circumstances, the "neither confirm nor deny" response option to an access request in clause 49(3) and 50(4) should be moved to a standalone provision.

Sub-clauses 59(1), (2)(a), (3) and (4) should be deleted.

[116] https://privacy.org.nz/the-privacy-act-and-codes/privacy-principles/access/neither-confirm-nor-deny/

Clause 50(3): Limited reasons to refuse

4.33 Clause 50(3) continues the limit on the reasons for which an agency can refuse to provide access to personal information in section 30 of the Privacy Act 1993. However clause 50(3) refers only to the Privacy Act refusal grounds, and omits reference to reasons in other legislation that may restrict access, as contemplated in clause 22(1)(b) of the Bill. I therefore recommend that the clause be amended.

4.34 To ensure this important provision continues to be given due prominence, my preference is to retain a standalone provision. A provision along the following lines is recommended:

An agency may refuse an access request only in accordance with –
(a) sections 52 to 57; [good reasons to refuse access]
(b) section 22(b) [other law];
(c) section 49(2)(c)/50(2)(c) [neither confirm nor deny]

RECOMMENDATION B.4.5

The limit on the reasons to refuse an access request in clause 50(3) should be moved to a standalone provision.

To carry over the effect of section 30 of the Privacy Act 1993, the scope of the limit should include the requirements of other laws that may provide good reason to refuse an access request.

Clauses 51 & 71: Extension of time limits

4.35 Clauses 51 and 71 continue section 41 of the Privacy Act 1993 that allows an agency to extend the time limit for responding to the request. There are two issues of note. Firstly, section 41 of the Privacy Act 1993 allows an agency to extend the time limit if the request is for a large quantity of information. This has been omitted in clause 51 of the Bill and should be restored.

4.36 Secondly, an amendment in clause 51 to implement a Law Commission recommendation[117] should be mirrored in clause 71 (if two provisions are retained). A new justification for an agency to extend the time limit is where the processing of the request gives rise to issues of such complexity that a response cannot reasonably be given within the original time limit.

4.37 The Law Commission did not confine the recommendation to access requests. Correction requests can also raise issues of complexity for agencies that may justify a time extension, although less often than access requests. I recommend that the amendment extend to correction requests as well as to access requests.

[117] NZLC R123, R29.

RECOMMENDATION B.4.6

Clause 51 should be amended to include requests for a large quantity of information.

If retained, clause 71 should be amended for consistency with new clause 51(1)(c).

Clause 52(1)(a)(i): Endangering the safety of an individual

4.38 This clause continues the refusal ground that allows an agency to refuse an access request if releasing the information would create a danger to the safety of any person. The Law Commission recommended that the refusal ground to protect individual safety be broadened so that an agency may refuse access if disclosure would be likely to present a serious threat to public health or safety, or to the life or health of any individual.[118] Although included as a recommendation to be implemented in the supplementary government response,[119] this has not been included in the Bill, and I recommend that it should be.

4.39 The scope of the current safety ground in s 27(1)(d) of the Privacy Act (on which clause 52(1)(a)(i) is based) has been interpreted as being limited to a risk of physical harm.[120] The amendment proposed by the Law Commission would allow serious risks to mental and emotional safety as well as an individual's physical safety to justify a refusal of access to an individual.

4.40 It is timely to reform the scope of this provision, in light of recent developments such as the Harmful Digital Communications Act 2015 that specifically defines "serious emotional distress". The amendment proposed would also be consistent with the approach taken in the comparable Australian privacy principle.[121]

4.41 The new harassment refusal ground in clause 52(1)(a)(ii) and the new ground to protect victims from significant harm in clause 52(1)(a)(iii) will expand the grounds for refusing a request where there is a serious risk of harm to another individual. However, I support the additional recommendation to cover circumstances where the risk to mental and emotional safety does not fall within the category of harassment, or the person affected does not fall within the definition of a victim, but is serious enough to justify access being refused.

RECOMMENDATION B.4.7

Clause 52(1)(a)(i) should be amended to implement Law Commission recommendation 22.

[118] NZLC R 123, R22. This would align the refusal ground with the comparable IPP 11(1)(f) disclosure exception.
[119] Appendix A, Part A: recommendations to be implemented.
[120] *O v N* (1996); *M v Ministry of Health* [1997].
[121] Privacy Act 1988 (Cth), APP 12.3(a).

Clause 52(1)(c): Contrary to the interests of a person under the age of 16

4.42 This clause continues the access refusal ground from section 29(1)(d) of the Privacy Act 1993 that allows an agency to refuse an access request where disclosing the information would be contrary to the interests of a young person.

4.43 The provision has been inadvertently narrowed in the Bill by replacing "individual" with "requestor". This means that the ground could only be used to refuse access where contrary to the requestor's interests. It would no longer apply to refuse access where personal information is sought by another person on behalf of a young person, for example by a parent. It is necessary to retain the current scope of the provision by retaining the term "individual", rather than changing the term to "requestor".

RECOMMENDATION B.4.8

Clause 52(1)(c) should be amended to replace "requestor" with "individual" to preserve the scope of section 29(1)(d) of the Privacy Act 1993.

Clause 52(1)(d): Prejudice to safe custody and rehabilitation

4.44 This clause continues the access refusal ground from section 29(1)(e) of the Privacy Act 1993 that allows an agency to refuse an access request where disclosing the information would be likely to prejudice the safe custody or the rehabilitation of an individual.

4.45 The provision has been inadvertently narrowed in the Bill by replacing "individual" with "requestor". This means that the provision could only be used to refuse access to requestors whose safe custody or rehabilitation would be prejudiced. It would no longer apply to refuse access to information that is mixed personal information about the requestor and another individual, where providing access to that information to the requestor could prejudice the custody or rehabilitation of the other person. It is necessary to retain the current scope of the provision by retaining the term "individual", rather than changing the term to "requestor".

RECOMMENDATION B.4.9

Clause 52(1)(d) should be amended to replace "requestor" with "individual" to preserve the scope of section 29(1)(e) of the Privacy Act 1993.

Clause 57(b): Maintenance of the law

4.46 The Law Commission recommended that this refusal ground be narrowed (and aligned with the comparable IPP 11 disclosure exception) by limiting reliance on this ground to maintenance of the law "by a public sector agency".[122] Although included as a

[122] NZLC R123, R93.

recommendation to be implemented in the supplementary government response,[123] this has not been implemented in the Bill, and I recommend that it should be.

4.47 The scope of the current refusal ground in s 27(1)(c) of the Privacy Act (on which clause 57(b) is based) has been interpreted as only occasionally applying to private companies, usually where they act as a conduit of information from informants to the Police, such as insurance companies.[124] The proposed amendment would assist to clarify the scope of the refusal ground.

RECOMMENDATION B.4.10

Clause 57(b) should be amended to implement Law Commission recommendation 93.

Clause 57(h): Duress

4.48 The Law Commission recommended an amendment to deal with the problem of coerced access requests. The proposed amendment was a new obligation on agencies to withhold access if the agency has reasonable grounds for believing that access request was made under duress in the form of actual or threatened physical harm or psychological abuse.[125] The Law Commission suggested this could sit with other "precautionary" measures an agency needs to take before providing to access to information.[126]

4.49 Implementing this recommendation as a refusal ground in clause 57(h) of the Bill however does not meet the intent of the Law Commission's proposal. I recommend deleting clause 57(h) and instead amending clause 63 to give effect to the Law Commission's recommendation.

4.50 Adding a refusal ground creates discretion for the agency to refuse the request, but not an obligation to do so.[127] In addition, duress may not be evident at the time an agency makes a decision about the request, but may become evident when addressing the agency's responsibilities under clause 63. Conceptually, the issue does not sit comfortably in the refusal grounds, as this is an issue about the circumstances of the request, rather than the nature of the information being requested.

4.51 The Law Commission further recommended creating a complaint right for individuals in cases where an agency failed to comply.[128] Although included as a recommendation to be implemented in the supplementary government response,[129] this has not been implemented in the Bill, and I recommend that it should be.

[123] Appendix A, Part A: recommendations to be implemented.
[124] Privacy Commissioner Case Note 207459 [2009] NZPrivCmr 17.
[125] NZLC R123, R17.
[126] Privacy Act 1993, s 45, Privacy Bill, cl 63.
[127] *M v Ministry of Health* (1997) 4 HCNZ 79, p7.
[128] NZLC R123, R18.
[129] Appendix A, Part A: recommendations to be implemented.

4.52 Amending clause 63 to create an obligation on agencies not to release information in circumstances of duress would allow an agency's release of information in those circumstances to become a ground of complaint under clause 75(3)(c) of the Bill. It may be necessary to amend clause 75(3)(i) by deleting the words "in relation to the request". Clause 205 may also require amendment as a consequence.

RECOMMENDATION B.4.11

Clause 57(h) should be deleted. To implement Law Commission recommendation 17, clause 63 should be amended.

To implement Law Commission recommendation 18, clause 75(3) of the Bill should be reviewed to ensure that it provides a ground of complaint for an agency's breach of clause 63, as amended.

Clause 58: Conditions

4.53 This provision is new and confirms that conditions of access may be imposed as an alternative to refusing access.[130] The reference to "clause 57" in the clause title is inconsistent with clause content.

RECOMMENDATION B.4.12

The title of clause 58 should be amended by deleting "under section 57".

Clause 62: Ways information to be made available

4.54 This provision continues the right of individuals to express a preference for the form in which access to their personal information is provided to them. Options include a written or oral summary of the information, a transcript and options to view a video file or listen to a sound file.

4.55 The provision is modelled closely on section 16 of the Official Information Act 1982. However an update to the OIA provision was made in 2015 to add new section 16(1A):

Subject to subsections (2) and (3), information made available in any of the ways listed under subsection (1) may be made available in electronic form or by electronic means.

4.56 In my view, it is timely to update the provision. I recommend an amendment to clause 62 based on section 16(1A) of the Official Information Act.

4.57 In addition, I recommend that the clause include express options for an individual to request their personal information in machine readable format, and, where technically feasible, to have the information transferred to another agency. There is precedent for this option in the EU General Data Protection Regulation that entitles an individual to

[130] See Privacy Act 1993, s 66(2)(a)(iii).

receive their personal data in a structured, commonly used and machine-readable format and to have their personal data directly transferred to another entity.[131]

RECOMMENDATION B.4.13

Clause 63 should be amended to expressly include options for an individual to request their personal information be made available to them electronically and in machine readable format. Clause 63 should also entitle an individual to request that their personal information be transferred, where technically feasible, to another agency.

Clause 70: Decision on access request under IPP 7(2)(b)

4.58 This provision contains the process for an agency to attach a statement of correction to be read with an individual's personal information, where the agency refuses to correct the information itself on a request under IPP 7(1)(a). The clause title should be amended to reflect that an agency is required to take steps to attach a statement of correction, if a correction request has been refused. It does not require an agency decision about whether or not to grant the request to attach a statement. An alternative clause title would be "Statements of correction."

4.59 IPP 7(3) in the Privacy Act does not currently provide a timeframe for attaching a statement of correction and it would be useful to do so in the Bill. Clause 70(2) proposes that the statement should be attached within 20 working days of the agency receiving the request under IPP 7(2)(a). However, this proposed timeframe may be impractical in circumstances where a correction request under IPP 7(1)(a) and request to attach a statement under IPP 7(2)(b) in the alternative, are made together. 20 working days may have elapsed in making the initial decision on the correction request under IPP 7(1)(a) leaving no further time to attach the statement of correction.

4.60 In my view, the timeframe for attaching a statement of correction should simply be "as soon as practicable" after the decision under IPP7 (1)(a) or after receiving a request to attach the statement, if later. I recommend deleting "in any case not later than 20 working days after the day on which the correction request made under IPP 7(2)(b) is received".

RECOMMENDATION B.4.14

Clause 70 should be renamed "Statements of Correction."

Clause 70(2) should be amended by deleting "and in any case not later than 20 working days after the day on which the correction request made under IPP 7(2)(b) is received".

[131] EU GDPR, article 20, right to data portability.

Clause 72: Charging

4.61 Clause 72 of the Bill carries over current provisions relating to charging. The ability to charge varies depending on whether the agency concerned is a public sector or private sector agency. I recommend the following amendments to clause 72.

4.62 Firstly, the ready reference list for public sector agencies from section 35(1) should be retained, including the limit on charging for providing assistance. Although the limit on charging for assistance is now implied by clause 72(2), it is desirable to retain the express limitation.

4.63 Secondly, the express limits on public sector charging for making information available in response to an access request[132] and for attaching a statement of correction[133] have been moved to clause 72(3) as matters that a public sector agency may charge for if authorised to do so. However, the grounds for authorising charges for these actions are limited to the rare circumstance of commercial disadvantage. For clarity, these should remain on a full list of prohibited charges, subject to the exceptional circumstances of an authorisation.

4.64 Thirdly, an agency (whether public or private sector) may no longer charge for correcting information under IPP 7(1)(a).[134] This is not included in clause 72(1) and I recommend that it should be.

4.65 In summary, I recommend replacing clause 72(1)-(3) along the following lines:

(1) An agency may not impose a charge for –

(a) providing assistance in accordance with sections [47 or 67]; or

(b) receiving an access or correction request; or

(c) transferring an access or correction request to another agency; or

(d) correcting information in compliance in whole or in part with a request under IPP 7(1)(a).

(2) Subject to section [73], a public sector agency may not impose a charge for –

(a) making information available in whole or in part in compliance with an access request; or

(b) attaching a statement of correction in compliance with a request under IPP 7(2).

(3) A private sector agency may impose a charge for –

[132] Privacy Act 1993, s 35(1)(e).
[133] Privacy Act 1993, s 35(1)(f)(ii).
[134] NZLC R123, R28. Supplementary government response Appendix A, Part A recommendations to be implemented.

(a) making information available in compliance, in whole or in part with an access request:

(b) attaching a statement of correction in compliance with a request under IPP 7(2):

(c) providing assistance with an access request if the agency makes information available in compliance, in whole or in part, with an access request.

RECOMMENDATION B.4.15

Clause 72 should be redrafted to make clearer the matters for which an agency may or may not charge. An indicative provision is suggested.

Clause 73: Commissioner may authorise charge by public sector agency

4.66 This clause carries over section 36 of the Privacy Act that sets out the two instances in which the Privacy Commissioner may authorise a public sector agency to impose a charge (one relating to commercial disadvantage, and one relating to the nationality of the requestor).

4.67 The clause requires redrafting to reflect the independent authorisation grounds as contained in section 36 (1) and (1A) of the Privacy Act 1993. Clause 73(1) and (2) should reflect two separate grounds on which the Privacy Commissioner may authorise charging, that are not dependent on each other.

4.68 In addition, clause 73(1)(a) should be drafted consistently with clause 72(3)(a) and allow charging, if authorised, for making information available, rather than for granting an access request.

RECOMMENDATION B.4.16

Clause 73 should be redrafted to carry over the proper effect of section 36 of the Privacy Act 1993.

Privacy Commissioner's recommended reorganisation of Part 4 of the Bill

4.69 The following table below sets out the Commissioner's recommended reorganisation for Part 4 (recommendation B.4.1):

a) the left hand column represents the Commissioner's recommended structure and ordering of provisions for Part 4 in four subparts;

b) the middle column gives Bill clause references; and

c) the right hand column outlines the necessary amendments to reorganise Part 4.

Privacy Commissioner recommendation for proposed re-ordering of Part 4	Privacy Bill (current) subpart/clause	Recommended amendments to Bill clauses
Part 4(1) access to personal information	Subpart 4(1)	No change required.
44 Individuals may make access request	44	1. Replace clause 44(1) with the following: (1) In this subpart and subpart 4, access request means a request made by an individual to an agency under IPP 6 including a request under – (a) IPP 6(1)(a) to confirm the agency holds personal information about the requestor; (b) IPP 6(1)(b) to access the requester's personal information; (c) under IPP 6(1)(a) and (b). [Clause 45 can be deleted if covered by amended clause 44].
45 Urgency	46	No change required.
46 Assistance	47	Note submission recommendation B.4.2.
47 Decision on access request	49(1) and (2); 50(2),(5), (6)	1. In clause 49(1) delete: "made under IPP 6(1)(a)" 2. Replace clause 49(2) and 50(2) with the following: (2) Subject to subsection (3), a response must – (a) confirm that the agency holds personal information about the requestor and that access to some or all of the information is granted, including the way the Agency will make the information available, and the charge (if any) payable under section [68]; (b) confirm that the agency holds personal information about the requestor and access to some or all of the information is refused,

Privacy Commissioner recommendation for proposed re-ordering of Part 4	Privacy Bill (current) subpart/clause	Recommended amendments to Bill clauses
		including the reason for refusal and other matters under section [51]; (c) confirm that the agency does not hold personal information about the requestor; (d) state that the agency neither confirms not denies that it holds personal information about the requestor, in accordance with section [50]. 3. Add new subclause (3): (3) A response to an access request solely under IPP 6(1)(a) must confirm that the agency holds personal information about the requestor or does not hold personal information about the requestor
48 Agency may impose conditions instead of refusing access to information	58	Amend clause title – submission recommendation B.4.12.
49 Withholding information contained in a document	61(1)	No change required.
50 Neither confirm nor deny	49(3), 50(4), 59	Note submission recommendation B.4.4.
51 Reasons for refusal, grounds in support and informing of right of complaint	60, 61(2)-(4)	1. Amend title of clause 60. 2. Replace clause 60(1) with the following: "(1) Subject to clause [50], this section applies if an agency – (a) refuses access to information under section [47(2)(b)]; or (b) grants access to information contained in a document with deletions or alterations under section [49]." 3. Replace clause 60(2) with the following: (2) The agency must inform the requester of – (a) the reason for the refusal or decision under subsection (1); and

Privacy Commissioner recommendation for proposed re-ordering of Part 4	Privacy Bill (current) subpart/clause	Recommended amendments to Bill clauses
		(b) the requestor's right to make a complaint to the Commissioner in respect of that refusal or decision. 4. In clause 60(4)(b) replace "sections 52, 54 and 57(e) to (i)" with updated clause reference to clauses 52, 54 and all of clause 57. 5. Delete clause 61(2)-(4).
52 Refusal not permitted for any other reason	50(3)	Note submission recommendation B.4.5.
53 Ways information to be made available	62	Note submission recommendation B.4.13.
54 Responsibilities of agency before giving access to information	63	Note submission recommendation B.4.11.
Part 4(2) Good reasons for refusing access to personal information	Part 4(1)	New subpart heading
55 Protection etc. of individual	52	Amend clause heading
56 Evaluative material	53	Amend clause heading
57 Maintenance of the law, privilege etc.	57	Amend clause heading.
58 Security, defence, international relations	54	Amend clause heading
59 Trade secret	55	Amend clause heading
60 Administrative reasons for refusing request	56	Amend clause heading
Part 4(3) Correction of personal information	Part 4(2)	Update numbering of subpart.
61 Individual may make correction request	64	For consistency with IPP 7(2), replace clause 64(1) with the following: "In this subpart and subpart 4, correction request means any request by a requester to an agency – (a) under IPP 7(1)(a) to correct personal

Privacy Commissioner recommendation for proposed re-ordering of Part 4	Privacy Bill (current) subpart/clause	Recommended amendments to Bill clauses
		information about the requestor; or (b) under IPP 7(1)(b) to attach a statement of correction; or (c) under IPP 7(1)(a) and 7(1)(b) to correct personal information about the requestor or, if the agency is not willing to correct the information, to attach a statement of correction." [Clause 65 can be deleted if covered by amended clause 64(1).]
62 Urgency	66	No change required.
63 Assistance	67	Note submission recommendation B.4.2.
64 Decision on request under IPP 7(1)(a)	69	No change required.
65 Decision on request under IPP 7(2)	70	Note submission recommendation B.4.14.
Part 4(4) Transfer, extension of time limit and charges	Part 4(3)	New heading for subpart.
66 Transfer of access or correction request	48, 68	Minor adjustments to extend clause 48(1) and (2) to both access and correction requests, delete clause 68. Note submission recommendation B.4.3.
67 Extension of time limits	51, 71	Minor adjustments to extend clause 51 to both access and correction requests, delete clause 71. Note submission recommendation B.4.6.
68 Charges	72	Note submission recommendation B.4.15.
69 Commissioner may authorise public sector agency to impose charge	73	Note submission recommendation B.4.16.

PART 5 – Complaints, investigations and proceedings

5.1 Part 5 of the Bill carries over Parts 8 and 9 of the Privacy Act 1993 that contain the procedures relating to complaints about interference with privacy. This includes the provisions relating to the making of complaints, the Commissioner's complaint functions, that include resolution, investigation and referral to the Director of Human Rights Proceedings and provision in relation to proceedings before the Human Rights Review Tribunal in relation to complaints.

5.2 Part 5 also includes various enhancements to the complaint's processes. The most significant enhancement is the Commissioner's new discretionary power to issue a binding direction that an individual be given access to their personal information.[135] An access direction can be appealed to the Tribunal.[136] Access directions may, if necessary, be enforced by the individual applying to the Tribunal for an access order.[137]

5.3 I support these reforms and consider this will help ensure more efficient resolution of complaints that is advantageous to both parties.

5.4 An outstanding recommendation that has not been implemented in the Bill is for the role of the Director of Human Rights Proceedings to be brought within the Office of the Privacy Commissioner.[138] In Part A of my submission I submit that this recommendation should be implemented in the Bill.

Clause by clause comments

5.5 In this part of the submission I comment and make recommendations on the carrying over of the existing provisions governing the complaint processes so as to correct inadvertent changes and ensure the provisions retain their current effect. I also make recommendations in respect of the implementation of new reforms.

5.6 I note that the complaints function is one of the core functions of my Office and the effectiveness and efficiency of the process is important in protecting individuals' privacy. The complaints regime has purposely been designed to be deliberately flexible and it is important that the carryover of the regime retains does not inadvertently lose any of that flexibility.

5.7 This flexibility is essential for efficiency and effectiveness given the varied nature of privacy complaints that can involve a myriad of circumstances and can be multifaceted, involving more than one type of interference and information privacy principle. Complaints may also involve more than one individual and can be brought by a representative on behalf of one or more individuals, including a class of individuals.

[135] Privacy Bill, cl 96. See NZLC R123, R56- 59.
[136] Privacy Bill, cl 110.
[137] Privacy Bill, cl 109.
[138] NZLC R123, R55.

5.8 The wide discretion in process allows the process to be tailored as necessary to ensure a matter is dealt with efficiently and this may include taking different tracks at different times with each aspect. For example, a complaint may involve two separate alleged interferences with privacy - that the individual's personal information was wrongly disclosed (a breach of IPP 11) and that the agency wrongly refused the individuals request to access their personal information (a breach of IPP 6). I may be able to settle the disclosure aspect (IPP 11) of the complaint but not the access aspect (IPP 6) and it may be necessary to make a decision on an aspect and/or a binding access direction (either before or after the other aspect has been settled).

Clause 74: Interpretation

5.9 This clause provides specific definitions for Part 5 and therefore will apply in respect of the whole complaint process, including investigations and proceedings in the Tribunal. The definitions must be sufficiently broad or extensive to account for the varied nature of complaints, including those brought by a representative on behalf of a class of aggrieved individuals (as further discussed below in relation to clauses 77, 80, 86 and 103).

5.10 I recommend amendments to three of the definitions – "aggrieved individual", "complainant", and "parties".

5.11 The definition of an "aggrieved individual" applies only to a complaint under subpart 1 and an investigation under subpart 2. The term "aggrieved individual" is however also used extensively in subpart 5(3) - Proceedings before Human Rights Review. Accordingly the definition should also expressly refer to subpart 3. I recommend the definition of "aggrieved individual" should be amended to include (c) a proceeding under subpart 3.

5.12 The definition of "complainant" includes any person whom made a complaint, that includes an aggrieved individual and a representative of 1 or more aggrieved individuals (clause 77 refers). The definition is however currently too narrow in that it refers to "the individual who made the complaint" and therefore does not provide for complaints that may be brought by a representative that is not an individual, for example an incorporated society on behalf of a class of individuals.[139] I recommend the definition be amended by replacing "individual" with "person" (whereby the broader definition in the Interpretation Act 1999 will apply which includes corporate and unincorporated bodies.)

5.13 The definition of "parties" provides separately both for investigations conducted by the Commissioner (a) on receiving a complaint and (b) on the Commissioner's own initiative. The part of the definition, (a), in respect of investigations conducted on receiving a complaint currently includes as parties both the complainant and the aggrieved individual (if not the complainant), as well as the respondent. It is however not appropriate, nor necessary, for a complainant that is not an aggrieved individual to be a party to investigation in addition to the aggrieved individual. For example, a lawyer

[139] See for example *Child Poverty Action Group Inc. v Attorney-General* [2013] NZCA 402 where an incorporated society brought a representative complaint and consequential proceedings on behalf of a class of individuals under Part1A of the Human Rights Act 1993.

representing an aggrieved individual should not be party to the investigation, only the aggrieved individual. The only circumstance where it may be appropriate for a complainant to be a party to the investigation is when the complaint is a representative complaint brought on behalf of a class of aggrieved individuals. I recommend the definition should be amended by deleting (a)(i) and including in (a)(ii) the words "or the representative of a complaint brought on behalf of a class of aggrieved individuals."

RECOMMENDATION B.5.1

Clause 74 definition of "aggrieved individual" should be amended by adding the following text "(c) a proceeding under subpart 2 of this Part."

Clause 74 definition of "complainant" should be amended by replacing the word "individual" with the word "person".

Clause 74 definition of "parties" should be amended by deleting (a)(i) and including in (a)(ii) the words "or the representative of a complaint brought on behalf of a class of aggrieved individuals."

Clause 77: Who may make complaint

5.14 This provision makes explicit that a representative may bring a complaint on behalf of one or more individuals whose privacy has been breached (referred to as "aggrieved individuals"). This implements a Law Commission recommendation that the Privacy Act should specifically provide for representative complaints brought on behalf of a class of aggrieved individuals, and supporting details.[140]

5.15 I recommend that, for the purposes of clarity, this provision should expressly refer to complaints brought on behalf of a class of aggrieved individuals. Clause 77(1)(b) should be amended by adding the words "or a representative of a class of aggrieved individuals."

5.16 To properly implement this recommendation, other amendments have been recommended to various clauses, including those noted above, to ensure representative complaints in respect of a class of aggrieved individuals are expressly provided for throughout the whole of the complaints process.

RECOMMENDATION B.5.2

Clause 77 should be amended by adding to (1)(b) the words "or a representative of a class of aggrieved individuals."

Clause 80: Commissioner may decide not to investigate

5.17 Clause 80 sets out the grounds on which the Commissioner may exercise the discretion not to investigate a complaint. New grounds are included in clause 80(a) and 80(e).[141]

[140] NZLC R123, R60.
[141] *Necessary and Desirable*, recommendations 106, 104A.

5.18 I recommend a further amendment to align with the discretion in clause 88(3)(b). That provision allows the Privacy Commissioner to decline to further investigate a complaint where any further action is considered unnecessary or inappropriate. I recommend that this refusal ground should also apply before the commencement of an investigation. This is consistent with a 2015 amendment to the Ombudsman Act.[142]

5.19 Clauses 80(a) provides the discretion for the Commissioner not to investigate a complaint if there has not been reasonable efforts made to resolve the complaint with the agency concerned. The clause refers to "the complainant" not having made reasonable efforts which is not always apt in this context given complainant is defined to include a representative of an aggrieved individual. The policy intent of the clause can be maintained by removing the reference to "complainant". I recommend clause 80(a) should be amended to remove the reference to "complainant" by replacing the words "the complainant has not" with the words "there has not been".

5.20 Clause 80(b) provides the discretion for the Commissioner not to investigate a complaint if there is an alternative dispute resolution process available because of the agency's membership of a particular profession or industry. This clause also refers to "the complainant" which is problematic for the reason described above. The policy intent of the clause can be maintained by removing the reference to "complainant". I recommend clause 80(b) should be amended to remove the reference to "complainant" by deleting the words "to the complainant".

5.21 Clause 80 (e) provides for the discretion for the Commissioner not to investigate a complaint where the complainant knew about the action that is the subject of the complaint for 12 months or more before making the complaint. The reference to "complainant" here is similarly problematic given it will include a representative of an aggrieved individual (whom may have only recently been advised of the action at issue). To maintain the policy intent of the clause it should refer solely to aggrieved individual. I recommend clause 80(e) should be amended by replacing the word "complainant" with "aggrieved individual".

RECOMMENDATION B.5.3

Clause 80 should be amended to provide that the Commissioner may decide not to investigate a complaint if he or she considers in the circumstances, following preliminary inquiries, that any action is unnecessary or inappropriate.

Clause 80(a) should be amended by replacing the words "the complainant has not" with the words "there has not been".

Clause 80(b) should be amended by deleting the words "to the complainant".

Clause 80(e) should be amended by replacing the word "complainant" with "aggrieved individual".

[142] Ombudsman Act 1975, s 17(1)(f).

Clauses 80(a) and 81: Commissioner may decide not to investigate or to defer taking action on complaint

5.22 These new provisions implement a recommendation of the first Privacy Commissioner,[143] to provide discretion not to investigate or to defer an investigation where the Commissioner considers the complainant has not made reasonable efforts to first resolve the complaint directly with the agency concerned.

5.23 In my view, implementation of the reform in clause 80(a) is sufficient, and it is unnecessary to also include clause 81. A complaint declined under clause 80(a) can be raised again with the Commissioner, once the complainant has made reasonable efforts to resolve it with the agency concerned. That is a more efficient process than deferring an investigation. The option of a two-track complaint consideration process would introduce unnecessary complexity, and I recommend deleting clause 81. As a consequence, clause 79(1)(b) should also be deleted.

RECOMMENDATION B.5.4

Clause 81 should be deleted. As a consequence, clause 79(1)(b) should also be deleted.

Clause 82: Referral of complaint to another person

5.24 This provision carries over current provisions in the Privacy Act that allow the Privacy Commissioner to refer a complaint to another body, as appropriate. The Independent Police Complaints Authority is now included as one of the bodies a complaint can be referred to.[144]

5.25 A further amendment to clause 82(1) is required to clarify that the referral to another body may arise not only on receipt of the complaint, but also at any time during an investigation by the Privacy Commissioner, as relevant facts come to light. I recommend replacing the words “on receiving a complaint” with the words “at any time after receiving a complaint.”

RECOMMENDATION B.5.5

Clause 82(1) should be amended to replace the words “on receiving a complaint” with the words “at any time after receiving a complaint.”

Clauses 84(2)(b) and 87(3)(b)

5.26 Clause 84 provides for the possibility of settlement and assurance prior to investigating a complaint and clause 87 provides for that possibility during investigation. Both clauses also provide discretion for the Commissioner to refer a complaint to the Director in the

[143] Necessary and Desirable, recommendation 106.
[144] Necessary and Desirable, recommendation 107.

various circumstances set out in clauses 84(2) and 87(3). Those circumstances include in clause 84(2)(b) and 87(3)(b) where it appears that a term of settlement previously secured between the agency and complainant has not been complied with. The term "complainant" is inapt in this context (given it is defined to include a representative of an aggrieved individual) and should be replaced with aggrieved individual. I recommend clauses 84(2)(b) and 87(3)(b) should be amended by replacing the word "complainant" with "aggrieved individual".

RECOMMENDATION B.5.6

Clauses 84(2)(b) and 87(3)(b) should be amended by replacing the word "complainant" with "aggrieved individual".

Clause 86: Commencing investigation

5.27 This clause provides that the first step of an investigation must be notification to the parties and sets out the notice requirements. Clause 86(1) provides whom must be notified and is both unnecessarily complex and inapt in respect of complaints made by a representative, including in particular those on behalf of a class of aggrieved individuals. To simplify the clause whilst meeting its purpose and for consistency with the approach taken in clause 88(4), I recommend clause 86(1) be amended by deleting clauses 86(1)(a) and (b) and replacing the words "the following persons" with "the parties".

RECOMMENDATION B.5.7

Clause 86(1) should be amended by deleting clauses 86(1)(a) and (b) and replacing the words "the following persons" with "the parties".

Clause 96: Procedure after completion of investigation relating to breach of IPP 6

5.28 This provision details the procedure to be followed by the Commissioner after an investigation relating to a breach of IPP6. This includes the Commissioner's new discretionary power to issue a binding direction that an individual be given access to their personal information (an access direction).

Access directions requirements – should be in separate standalone provision

5.29 The ability for the Commissioner to make an access direction is a significant new development and should be more prominent and accessible in the statutory scheme. In my view it is deserving of its own separate provision for the purposes of clarity and accessibility.

5.30 Accordingly I recommend the details relating to access directions in clauses 96(7), 96(8)(c) and 96(9) be put in a new separate provision - Clause 96A, entitled "Commissioner may make access direction." In addition the reference in 96(7)(b) and (c) to "complainant" is inapt in this context and needs to be replaced with "aggrieved individual".

5.31 In addition, to ensure efficiency and effectiveness, the Bill should expressly provide that access directions can be varied or cancelled by the Commissioner (similar to the ability to vary or cancel a compliance notice in clause 128).

5.32 Accordingly, I recommend that new clause 96A provides that the Commissioner may vary or cancel an access direction at any time if he or she considers (a) any of the information specified needs to be added to or amended in the direction; or (b) the particular way in which specified information is to be made available needs to be amended; or (c) all or part of the notice is no longer needed.

5.33 A consequential amendment to clause 95(5)(a) would also be required to refer to new clause 96A.

Amendments to remainder of clause 96

5.34 In respect of the remainder of clause 96, I consider this needs simplifying to ensure it properly carries over the relevant provisions in the current Act that provide necessary flexibility for efficiency and effectiveness of investigations.

5.35 Firstly, this should include removing references to "completed" and "completion" in this clause, as it can lead to confusion given investigations are not always completed in the traditional sense before the steps set out in clause 96 would occur (for example settlement, making access direction or taking any other action). The current wording may imply more formality is required in the complaint process than is necessary or appropriate. It is therefore preferable to revert to wording closer to that in section 77 of the current Act that is entitled "Procedure after investigation" and uses the phrase "after making any investigation".[145]

5.36 Accordingly, the title of clause 96 should be amended by deleting the words "completion of" so it refers to "Procedure after investigation relating to breach of IPP 6". Clause 96(1) should be amended by deleting the words "completed an" and replacing these with "made any".

5.37 Secondly, this should include deleting clause 96(2) and amending clause 96(8). Clause 96(2) appears redundant given the requirements in clauses 96(3) and (4). Further, retaining clause 96(2) could lead to unnecessary confusion given its reference to a determination that a complaint either "has substance" or "does not have substance". This combined with the requirement in clause 96(8)(a) to given notice of this determination appears to inadvertently implement a new obligation for the Commissioner to give reasons when a complaint is settled or mediated.

5.38 The notice requirement in clause 96(8) is unnecessary and suggests a level of unnecessary formality, not currently required under the current Act (s 75 provides that the parties be informed of the result of investigation after conclusion and in such manner as the Commissioner thinks proper). The status quo is simple and clear and should be

[145] Privacy Act 1993, s 77(1).

reverted to. The requirements for a notice of an access direction will be separately included in clause 96A.

5.39 I recommend clause 96(8) should be deleted and replaced with the following; "As soon as practicable, the Commissioner must inform the parties of the result of the investigation, including any action taken under (5) or (6)."

RECOMMENDATION B.5.8

Clauses 96(7), 96(8)(c) and 96(9) should be removed into a separate stand-alone clause - clause 96A entitled "Commissioner may make access direction", and a consequential amendment to clause 96(5)(a) so it refers to clause 96A;

The remainder of clause 96 should be amended as follows:

The title should be amended by deleting the words "completion of" so it refers to "Procedure after investigation relating to breach of IPP 6";

Clause 96(1) should by amended by replacing the words "completed an" with "made any";

Clause 96(2) should be deleted;

Clause 96(8) should be replaced with the following; "As soon as practicable, the Commissioner must inform the parties of the result of the investigation, including any action taken under (5) or (6)."

RECOMMENDATION B.5.9

There should be a new Clause 96A that provides for the making of an access direction and is entitled "Commissioner may make access direction".

Clause 96A should include the requirements for a notice of an access direction currently in clauses 96(7), 96(8)(c) and 96(9).

Clause 96A should also provide that the Commissioner may vary or cancel an access direction at any time if he or she considers (a) any of the information specified needs to be added to or amended in the direction; or (b) the particular way in which specified information is to be made available needs to be amended; or (c) all or part of the notice is no longer needed.

Consequential amendments will need to be made to clauses 109 to 112 so these refer to new clause 96A.

Clause 97: Procedures after completion of investigation relating to charging

5.40 Clause 97 carries over the Commissioner's current power to make determinations about the reasonableness of a proposed charge, expanded to now include all charging complaints.[146] These determinations are final and there is no right of appeal.

5.41 Clause 97(6) would now allow the individual to bring proceedings in the Tribunal under IPP 6 where an agency refuses to comply with a charging determination. However, this clause is not only unnecessary but also confusing it that it suggests the Commissioner's decision on charging is not final.

5.42 The Bill does not need to make special provision for enforcement of the Commissioner's charging determinations, as charging is integrally linked to an individual's right of access under IPP 6. If an agency refuses to provide access to the information, that refusal will potentially be an interference with the privacy of an individual under clause 75(3). The appropriate process, before commencing proceedings in the Tribunal, is for the complainant to make a complaint to my Office (if they have not already done so). The new access direction power could be used to uphold the individual's right of access.

5.43 I recommend that clause 97(6) should be deleted, with consequential deletions of clauses 103(1)(g) and 103(6).

5.44 Clause 97 should also be amended by removing references to "completed" and "completion" in this clause for the reasons discussed in relation to clause 96 above. The clause should revert to wording more similar to that in the current Act section 78 that is entitled "Procedure in relation to charging" and that refers in section 78(1) to "after making any investigation".

5.45 I recommend the title of clause 97 be amended by deleting the words "completion of" so it refers to "Procedure after investigation relating to charging". And, clause 97(1) should be amended by deleting the words "completed an" and replacing these with "made any".

RECOMMENDATION B.5.10

Clauses 97(6), 103(1)(g) and 103(6) should be deleted.

Clause 97 should be amended by deleting the words "completion of" in the title so it refers to "Procedure after investigation relating to charging".

Clause 97(1) should by amended by replacing the words "completed an" with "made any".

Clauses 98

5.46 Clause 98 should also be amended by removing references to "completed" and "completion" in this clause for the reasons discussed in relation to clause 96 above and

[146] Necessary and Desirable, recommendation 110.

for consistency.

5.47 I recommend the title of clause 98 be amended by deleting the words "completion of" so it refers to "Procedure after investigation relating to charging". And, clause 98(1) should be amended by deleting the words "completed an" and replacing these with "made any".

RECOMMENDATION B.5.11

Clause 98 should be amended by deleting the words "completion of" in the title so it refers to "Procedure after investigation relating to charging";

Clause 98(1) should by amended by replacing the words "completed an" with "made any".

Clause 99

5.48 Clause 99 similarly needs simplifying for the same reasons as discussed above in relation to clause 96, to ensure it properly carries over the relevant provisions in the current Act that provide necessary flexibility for efficiency and effectiveness of investigations.

5.49 Accordingly I recommend clause 99 should be simplified in the same manner as clause 96 as follows.

5.50 The title of clause 99 should be amended by deleting the words "completion of" so it refers to "Procedure after other investigations".

5.51 Clause 99(1) should be deleted and replaced with the following "The section applies after the Commissioner has made any investigation under this subpart, other than an investigation to which sections 96, 97 or 98 applies."

5.52 Clause 99(8) should be deleted and replaced with the following; "As soon as practicable, the Commissioner must inform the parties of the result of the investigation, including any action taken under (4)."

RECOMMENDATION B.5.12

Clause 99 should be amended by deleting the words "completion of" in the title so it refers to "Procedure after other investigations".

5.53 Clause 99(1) should be deleted and replaced the following "The section applies after the Commissioner has made any investigation under this subpart, other than an investigation to which sections 96, 97 or 98 applies."

5.54 Clause 99(8) should be deleted and replaced with the following; "As soon as practicable, the Commissioner must inform the parties of the result of the investigation, including any action taken under (4)."

Clause 100(2)

5.55 Clause 100(2) should be amended by replacing the word "completing" with "making" for the reasons discussed in relation to clause 96 above and for consistency.

5.56 I recommend that clause 100(2) should be amended by replacing the word "completing" with "making".

RECOMMENDATION B.5.13

Clause 100(2) should be amended by replacing the word "completing" with "making".

Clause 102: Director may commence proceedings in Tribunal

5.57 Clause 102 provides the Director's process following a referral by the Commissioner. As referral can occur prior, during or after to an investigation (clauses 84, 87, 96 and 99) it is necessary to amend the clause to ensure it provides for referral at each stage.

5.58 Accordingly, I recommend clause 102(1) be amended to include references to clauses 84 and 87 and clause 102(2)(b)(iii) be amended by deleting the words "Commissioner's investigation" and replacing these with "complaint or matter".

RECOMMENDATION B.5.14

Clause 102(1) should be amended to include references to clauses 84 and 87.

Clause 102(2)(b)(iii) should be amended by deleting the words "Commissioner's investigation" and replacing these with "complaint or matter".

Clause 103: Aggrieved individual may commence proceedings in Tribunal

5.59 Clause 103 provides for when an aggrieved individual may bring proceedings and carries over section 83 of the current Act.

5.60 The clause does not clearly provide for the bringing of proceedings by a representative of a class of aggrieved individuals. This is because it refers solely to "aggrieved individual" throughout the clause.

5.61 To accommodate proceedings brought by a representative of a class of aggrieved individuals, I recommend the following amendments.

5.62 Clause 103 (1) should include after the words "aggrieved individual" the words "or the representative of a class of aggrieved individuals."

5.63 Clauses 103(2)-(8) inclusive should be amended by the replacing the words "An aggrieved individual" with "A person".

5.64 Clause 103(9)(a) should be amended by including after the words "aggrieved individual" the words "or the representative of a class of aggrieved individuals."

RECOMMENDATION B.5.15

Clause 103 (1) should include after the words "aggrieved individual" the words "or the representative of a class of aggrieved individuals."

Clauses 103(2)-(8) inclusive should be amended by replacing the words "An aggrieved individual" with "A person".

Clause 103(9)(a) should be amended by including after the words "aggrieved individual" the words "or the representative of a class of aggrieved individuals."

Clause 109: Enforcement of direction made by Commissioner under section 96(5)(a) after investigation of IPP 6 breach

5.65 This provision provides for the enforcement of an access direction by way of application to the Tribunal for an access order. I consider it is unnecessarily complex to provide the circumstances in which an access order can be sought in two separate sub-clauses. I recommend the clause be simplified by amalgamating clauses 109(1) and (2).

RECOMMENDATION B.5.16

Clause 109 should be amended by amalgamating clauses 109(1) and 109(2).

Clause 110: Appeal to Tribunal against direction of Commissioner under section 96(5)(a)

5.66 This provision provides for the respondent agency that receives a direction notice to appeal to the Tribunal against the access direction. The provision currently refers to "an agency" and it is recommended for clarity that the clause expressly refers to the respondent (this term is defined in clause 74). I recommend that clause 110(1) be amended by deleting "An agency" and replacing it with "A respondent".

RECOMMENDATION B.5.17

Clause 110(1) should be amended by deleting "An agency" and replacing it with "A respondent".

Clause 111: Time for lodging appeal

5.67 This provision provides the time period for lodging an appeal from an access direction. An appeal must be brought within 20 working days unless there are exceptional circumstances preventing the appeal being brought within the appeal period, then the Tribunal may accept an appeal within 3 months after the appeal period (a late appeal). The provision does not make clear that the Tribunal must give express permission before accepting an appeal in the discretionary extended period. For clarity and

efficiency the provision should clarify that express permission or leave must be sought from the Tribunal to accept a late appeal. I recommend clause 111(2) be amended to clarify that express permission or leave must be sought from the Tribunal to accept a late appeal.

RECOMMENDATION B.5.18

Clause 111(2) should be amended to clarify that express permission or leave must be sought from the Tribunal to accept a late appeal.

Clause 114: Determination of appeal

5.68 This provision provides how the Tribunal is to determine an appeal. It includes in clause 114(1) that for the purposes of an appeal the Tribunal may require the Commissioner to provide either a written report setting out relevant considerations (clause 114(1)(a)) or any information held by the Commissioner that is required to determine the appeal (clause 114(1)(b)).

5.69 I am concerned that the latter requirement could undermine complainants and respondent agencies' trust that their material or documents provided for an investigation is not provided to third parties. The Tribunal can already ask for information, such as it sometimes does - for example for further explanation on a matter. It is also preferable for the parties to the appeal to provide the information required, rather than the Commissioner. The written report should be sufficient.

RECOMMENDATION B.5.19

Clause 114(1)(b) should be deleted.

PART 6 – Mandatory breach notification and compliance notices

Notifiable privacy breaches and compliance notices

6.1 Part 6 introduces two significant new compliance features to New Zealand's privacy law being:

a) notifiable privacy breaches (subpart 1); and
b) compliance notices (subpart 2).

6.2 I support these two features and see them as critical in making the law more effective in ensuring accountability by agencies in their handling of personal information, protecting the interests of individuals and efficiently enforcing compliance. Both approaches are now seen as standard in modern privacy laws and align with international best practice for privacy regulation.

6.3 My submission makes a number of suggestions to improve workability, enhance individual rights and better achieve the aims of the legislation.

SUBPART 6(1) - Notifiable privacy breaches

6.4 The Law Commission recommended the adoption of mandatory breach notification in 2011 having reflected upon experience up to that date on a voluntary and mandatory basis in other jurisdictions[147] and analysing how useful that might be in New Zealand conditions. Since then the case has become stronger with:

a) mandatory breach notification having been legislated for in many similar jurisdictions including, in the last 3 years alone, Australia,[148] Canada[149] and throughout the European Union;[150] and
b) the practice having been recommended by both the OECD (2013)[151] and APEC (2015)[152] for inclusion in domestic privacy laws.

6.5 I strongly advocate that mandatory breach notification should be enacted and I support subpart 6(1) as a suitable approach. My submission seeks to improve aspects of the subpart.

6.6 Before commenting clause-by-clause, I first raise issues relating to clarifying the position of processors, including a duty to minimise harm, and providing for follow up reporting.

Imposing a clear duty upon processors that become aware of a breach

6.7 International instruments on privacy, and the privacy laws of many other countries particularly in Europe, differentiate between organisations they term information or data 'controllers' and those they call information or data 'processors'.[153] The Bill also makes a distinction between these two types of organisation in clause 8 but does not use the controller/processor terminology instead referring to both as 'agencies'.

6.8 The Bill provides in clause 8 that where an agency is simply processing information, or holding information for the purpose of safe keeping, on behalf of another agency (let's call them the 'processor' for this discussion) the information is deemed to be held by that other agency (which we refer to in this discussion as the 'controller').[154] Clause 8 is a neat drafting solution that has worked reasonably well in the existing Act without the need to unduly complicate the law with different terms for different types of agency as

[147] NZLC 123, R67.
[148] Privacy Act 1988 (Cth), Part IIIC.
[149] Personal Information Protection and Electronic Documents Act 2000 (Canada), section 10.1.
[150] GDPR, articles 33 and 34.
[151] OECD Privacy Guidelines (2013), clause 15(c).
[152] APEC Privacy Framework (2015), clause 54.
[153] For a discussion of the difference between controllers and processors in EU law, see: Information Commissioner's Office (UK), Data controllers and data processors: what the difference is and what the governance implications are.
[154] Although we use the controller/processor language to clarify this part of the discussion we do not seek a change to the Bill's adoption of the term 'agency' which has been embedded in New Zealand's privacy law since 1993. As we propose in the recommendation, it is possible to address the processor issue using the language in clause 8.

would be the case if the controller/processor terminology were to be adopted. However, to ensure a comprehensive and effective mandatory breach notification scheme it is desirable explicitly to set out a key duty on processors. This is one context where simply deeming the information to be held by the controller is not sufficient.

6.9 It is reasonable to start with the following two assumptions:

a) it will always be appropriate that the controller take all the key decisions (e.g. deciding a breach is notifiable), and to be responsible for the core breach notification obligations (e.g. notifying affected individuals), in relation to a breach affecting the controller's information; and
b) conversely, it will be inappropriate for the processor to take any key decisions or, of its own volition, to perform the core breach notification obligations in relation to the controller's information (although the processor may render critical assistance to the controller in various aspects of detecting, containing and rectifying breaches).

6.10 If those were the only two considerations then the regular approach taken in clause 8 would work well. However, a further consideration is that some breaches will become apparent first to the processor and may become apparent to the controller only much later. Indeed, some breaches apparent to the processor might only come to the attention of the controller when affected individuals report harmful effects.

6.11 In this scenario the notifications required under law will only occur promptly, and in some cases at all, if the processor takes the essential step of reporting what it has discovered to the controller. Part 6(1) does not oblige the processor to take that step and we submit that it should. Clause 8 does not resolve this issue but may simply have the effect of attributing the processor's inaction to the controller in terms of liability. However, the objective is to ensure that notification to an affected individual is promptly made and not simply to hold someone liable if notification is neglected or much delayed.

6.12 The EU GDPR addresses this issue in article 33(2) when it simply provides:

> *"The processor shall notify the controller without undue delay after becoming aware of a personal data breach".*

6.13 A processor's failure to meet that obligation renders it liable to an administrative fine of up to €10 million or up to 2% of an undertaking's worldwide annual turnover.[155]

6.14 I submit that a similar duty on agencies processing information or providing safe custody of information on behalf of other agencies is needed in subpart 6(1).

6.15 In terms of redress or enforceability, a failure to meet this obligation could be an interference with privacy (akin to a failure to notify the individual: clause 120(5)), an offence (akin to a failure to notify the Privacy Commissioner: clause 122) or, to adopt an

[155] GDPR, article 83(4)(a).

approach not currently provided for in the Bill, a failure to meet a statutory duty that is subject to a civil penalty.[156]

6.16 Imposing the duty will also mean that the Privacy Commissioner's compliance notice powers under clause 124 will be available in the event that non-compliance was discovered and the processor did not promptly rectify the situation. I favour the use of civil penalties which is also consistent with the 'administrative fine' approach of the EU GDPR.

RECOMMENDATION B.6.1

The mandatory privacy breach notification scheme in subpart 6(1) should include an express obligation on an agency processing personal information or providing safe custody of information on behalf of another agency to notify that other agency without undue delay after becoming aware of a privacy breach affecting the information.

Inclusion of a duty upon agencies to minimise downstream harm

6.17 Subpart 6(1) does not include any clear duties upon agencies to take reasonable steps to minimise the risks to affected individuals for information it no longer holds. The information security principle, IPP 5, extends only to information held by the agency. Clause 121(1)(b) and (2)(b) require an agency to explain the steps it has taken or intends to take in response to the breach, but does not explicitly require the agency to take mitigating steps. In the absence of a statutory duty the Privacy Commissioner would not be able to issue a compliance notice requiring such a step even if it were to be a simple and obvious step for the agency to take.[157] I submit that there should be such a duty.

6.18 Notification will enable affected individuals to take what steps they can to mitigate any harm resulting from the breach. This is clear from clause 121(2)(c) which provides that the notice to the individual must:

> *"Where practicable, set out the steps the affected individual may wish to take to mitigate or avoid potential loss or harm (if any)." [Emphasis added.]*

6.19 While involvement of the individual in mitigation is essential, the agency may also be well placed to take steps to minimise potential downstream harm to affected individuals whose information has already been lost. Subpart 6(1) does not clearly oblige the agency to take any such steps and I submit that it should. Such steps will differ from steps to contain the breach and limit ongoing harm to information still held within the system (e.g. to initiate password changes for compromised accounts) which can be inferred to be general obligations under IPP 5. Referring here to reasonable steps are steps to protect the interests of individuals whose information is no longer within the control of the agency.

[156] See recommendation A.1.
[157] Clause 124 powers to issue a compliance notice are premised upon "a breach of this Act" etc.

6.20 In some cases, especially in the early phases of managing the results of a breach, the agency may be in a better position than an affected individual to act effectively because:

a) the agency's understanding of the breach and the general risks should be greater than affected individuals;
b) the agency will have the ability to act sooner than affected individuals;
c) the agency is well placed to put in place a programme of action to benefit many people rather than leaving them entirely to act individually; or
d) an exception to the notification obligation applies and the agency does not propose to notify affected individuals at all.

6.21 It should be emphasised that the proposal to oblige agencies to take steps to minimise harm does not imply that individual mitigation is unnecessary. Individual action to respond to risk is still necessary both from a general legal liability perspective, since the individuals concerned may be best placed to identify their individual risks and act to mitigate them, and from a privacy or autonomy perspective, in that individuals may wish to exercise some choice (bearing in mind also that in the wake of a breach individuals may be wary of vesting complete trust in an agency that may appear to have failed to protect their interests).

6.22 I recommend that the Bill oblige agencies to take reasonable steps (if any) to seek to minimise the risk of harm to affected individuals from a notifiable breach including in relation to personal information that is no longer held by the agency as a result of the breach. The obligation would enable the Privacy Commissioner in appropriate cases to issue a compliance notice to specify a step required to be taken.

6.23 While this duty is not explicitly expressed in all overseas breach notification laws, the proposal is consistent with article 33(3)(d) and of the European Union General Data Protection Regulation which provides that notices to both the regulator and the affected individuals:[158]

> *"Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate the possible adverse effects." [Emphasis added.]*

RECOMMENDATION B.6.2

The mandatory privacy breach notification scheme in subpart 6(1) should include an obligation on agencies to take appropriate measures to minimise the potential harm to affected individuals from a notifiable breach, including in relation to personal information that is no longer held by the agency as a result of the breach.

Usefulness of mandatory follow-up reporting

6.24 The Bill requires notification of key details to affected individuals soon after a breach is discovered. Notification is the key to enabling the individual to mitigate possible harm.

[158] EU GDPR, articles 33(3)(d) and 34(2).

6.25 The Bill also requires notification to the Privacy Commissioner. This notification serves slightly different statutory aims. As the Privacy Commissioner, I will supervise and enforce the operation of the law and may assist or provide advice. However, a principal reason for involving the Privacy Commissioner is not merely to encourage the proper containment and resolution of a particular breach but to promote and incentivise improved information handling behaviour by that agency and overall.

6.26 In that respect the Bill would be improved by requiring a follow up report focused upon the completion of the response to the breach and reporting on changes in agency practices implemented as a result. I recommend that the Bill provide discretion for the Privacy Commissioner to require that such a report be submitted by the notifying agency, by such later date as the Commissioner considers appropriate.

RECOMMENDATION B.6.3

The mandatory privacy breach notification scheme in subpart 6(1) should include discretion for the Privacy Commissioner to require that a notifying agency that has submitted a notice to the Commissioner under clause 118 must also submit a follow up notice recording the steps taken in response to the breach, by such later date as the Commissioner considers appropriate.

Clause by clause comment

Clause 117: Interpretation - definition of "notifiable privacy breach"

6.27 This definition is pivotal to the operation of the mandatory breach notification scheme. The challenge is to create a threshold for notification that is set at a suitable level to ensure that affected individuals are notified in appropriate cases, while minimising unnecessary notifications and the risk of "notification fatigue". The threshold also needs to take account of the compliance burden on agencies and should be set at an appropriate level that justifies the additional agency obligation.

6.28 I note that the threshold is not a particularly high one compared to thresholds used in other jurisdictions. I am concerned that the definition in the Bill may not provide agencies with sufficient guidance about how to assess whether a privacy breach is notifiable in the circumstances. If agencies are uncertain about the threshold, there is a risk of over-notification that could undermine the policy intent of the new scheme. I have identified two practical options to help address this, should this be a significant issue in submissions the Committee receives on the Bill.

6.29 First, I note that the Law Commission recommended a factors-based approach to whether a breach should be notified.[159] This approach is used in another context in the Privacy Act. The definition of "serious threat" requires an agency to have regard to three factors to determine whether the relevant exception to IPP10 or IPP 11 applies in the circumstances.

[159] NZLC R123, R69.

6.30 I endorse this approach. Including a set of factors in the definition of a "notifiable privacy breach" would provide more certainty for agencies about how to carry out the necessary risk assessment and could further be explained by examples and practical guidance by my Office. Relevant statutory factors include the nature of the personal information involved, the number of individuals affected, the distribution of the information and associated risk depending on the recipient or potential recipient of the information and the likelihood and severity of the potential consequences.

6.31 Secondly, it may be useful to provide brief illustrative examples of what would or would not be notifiable privacy breaches such as the following:

> **Notifiable privacy breach** means 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 that it will do so
>
> **Example**
> An unauthorised disclosure of medical records may be likely to result in significant humiliation to the individual concerned.
>
> **Example**
> Loss of information that has been rendered unintelligible through encryption would not put individuals at risk of harm.

RECOMMENDATION B.6.4

The definition of "notifiable privacy breach" should provide more guidance and certainty for agencies about when a privacy breach is notifiable, for example by including factors to be taken into account and providing examples of privacy breaches that would, or would not, be notifiable.

Clause 118: Agency to notify Commissioner of notifiable privacy breach

6.32 Notification by an agency of a privacy breach does not necessarily result in any particular action by the Privacy Commissioner but a variety of scenarios may be foreseeable ranging from informal engagement to seek assurance that the breach is contained and being appropriately handled through to investigation and the potential for formal steps such as the issue of a compliance notice. In addition, in some cases affected individuals may lodge complaints if the breach appears to be an interference with privacy which may also result in an investigation with a view to resolving the complaint.

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

6.33 We comment only on subclause 119(5). This subclause establishes the right of action for an individual in cases where the agency fails to meet its obligation to notify the individual as required. It is a critical part of the notification scheme as it ensures that a failure to notify has consequences for an agency. The subclause acts both as an incentive for agencies to 'do the right thing' and also enables affected individuals to obtain redress where they have been harmed by an agency's failure to meet the statutory notification obligation.

6.34 We suggest that it be made clear that a failure to make timely notification may be an interference with privacy as well as a complete omission to notify. There would be many ways that this could be achieved in this clause or clause 75. One suggestion is to insert the following words:

> A failure to notify the individual under this section *as soon as reasonably practicable* may be an interference with privacy under this Act (see section 75(2)(a)(iv).

RECOMMENDATION B.6.5

Clause 75 should make clear that undue delay in notification might constitute an interference with privacy.

Clause 120: Exceptions to obligations to notify affected individual or give notice of notifiable privacy breach

6.35 I suggest that an exception be included modelled upon the 'domestic affairs' exemption in clause 24(2). This would be consistent with the EU GDPR that generally excludes from scope processing by a natural person in the course of purely personal or household activity.

RECOMMENDATION B.6.6

Clause 120 should include an exception to the requirement to notify affected individuals of privacy breaches where the agency is an individual and the information is limited to information obtained lawfully and held by that individual in connection with household or personal affairs.

Clause 121: Requirements for notification

6.36 I recommend making provision for additional reporting requirements not specifically listed in the clause to be specified in regulations. This could prove useful from an administrative perspective. Regulations could also be useful to prescribe reporting formats if desired.

6.37 This would provide flexibility should there be technical or other requirements once the scheme is operational. It may also be useful in relation to the discretionary follow up reporting recommended above.

RECOMMENDATION B.6.7

Clause 121 should allow for the use of regulations to prescribe additional reporting requirements or specify reporting formats. A consequential amendment to clause 213 should be made to allow for regulations to be made for this purpose.

Clause 122: Offence to fail to notify Commissioner

6.38 Although not recommended by the Law Commission, the Bill proposes that a failure to notify the Privacy Commissioner would be a criminal offence. This will only apply to private sector agencies, the former Minister being satisfied that the most effective deterrent for public sector agencies is 'naming and shaming'.[160] The former Minister anticipated that this criminal offence would be reconsidered in light of the Law Commission's work on pecuniary penalties.[161]

6.39 In Part A of my submission, I recommend a scheme for imposing civil penalties would be of value and generally preferable in this context to using criminal sanctions.[162] For example, a civil penalty could be elevated if there had been a repeated pattern of behaviour by an agency involving non-notification.

6.40 The proposed enforcement of the breach notification scheme should also be reassessed in light of the Australian scheme that has now commenced. Under that scheme, the failure to report a serious breach, or the failure to report a notifiable breach on two or more separate occasions allows the Australian Information Commissioner to seek a civil penalty against the organisation, depending on the significance and likely harm that may result from the breach.

RECOMMENDATION B.6.8

Clause 122 should be replaced with a civil penalty provision where an agency fails to notify the Commissioner of a notifiable privacy breach.

Clause 123: Publication of identity of agencies in certain circumstances

6.41 Clause 123 acts to authorise the publication by the Commissioner of the identities of agencies that have reported a breach and as a possible limit on that power of publication.[163] The clause authorises publication in the public interest which is the only basis on which a release of any details would be considered necessary.

6.42 For notification to the Privacy Commissioner to serve a useful purpose, there needs to be clear statutory authority as provided in this clause to share the information from the notification (which names the agency) with anyone who properly needs the information (such authority is to be found in clause 123, 206 and 207). There will be cases where it is desirable to release details of the breach in the public interest, which clause 123 anticipates.

6.43 The language used in the clause should more closely reflect the policy intent which is that the identity of an agency that notifies a privacy breach will not be publicly released, without its consent, unless there is a public interest. The clause uses the term "publish"

[160] Cabinet Social Policy Committee *Reforming the Privacy Act 1993* (May 2014) [46].
[161] Law Commission *Pecuniary Penalties: guidance for legislative design* (NZLC R133, 2014).
[162] Recommendation A.1.
[163] NZLC R123, R 72.

that can apply to more limited disclosures, as well as to a public release. However, in my view there is a distinction to be made between publicly releasing an agency's identity (to be governed by clause 123), and disclosing an agency's details to another regulator (that should be governed by the secrecy provision in clause 206). I recommend the following clarifying amendments to clause 123:

(1) The Commissioner may ~~publish the identity of~~ publicly identify an agency that has notified the Commissioner of a notifiable privacy breach if –
  (a) the agency consents ~~to publication~~; or
  (b) the Commissioner is satisfied that it is in the public interest to do so.
(2) This section does not prevent the ~~publication of~~ details of any notifiable privacy breach being made public in a form in which the agency or any affected individual is not identified and for the purpose of informing the public about the extent and nature of privacy breaches.

RECOMMENDATION B.6.9

Clause 123 should be amended to clarify that it applies to the public release of details of a breach.

Amendment to clarify application of subpart 6(1)

6.44 Clause 20 addresses how personal information held overseas is to be treated for purposes of the IPPs. This should extend to confirming how such information is to be treated for the purposes of subpart 6(1) of the Bill (breach notification).[164]

6.45 Subpart 6(1) should apply, for example, where personal information held (or treated as held) by an agency under clause 20(1) is affected by a notifiable privacy breach.

6.46 The inclusion of an express provision about the Privacy Act's application to overseas agencies (as recommended above in Part 1) will also need to take account of the new breach notification obligation in Part 6(1) of the Bill and clarify the scope of its application.

RECOMMENDATION B.6.10

Clause 20 of the Bill should clarify the circumstances in which personal information held outside New Zealand is subject to subpart 6(1).

Schedule 1: Transitional, savings and related provisions (clause 10)

6.47 The transitional provision provides that subpart 6(1) applies to a notifiable privacy breach that occurs before 1 July 2019 (the date indicated in the Bill as being the commencement of the Act) if it continues after that date.

[164] See for example, OAIC guidance – entities covered by the Notifiable Data Breach scheme (December 2017), p 4, noting that the scheme applies to organisations with an Australian link https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/entities-covered-by-the-ndb-scheme.

6.48 The transitional approach is that, after commencement, all breaches that continue to create a risk of harm to individuals are subject to the same notification obligation regardless of the precise date of the breach. This may have particular merit for relatively recently occurring or discovered breaches.

6.49 While the merit for individuals is recognised, this approach may have a downside in terms of complications for agencies and for my Office. The simpler alternative, which I understand has been followed overseas on the introduction of breach notification laws, is for the obligation to start at commencement with no application to earlier breaches.

6.50 The main complication will be in relation to older breaches where agencies may become confused as to what their obligations may be and where the merit of much delayed notification may be slight. Accordingly, one option that should be considered, if the transitional provision is retained, is that subpart 6(1) applies only to breaches that occurred after the date of enactment of the Bill. This will have the dual effect of limiting the application to comparatively recent breaches and minimising confusion. During that period agencies will have constructive knowledge of the enacted law.

6.51 If the transitional provision is not limited in the way recommended, I suggest alternatively that the offence provision in clause 122 be excluded from applying to notifications required solely by reason of the transitional provision.

RECOMMENDATION B.6.11

To simplify the implementation of the mandatory privacy breach notification scheme in subpart 6(1), clause 10 of Schedule 1 should be omitted so that obligations do not arise in relation to notifiable privacy breaches occurring before commencement. However, if the clause is retained, its application should be limited to notifiable privacy breaches that an agency became aware of after enactment of the Bill.

SUBPART 6(2) - Compliance notices

6.52 Subpart 6(2) of the Bill implements the Law Commission's recommendation to include a new power to issue a compliance notice to direct an agency to take a certain action, or to stop a certain action, in order to comply with the Privacy Act.[165] Statutory factors set out the considerations the Privacy Commissioner must take into account before issuing a compliance notice.[166] An agency has a right to be heard and a right of appeal.[167] If not challenged, the compliance notice is enforceable by order of the Human Rights Review Tribunal,[168] and non-compliance is an offence.[169]

[165] NZLC R123, R63. See also OPC's discussion paper for the Law Commission, "Enforcement, Compliance, Complaints: A Proposal to Reform the Privacy Act (May 2009). https://privacy.org.nz/assets/Files/Reports-to-ParlGovt/Enforcement-Compliance-Complaints-A-proposal-to-reform-the-Privacy-Act-1-May-2009.doc
[166] Cl 125.
[167] Cl 125(3); clause 131.
[168] Cl 130.

6.53 Other jurisdictions have comparable powers. The United Kingdom's Information Commissioner's Office has the power to issue enforcement notices, and the Australian Office of the Information Commissioner has enforcement powers that include accepting an enforceable undertaking and seeking an injunction. Under the EU General Data Protection Regulation (GDPR), supervisory authorities (the equivalent of the Privacy Commissioner) are required to have corrective powers including the ability to issue warnings and reprimands; order an agency to bring its operations into compliance with the GDPR (within specific direction and time period if appropriate); and impose a temporary or definitive ban on the processing of personal data by an agency.

6.54 I support subpart 6(2) as a suitable approach to providing enforcement powers that will allow my Office to address agency non-compliance in addition to the existing privacy complaints system. However one element of the Law Commission's recommendation 63 that has not been expressly implemented in Part 6(2) is making express provision for the Privacy Commissioner to publish the fact a compliance notice has been issued. I support this aspect and recommend its inclusion in the Bill.

Making express provision for the Privacy Commissioner to publish the issue of a compliance notice

6.55 In my view it would be appropriate for the Bill to make express provision for the publication of regulatory action in this context, and would support the overall policy intent of including the new form of regulatory action. I note that express provision is made for publication of notifiable privacy breaches under clause 123 in subpart 6(1) and recommend a provision also be included in subpart 6(2).

6.56 Privacy regulators in other jurisdictions with enforcement powers routinely publish the fact of enforcement action being taken. This public action encourages agencies to comply in order to avoid the issuing of a notice. The issue of a compliance notice represents enforcement action, with a public announcement generally expected, except in special circumstances. It would be appropriate to expressly provide for this in subpart 6(2) as recommended by the Law Commission.

RECOMMENDATION B.6.12

Subpart 6(2) should, as recommended by the Law Commission, expressly include the Privacy Commissioner's discretion to publish the fact that a compliance notice has been issued.

Clause by clause comment

Clause 124: Compliance notices

6.57 This clause defines the scope of the new power to issue a compliance notice, namely the types of breaches that qualify for a compliance notice to be considered. It properly

[169] Cl 133(3).

includes any breach of the Act, including any interference with privacy as defined in clause 75, and actions that are to be treated as privacy breaches under other Acts.

6.58 The clause does not extend to a breach of a settlement assurance that an agency may have previously given as part of a complaint investigation.[170] This was, however, one of the problems the Law Commission considered in its report, noting that the Act anticipates that assurances may form part of a settlement. However it does not provide for any sort of enforcement if an assurance is breached.[171]

6.59 The compliance notice power would be a useful means of enforcing an agency's obligation to honour an assurance. For example, an agency may undertake to update its processes, or to engage in training. If it neglects to do so, or if there are repeated instances of the same issue arising in an agency that indicated the assurance has not been complied with, it is desirable to address this by the Commissioner requiring action be taken.

RECOMMENDATION B.6.13

Clause 124 should be expanded in scope to include an agency's breach of a settlement assurance it has given to the Privacy Commissioner.

6.60 Before issuing a compliance notice, the Privacy Commissioner may assess whether any person has suffered harm (clause 124(2)(a)). In my view it should be made clear that this allows an assessment by the Commissioner of potential harm as well as actual harm. This could be achieved by adding the words "or may suffer" after the words "has suffered".

RECOMMENDATION B.6.14

Clause 124(2)(a) should be amended by adding the words "or may suffer" after the words "has suffered".

Clause 125: Issuing compliance notice

6.61 Before issuing a compliance notice, the Privacy Commissioner must provide the agency with a reasonable opportunity to comment on a written notice outlining details of the breach. I submit that it would be desirable for this clause to explicitly state that an agency's assurance may be accepted at this point in the process.

6.62 The previous Privacy Commissioner, who proposed the reform, and the Law Commission anticipated that the new power would afford an opportunity for the Commissioner to raise matters of non-compliance with agencies, who may then be willing to provide an assurance that it will take steps to address the problem identified.[172]

[170] Clauses 84, 87, 96, 99.
[171] NZLC R123 at [6.69]. See also Necessary and Desirable, recommendation 112.
[172] NZLC IP 17, [8.65]; OPC *Enforcement, Compliance, Complaints* at [2.27].

6.63 This is consistent with the Privacy Commissioner's conciliation role in the complaints jurisdiction. The Bill carries over express provisions that anticipate that agencies may settle complaints by offering assurances about their future practice or process.[173]

6.64 However subpart 6(2) does not expressly provide that the Privacy Commissioner may, at his or her discretion, accept an assurance from an agency in relation to a matter of non-compliance outside the context of an investigation under Part 5. It would be desirable to do so as a practical means of achieving agency compliance, and as a necessary ancillary option to the new compliance notice power.

6.65 I recommend that clause 125 should include the option for an agency to give an assurance as to the steps it will take to address its non-compliance, as an alternative to the Privacy Commissioner issuing a compliance notice. The compliance notice would provide a back-up power as required.

RECOMMENDATION B.6.15

Clause 125 should be amended to allow an agency's assurance to address a matter of non-compliance to be accepted by the Privacy Commissioner, at any time, at his or her discretion, including following a written notice outlining the breach in clause 125(3).

Clause 127: Agency response to compliance notice

6.66 The reference to "served" should be amended to "issued" to ensure consistency with the terminology throughout this part. Compliance notices are issued and notified to the agency concerned under the usual notification provisions in regulations.

RECOMMENDATION B.6.16

In clauses 127, the reference to "served" should be amended to "issued" to ensure the terminology is consistent throughout this part.

Clause 133: Enforcement, costs and enforcement

6.67 The penalty for failing to comply with a compliance notice is a criminal offence (clause 133(3)), as recommended by the Law Commission. In its Issues Paper, the Law Commission noted there may be advantage in having escalating sanctions such as civil pecuniary penalties as well as criminal offences.[174]

6.68 I support further development of the enforcement framework to allow the flexibility to seek a civil penalty for an agency's failure to comply with a compliance order, as an alternative to initiating a criminal prosecution. Civil penalties are discussed in more detail in Part A of this submission and in Appendix A. This enforcement option would allow the Commissioner to engage with an agency in default and negotiate an appropriate agreed

[173] Clauses 84, 87, 96, 99.
[174] NZLC IP 17 at [8.59].

outcome that would be approved by the court. Failing agreement, it would allow the Commissioner to ask the court to approve a suitable penalty that takes account of the particular circumstances of the breach and the seriousness of the conduct at issue.

6.69 I recommend the Bill provide for enforcement of compliance notices by civil penalty, as an alternative to criminal prosecution.

RECOMMENDATION B.6.17

The Bill should make provision for the Privacy Commissioner to seek the imposition of a civil penalty for failure to comply with a compliance notice, as an alternative enforcement option to the prosecution of a criminal offence.

PART 7 – Sharing, accessing and matching personal information

7.1 Part 7 provides for the sharing, accessing, and matching of personal information by specified agencies. It re-enacts Parts 9A, 10, 10A, and 11 (and the associated Schedules) of the Privacy Act 1993 by placing those parts in Part 7. Part 9A (Information sharing) becomes Subpart 1, Part 10A (Identity information) becomes Subpart 2, Part 11 (Law enforcement information) becomes Subpart 3, and Part 10 (Information matching) becomes Subpart 4.

7.2 Part 7 supports and enables proportionate information sharing with appropriate safeguards and oversight mechanisms to assess ongoing suitability and effectiveness of information sharing mechanisms.

SUBPART 1: Approved Information Sharing Agreements

7.3 This subpart provides a mechanism for Approved Information Sharing Agreements (AISAs) approved by Order in Council. The AISA mechanism was introduced in 2013 (Part 9A of the Privacy Act 1993) following the Law Commission's 2011 report that concluded that the prescriptive requirements of Part 10 had become outdated and recommended a new more flexible information sharing framework.

7.4 The AISA framework provides the flexibility required by government, together with the inclusion of process safeguards for the individuals whose personal information is being shared. The framework ensures proportionality, transparency and accountability and guards against unwarranted privacy intrusions – features that are essential for citizens to trust how government shares their personal information.[175]

[175] In support of the Part 9A framework OPC submitted that a more consistent framework for sharing personal information should be created, in which the privacy risks are properly identified and managed while reducing the current need for lengthy bureaucratic processes https://www.privacy.org.nz/assets/Files/Reports-to-ParlGovt/Submission-on-the-Privacy-Information-Sharing-Amendment-Bill-March-2012.pdf

7.5 My Office has published guidance about the process to develop an AISA[176] and works with agencies to assist development of AISAs. There are now seven AISAs in operation (as set out in Schedule 3 of the Bill) and another seven at various stages of development.

7.6 Subpart 1 carries over Part 9A with amendments designed to improve particular aspects of the AISA mechanism. Following a Cabinet Directive in 2016 that instructed agencies to identify any barriers to information sharing proposals, feedback received by OPC and the Ministry of Justice was overwhelmingly that the barriers to effective information sharing are operational rather than legislative. Barriers identified include lack of a clear mandate, competing priorities, IT incompatibility and issues with data standards. Legislative change to the AISA mechanism was considered unnecessary, apart from specific amendments to improve particular aspects such as the "representative party" mechanism that requires adjustment.

7.7 I support the amendments and provide the following comment to further enhance the framework.

Clause 142 Agreement may apply to classes of agencies

7.8 The concept of representative party (current s 96G) is to be replaced by Clause 142 that enables an agreement to apply to a class of agencies, and for any member of that class to become a party to the agreement by being named as a party in a schedule to the agreement.

7.9 Clause 142 should expressly provide for agencies that are added or removed from the Schedule of Parties to be notified. All other parties to the agreement should also be notified of changes to the Schedule of Parties. Without notification, agencies (including existing parties) may be unable to exercise the rights in clause 142(3) to be removed and in clause 142(5) to refuse to participate. It is possible that an agency could be added without its knowledge and could receive information it does not want. Similarly if an agency is removed without its knowledge, it might incorrectly continue to share information under the agreement.

RECOMMENDATION B.7.1

Clause 142 should expressly provide that (a) agencies that are added or removed from the Schedule of Parties are to be notified, and (b) all other parties to the agreement are to be notified of a change to the Schedule of Parties.

[176] OPC *An A to Z of Approved Information Sharing Agreements (AISAs)* (March 2015) https://privacy.org.nz/news-and-publications/guidance-resources/approved-information-sharing-agreements-aisas/

SUBPART 3: Law enforcement

Clause 173 Power to amend Schedule 5 by Order in Council

7.10 Clause 173 provides that Schedule 5 (other than law enforcement information described in that schedule as court records) may be amended or replaced by Order in Council on the recommendation of the Minister of Justice after consultation with the Commissioner.

7.11 I support the reinstatement of the Order in Council process. Schedule 5 tightly prescribes the authorised arrangements for sharing of particular law enforcement information between specified agencies. The mandatory consultation process with the Privacy Commissioner, combined with the prescriptive nature of Schedule 5, ensures that the Order in Council mechanism will be used appropriately.

SUBPART 4: Authorised information matching programmes

7.12 Clauses 174 to 191 re-enact Part 10 of the Privacy Act 1993, together with Schedule 3 (information matching provisions)[177] and Schedule 4 (information matching rules)[178] which provides a continuing framework to govern authorised information matching programmes. However, subpart 7(4) will apply only to the authorised information matching programmes currently in existence. The Bill restricts any new information matching programmes being entered into under subpart 7(4).[179]

7.13 During the 25 years that the information matching framework has been in place, there have been significant changes in data processing technology and practice. These changes enable agencies to share information more efficiently and more cheaply than before. It is important to review the current privacy controls and use the opportunity that new technologies provide to improve government processes while continuing to manage privacy risks.

7.14 The information matching safeguards in the Privacy Act were proportionate and relevant when enacted and have proven their worth. But technology and government operations have changed. For example, transfers of large datasets over secure online connections have become normal practice. The use of personal information by government is aided by the evolution of governance, assurance and risk frameworks such as the NZ Information Security Manual (NZISM)[180] that supports privacy and sets minimum security standards.

7.15 In recognition of the changes in technology and security, the re-enactment of Schedule 4 (information matching rules) includes the removal of information matching Rule 3 (Online

[177] Privacy Bill, Sch 6.
[178] Privacy Bill, Sch 7.
[179] Privacy Bill, Sch 8. This is consistent with Law Commission proposals in 2011 that information matching should continue to be controlled under the Privacy Act, under a new framework for information sharing: NZLC R123, Appendix 1. Since the enactment of Part 9A of the Privacy Act 1993, seven AISAs have been approved including an agreement between Inland Revenue and the Ministry of Development that took several existing 'product-centric' agreements (including five Authorised Information Matching Agreements) authorised under various Acts with one approved agreement.
[180] https://www.gcsb.govt.nz/publications/the-nz-information-security-manual/

transfers) and Rule 8 (Time Limits) as recommended by the Law Commission.[181] I support the removal of these two information matching rules from Schedule 4 (now Schedule 7 of the Bill).

7.16 It is no longer justified to prohibit the use of online transfers except with the approval of the Privacy Commissioner. Online transfers are now an expected practice, not an exceptional one. Government agencies now have greater expertise and experience in the use of online mechanisms along with governance and leadership support from the Government Chief Digital Officer. I am cognisant of the compliance costs on agencies to comply with online transfer approval requirements.

7.17 Despite removal of Rule 3, I will maintain oversight of the safeguards applied to online transfers using the requirement on agencies to maintain detailed technical standards governing the operation of the programme.

7.18 Information Matching Rule 8 (Time Limits) requires that the agencies specify in the Technical Standards Report the number of times the programme will operate each year.[182] The Law Commission considered the rule too rigid. In today's environment, matching programmes routinely operate daily, sometimes more than once a day. Despite removal of Rule 8, I will maintain oversight of the scale of matching through annual reporting on information matching programmes[183] and periodic reporting on information matching provisions.[184]

Clause 181: Notice of adverse action proposed

7.19 This section continues section 103 of the Privacy Act in part. A slight change in clause 181(5) inadvertently alters the provision and should be deleted. The intent of the provision is that an agency may proceed to take adverse action against an individual, without complying with the prior notice requirements, if those notice requirements would prejudice an investigation into possible offending. However the addition of the word "even" suggests that there may be other reasons that justify non-compliance with the notice requirement, which is not intended.

RECOMMENDATION B.7.2

Clause 181(5) should be amended by deleting the word "even".

Consequential amendments - Social Welfare (Reciprocity Agreements, and New Zealand Artificial Limb Service) Act 1990

7.20 The Social Welfare (Reciprocity Agreements, and New Zealand Artificial Limb Service) Act 1990 empowers the Government to enter into social security reciprocity agreements with foreign governments. These agreements allow for inter-country sharing of information for social security purposes or mutual assistance in the recovery of social

[181] NZLC R123, Appendix 2.
[182] Privacy Act 1993, Sch 4, Information Matching Rule 4.
[183] Privacy Bill, cl 183.
[184] Privacy Bill, cl 184.

security debts. Section 19(D)(3)(b) of that Act empowers the Government to operate trans-border information matching programmes in support of these agreements.

7.21 An issue arises under the Bill as to new reciprocity agreements under this legislation after 1 July 2019. Firstly, the amendment in Schedule 8 will limit any new reciprocity agreements after 1 July 2019. Secondly, the amendment in Schedule 10 removes relevant criteria for the Privacy Commissioner's report to Ministers that is required prior to making an Order in Council approving a new reciprocity agreement.

Schedule 8 amendments

7.22 Section 19(D)(3)(b) is an information matching provision listed in Schedule 3 of the Privacy Act (and will transition into new Schedule 6 in the Bill). The information matching programmes currently operating under that provision that support the international agreements will continue to operate but, from 1 July 2019, no new programmes are permitted. The practical effect is that no new information matching programmes can be implemented using subpart 7(4) to support any future international agreements.

7.23 The information matching provisions in Part 7(4) of the Bill should not be discontinued in relation to trans-border information matching agreements under the Social Welfare (Reciprocity Agreements, and New Zealand Artificial Limb Service) Act 1990, without a suitable replacement. Subpart 7(1) (Information sharing) is not available as an alternative option for new trans-border agreements. An overseas agency cannot be a party to an information sharing agreement, thus excluding use of the information sharing framework to cover social security agreements.

Schedule 10 amendments

7.24 Currently, before a new trans-border social security reciprocity agreement can be approved by Order in Council, the Privacy Commissioner is required to report to Ministers on whether the relevant provision complies with the privacy principles, having regard to the information matching guidelines in section 98 of the Privacy Act 1993.[185]

7.25 The Bill repeals the information matching guidelines, and Schedule 10 makes a consequential amendment to remove reference to those guidelines from s 19(2A)(a) of the Social Welfare (Reciprocity Agreements, and New Zealand Artificial Limb Service) Act 1990. This will affect the criteria on which the Privacy Commissioner reports to Ministers and the quality of oversight of the international information sharing for social security purposes.

7.26 Appropriate criteria should be retained for the Privacy Commissioner to assess a proposed agreement and report to Ministers. Reference to the privacy principles alone will not capture relevant considerations in this context such as the strength of the public interest, the nature of the public benefits and the proportionality of the proposed

[185] Social Welfare (Reciprocity Agreements, and New Zealand Artificial Limb Service) Act 1990, s 19(2A), s 19A(2).

agreement. I recommend the information matching guidelines be retained for this purpose or replaced with a suitable alternative such as criteria modelled on clause 149(2) of the Bill.

RECOMMENDATION B.7.3

a) The information matching provisions in Part 7(4) of the Bill should not be discontinued in relation to trans-border information matching agreements under the Social Welfare (Reciprocity Agreements, and New Zealand Artificial Limb Service) Act 1990, without a suitable replacement.

b) The consequential amendment to section 19(2A)(a) of the Social Welfare (Reciprocity Agreements, and New Zealand Artificial Limb Service) Act 1990 should be amended to (i) retain the reference to the information matching guidelines for this purpose, or (ii) replace that reference with appropriate criteria on which the Privacy Commissioner reports to Ministers, such as the criteria in clause 149(2) of the Bill.

Unused Information Matching Provisions

7.27 Schedule 3 of the Privacy Act 1993 lists all the information matching provisions covered by Part 10 of that Act. In contrast, Schedule 6 of the Privacy Bill is a reduced list that has removed references to those information matching provisions for which there are no information matching agreements operating. The reference to section 298 of the Immigration Act 2009 should be removed from Schedule 6 as there is no information matching being undertaken under this section.

7.28 I am preparing a report under section 106 of the Privacy Act 1993 for the Minister of Justice on unused information matching provisions. Unused provisions do not deliver their intended benefits to society and therefore continuing Parliamentary authorisation of these privacy intrusive measures is unjustified. The Minister of Justice will table this report before Parliament.

7.29 To prepare this report, I have been asking agencies whether they have active plans to implement the information matches. Where there are no active plans to implement an information match, I recommend that the provision is not only removed from Schedule 6 of the Privacy Bill (as the Bill on introduction recommends) but that the Bill also repeals the authorising provision in its substantive statute (such as the Immigration Act).

7.30 My report will enable the Ministry officials and the Parliamentary Counsel Office to advise the Select Committee as to whether it is appropriate for the Privacy Bill to repeal, as a matter of consequential amendment, the authorising provisions for information matches in their substantive statutes.

Part 7 Technical amendment recommendations

7.31 Some minor technical and drafting matters should be addressed as follows:

a) Clause 136: Replace the word "authorised" as follows: *"… with an **approved** information sharing agreement to facilitate…"*

b) Clause 175: Replace reference to Schedule 3 of the 1993 Act with Schedule 6 of the Bill as follows: *"…by an information matching provision **specified in Schedule 6**".* It does not appear necessary to refer to "Schedule 3 of the Privacy Act before its repeal" in this clause as new Schedule 6 in the Bill includes all the necessary information matching provisions.

c) Clause 177, definition of "monetary payment": Reference to section 124(1)(da) of the Social Security Act 1964 can be deleted as that provision has been repealed.

d) Clause 183(1) and (5): Amend to align with clause 184: *"T/the **responsible** Minister must…*"

e) Clause 187: Replace the words "is used" to reflect applicable future tense: "*…if the sole or principal purpose for which that information is sought is **for use** in an information matching programme".* Refer Privacy Act 1993, section 109.

RECOMMENDATION B.7.4

Minor and technical amendments should be made to clauses 136, 175, 177, 183 and 187.

PART 8 – Transfer of personal information outside New Zealand

8.1 This Part of the Act continues provisions that were inserted into the Act in 2010 in order to provide a mechanism to demonstrate that NZ's law met EU standards. Part 11A of the Privacy Act 1993 plugged a theoretical loophole whereby a European company might transfer information through NZ to another country for processing in an attempt to circumvent EU controls.

8.2 In 2010, the Privacy Act was changed to meet European Union requirements with the enactment of the Privacy (Cross-border Information) Amendment Act 2010. This amendment inserted a new Part 11A (Transfer of personal information outside New Zealand) enabling the Privacy Commissioner to issue a transfer prohibition notice in relation to, amongst other scenarios, information received from the EU that was routed through NZ to another state in an attempt to circumvent EU requirements.

8.3 The 2010 Amendment Act enabled New Zealand's laws to be formally recognised by the European Commission in 2012 as meeting EU standards. It might be noted that Part 11A did not seek to protect the information of New Zealanders but was focused merely on information received from overseas.

PART 9 - Miscellaneous provisions

9.1 Part 9 continues a number of important provisions from the Privacy Act 1993, including liability and offences (clauses 211 and 212).

9.2 I make recommendations elsewhere in this submission on matters to which some of these clauses relate and these are noted below.

Clause by clause comment

Clause 201: Privacy Officers

9.3 To further encourage agency steps to compliance, I recommend this clause be expanded, as set out in part A of my submission (recommendation A.2).

Clause 212: Offences

9.4 Clause 212 continues the criminal offences for obstructing the Privacy Commissioner in the exercise of his powers under the Act, making a false statement to the Commissioner, and misrepresenting a person's authority under the Act.

9.5 Two criminal offences are also created in Part 6 of the Bill - clauses 122 and 133(3) - that I have commented on above (recommendations B.6.8 and B.6.16). In addition, clause 109 creates a criminal offence for failing to comply with an access order.

9.6 Clause 212 introduces two new offences (clause 212(2)(c) and (d)) and increases the maximum penalty for the existing offences from $2,000 to $10,000.The new offences implement Law Commission recommendations[186] and will prohibit impersonation in order to gain access to a person's information, and the destruction of information that is the subject of an access request under IPP6.

9.7 The new offence in clause 212(2)(c)(ii) prohibits impersonation of another person in order to have that individual's personal information used in some way or altered or destroyed. I recommend two amendments to ensure it reflects the intent of the Law Commission's recommendation.

9.8 Firstly, the offence should be narrowed to require that the impersonation or false pretences has the effect of misleading "an agency." This element of the proposed offence has not been included in the Bill. Without the reference to "an agency", the offence is potentially broad in scope as it would include misleading conduct that affects information not covered by the civil jurisdiction of the Bill.

9.9 Secondly, the offence should be broadened to include misrepresentation as to the existence or nature of the person's authorisation. This is an element of the recommended reform that is not currently included.

[186] NZLC R123, R66.

RECOMMENDATION B.9.1

To fully implement the Law Commission's recommendation 66(a), clause 212(2)(c) should be amended as follows:

a) include as a further element of the offence that the conduct in question misleads an agency; and

b) include an offence of misrepresenting to an agency the existence or nature of an authorisation from an individual that has the effects in clause 212(2)(c)(i) or (ii).

SCHEDULE 1 – Transitional, savings and related provisions

10.1 The Bill repeals and replaces the Privacy Act 1993. The Bill retains the current Act's provisions but updates and modernises these. It also adds additional reforms to enhance the regime and better protects individuals' privacy.

10.2 The Bill is intended to come into force six months after enactment to allow time to prepare for the new obligations on agencies under the Act.

10.3 The schedule provides for the transitioning of matters commenced under the Privacy Act 1993 and the savings of certain matters from that Act

Clause by clause comments

10.4 The following provides my comments and recommendations on the transitional provisions.

Schedule 1 - Clauses 7, 8 and 9: Complaints; Investigations and Inquiries; and Clause 9: Proceedings

10.5 Schedule 1, clause 7 provides for any unresolved complaints at the time of the new Act coming into force to be dealt with under the new Act, even though the action alleged to be an interference with privacy occurred prior. Similarly, Schedule 1, clause 8 provides for pending investigations and inquiries, and Schedule 1, clause 9 provides for proceedings before the Tribunal to be continued and completed under this Act.

10.6 I note that the new Act includes amendments that will result in certain actions becoming an interference with privacy, when they were not necessarily under the 1993 Act (and vice versa). Examples include the new obligations in respect of cross-border disclosures and new withholding grounds.

10.7 I recommend Schedule 1, clauses 7, 8 and 9 be amended to clarify that the provisions governing what was an interference with privacy under the 1993 Act that were in force at the time of the alleged interference, continue to apply.

10.8 I also recommend that Schedule 1, clause 7 should include a savings provision similar to that in clause 8(3) in respect of any decision made, or thing done, by the Commissioner under the Privacy Act 1993 in relation to the complaint.

RECOMMENDATION B.10.1

Schedule 1, clauses 7, 8 and 9 should be amended to clarify the provisions governing what was an interference with privacy under the 1993 Act, that were in force at the time of the alleged interference continue to apply.

RECOMMENDATION B.10.2

Schedule 1, clause 7 should be amended to include a savings provision that provides "Any decision made, or thing done, by the Commissioner under the Privacy Act 1993 in relation to a complaint that has not been resolved or otherwise dealt with by the Commissioner must be treated as if it had been made or done under this Act."

Clause 10: Notifiable privacy breaches

10.9 This clause provides that subpart 6(1) applies to a notifiable privacy breach that occurs before 1 July 2019 if it continues after that date.

10.10 I recommend above that this should be simplified (recommendation B.6.10).

Clause 11: Information sharing agreements

10.11 This provision provides for agreements that are already in force to continue in force under the new Act. I note that the provision does not currently provide for transition of the parts of the Privacy Regulations 1993 that govern reporting requirements for agreements. Nor does the provision provide for the preservation and continuity of acts taken in respect of agreements that have been sufficiently developed and relevant statutory steps undertaken that need to be preserved.

RECOMMENDATION B.10.3

Schedule 1, clause 11 should be amended to include a savings provision that provides "Any decision made, or thing done, under the Privacy Act 1993 in relation to a pending information sharing agreement or under the Privacy Regulations 1993 in relation to an approved information sharing agreement must be treated as if it had been done under this Act."

Schedule 1, clause 13: Police may continue to access law enforcement information in relation to persons aged 17 years

Schedule 1, clause 14: Legal Services Commissioner may continue to access law enforcement information in relation to persons aged 17 years

10.12 These provisions relate to the amendment to Schedule 5 that extends the restriction on access to details of hearings relating to offences that did not carry a liability to imprisonment to include 17 year olds (persons over 14 years but under 18 years of age - refer Schedule 5 page 133). Schedule 1, clause 13 provides for Police to continue to have access to these details in respect of 17 year olds that immediately before the Bill is in force are being investigated or have had proceedings against them commenced. Schedule 1, clause 14 provides for the Legal Services Commissioner to continue to have access for the purposes of determining a grant of legal aid.

10.13 I consider these transitional provisions are unnecessary and should be deleted as there is no rationale for them given the six month period between enactment and commencement of the Bill and that any continued required access to the information can be requested by the Police and Legal Services Commissioner as necessary and disclosed under the maintenance of law exception in IPP 11(1)(e).

RECOMMENDATION B.10.4

Schedule 1, clauses 13 and 14 should be deleted.

Privacy Commissioner
Te Mana Matapono Matatapu

Appendix A

Background paper: Including provision for the Commissioner to seek imposition of a civil penalty for serious privacy breaches

1. This paper provides background information on the Privacy Commissioner's recommendation that the Bill include provision for the Commissioner to seek imposition of a civil penalty where there is a serious or repeated breach of the Privacy Act.[1]

2. The proposed civil penalty power would fill an identified gap in the Bill's enforcement framework and complement the new compliance notice power and breach notification provisions in Part 6 of the Bill.

3. New Zealand's privacy law is increasingly out of step both internationally and domestically as compared with consumer rights regulation. Civil penalties ensure that non-compliant agencies are appropriately and meaningfully held to account, and provide effective incentives on agencies to comply. Increased compliance ultimately enhances individuals' privacy.

4. Internationally, it is recognised that privacy and data protection regulators need a variety of potential sanctions, including a power to seek civil penalties (or directly impose them through a fining power), to be able to effectively respond to serious, persistent or egregious breaches and non-compliance with the law.

5. The Bill provides an opportunity to update the design of the regulatory framework and enhance the range of sanctions. In the current data context, where the amount and significance of personal information being collected is expanding exponentially and serious privacy breaches can be catastrophic for both individuals and agencies, the Commissioner requires the right tools to appropriately respond.

6. Information privacy and data protection is a dynamic field which has developed rapidly against a background of significant technology changes, and further reforms including civil penalties provide a response to the evolution which has occurred since the 2011 review by the Law Commission.[2]

Including civil penalty provisions in the Privacy Bill

7. The Privacy Commissioner suggests an appropriate framework is to include provision in the Bill for the Privacy Commissioner to apply to the Court[3] for the imposition of a civil

---

[1] A report to the former Minister on the operation of the Privacy Act, recommended new provisions to allow the Commissioner to apply to the High Court for a "suitably significant" civil penalty (up to $100,000 in the case of an individual and up to $1 million in the case of a body corporate) to be imposed for serious breaches of the Privacy Act: Privacy Commissioner *Report to the Minister of Justice under section 26 of the Privacy Act 1993* (December 2016, tabled February 2017) recommendation 4, at [78]. https://privacy.org.nz/news-and-publications/reports-to-parliament-and-government/privacy-commissioners-report-to-the-minister-of-justice-under-section-26-of-the-privacy-act/

[2] Law Commission *Review of the Privacy Act 1993* (NZLC R123, 2011).

[3] District Court or High Court, depending on penalty amount sought.

penalty in circumstances where there is either a serious breach of the Privacy Act or repeated breaches. When imposing the penalty, the Court would be required to take account of the context, nature and extent of the breach, the extent of any loss or damage suffered and whether the agency was previously found to have engaged in any similar conduct.

8. This approach aligns with use of civil penalties in New Zealand and accords with the Law Commission's recommendation that pecuniary penalties should be imposed by a court on the civil standard of proof. It would also ensure that the court operates as an independent judicial check on the Commissioner's power to impose punitive penalties.

9. The Privacy Commissioner suggests a penalty provision (modelled on another New Zealand penalty provision)[4] along the following lines:

Pecuniary penalty for serious or repeated breaches

(1) On the application of the Privacy Commissioner, the court may order an agency to pay a pecuniary penalty to the Crown, or any other person specified by this court, if the court is satisfied that the agency has:

(a) done an act, or failed to do any act, or engaged in a practice, that is a serious breach of the Act or a code of practice; or

(b) repeatedly done an act, or failed to do any act, or engaged in a practice, that is a serious breach of the Act or a code of practice.

(2) Subject to the limits in subsections (3) and (4), the pecuniary penalty that the court orders the agency to pay must be an amount which the court considers appropriate taking into account all relevant circumstances, including -

(a) The nature and extent of the breach;
(b) The nature and extent of any loss or damage that has been or may be caused by the breach;
(c) The circumstances in which the breach took place;
(d) Whether the agency has previously been found by the Privacy Commissioner or the Human Rights Review Tribunal or the court to have engaged in any similar conduct.

(3) If the agency is an individual, the court may order the agency to pay a pecuniary penalty not exceeding $100,000 in respect of the breach that is the subject of the Privacy Commissioner's application.

(4) If the agency is not an individual the court may order the agency to pay a pecuniary penalty not exceeding $1 million in respect of the breach that is the subject of the Privacy Commissioner's application.

10. As is the practice for other regulatory agencies with civil penalty powers available in their range of regulatory responses, the Privacy Commissioner would provide guidelines

[4] Unsolicited Electronic Messages Act 2007, s 45.

regarding enforcement and what factors may be considered in applying to the court for imposition of a penalty.[5]

11. Additional clauses will need to be included to support the penalty provision, including provisions covering applicable rules, procedure, standard of proof, and time limits. The Privacy Commissioner is available to provide supporting advice to the Ministry of Justice and Parliamentary Counsel Office in drafting these provisions.

Function and use of civil penalties as a regulatory tool

12. The Bill currently lacks suitable sanctions for serious non-compliance. The principles of responsive regulation make clear that compliance is most likely to be achieved where a regulatory regime is enforced by way of a hierarchy (or pyramid) of interventions.[6] While the Bill includes specific criminal offences, these are limited to particular actions that breach the legislation, and do not provide a power for the Commissioner to enforce serious generic breaches.

13. The Law Commission 2014 report on the use of civil penalties as a regulatory tool noted that civil penalties are a punitive measure designed to punish the contravention and deter future contraventions, rather than being intended or designed to compensate those affected by a breach.[7]

14. The Law Commission concluded that civil penalties can be a flexible, efficient and effective regulatory tool, and that enforcement agencies with the power to commence these proceedings should develop and publish enforcement policies.[8]

15. As the Commissioner noted in the 2017 report under s 26 of the Privacy Act, criminal offences for non-compliance are a blunt tool that can prove resource intensive to prosecute, and of limited use against public sector agencies, or large corporates, due to complexity of criminal process rules. The maximum fine has been set at the relatively low level of $10,000, regardless of whether the defendant is an individual or a corporate entity.[9]

16. Offences in the Bill as introduced to the House are targeted at specific egregious acts such as failing to report a notifiable privacy breach, making false statements,

---

[5] The Law Commission in its review of pecuniary penalties noted that "the use and public release by agencies of enforcement guidelines" will assist enforcement agencies in exercising a high standard of care in their decision making regarding civil penalties. Law Commission *Pecuniary Penalties: Guidance for Legislative Design* (NZLC R133, 2014) at [10.21]. See for example the Office of the Australian Information Commissioner *Guide to Privacy Regulatory Action*, May 2018, Ch 6 Civil penalties https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-6-civil-penalties.

[6] Law Commission *Pecuniary Penalties*, above, at [5.23].

[7] Above, at [3].

[8] See for example the Commerce Commission's *Enforcement Response Guidelines* (October 2013), explaining enforcement responses and factors taken into account when deciding on the appropriate regulatory response. See also Office of the Australian Information Commissioner *Guide to regulatory action* (updated May 2018).

[9] Privacy Bill, clause 212.

impersonation or destroying information,[10] rather than providing a means of responding to significant privacy breaches more generally. In comparison, civil penalties offer a discretionary and flexible tool such that they can be used to respond to a significant breach more generally.

17. Civil penalties act as an incentive to encourage agencies to cooperate and to mitigate the risk of harm. Agencies may be more likely to comply when aware of the potential for the imposition of significant fines for serious non-compliance or disregard for privacy.

18. Currently, where an agency breaches the Privacy Act, this may result in that agency paying compensatory damages following a complaint to the Privacy Commissioner. Including civil penalties in the Bill would provide an enforcement mechanism that would operate alongside the current complaints resolution system.

19. Civil penalties would provide a means to punish serious breaches, including repeat offending. Currently, compensation for purposes of a complaint investigation is assessed on the extent of the harm suffered by a particular individual. Other factors, such as repeated breaches in the same or similar circumstances (indicating that an agency may have a particular disregard for compliance) are not relevant in settling individual complaints. In contrast, repeat offending is a key factor to be taken into account in privacy-related civil penalty provisions in other jurisdictions.

20. Civil penalties provide the flexibility for negotiation with an agency prior to applying to the Court for imposition of a penalty. This approach is used by other regulatory agencies when seeking the imposition of a civil penalty, and aligns with the regulatory approach operated by the Privacy Commissioner in the complaints resolution system, that emphasizes agency engagement and negotiated resolution.

21. It also aligns with consumer protection regulation. Information privacy protection is an example of consumer protection regulation - in the data economy, from a consumer perspective, personal data is essentially the currency for services. Civil penalties are commonly used by New Zealand regulatory and consumer protection agencies such as the Commerce Commission, the Department of Internal Affairs and Inland Revenue as a valuable tool to support their regulatory role and objectives.

22. The Commerce Commission is the regulatory body tasked with enforcing New Zealand's competition, fair trading and credit contract laws. It has a range of enforcement options, broadly grouped as low-level and high-level responses. Civil penalties are included in the high-level response enforcement options, alongside criminal proceedings. The Commerce Commission has the ability to seek civil penalties against both individuals and companies under various pieces of legislation, and a wide range of remedies are available including fines, statutory damages sought on behalf of affected parties, injunctions, declarations of breach, and direction or exclusion orders.

[10] Privacy Bill, clauses 122 and 212.

23. The Commerce Commission's *Enforcement Response Guidelines* set out the enforcement response model followed by the Commission.[11] This includes the criteria and factors the Commission take into account when deciding whether to investigate and which enforcement response to use, and factors to consider when determining whether to commence civil or criminal proceedings. It ensures transparency and clarity on the Commission's decision-making regarding enforcement. The Law Commission referred to these guidelines as an example of best practice, having noted the use and public release by agencies of enforcement guidelines will assist enforcement agencies in exercising a high standard of care in their decision making regarding civil penalties.

24. The Department of Internal Affairs also enforces legislative regimes that include civil penalties as an enforcement option. For example, DIA administers the Unsolicited Electronic Messages Act 2007, established to punish senders of spam emails. DIA has been successful in enforcing this Act in a range of cases and involving the imposition of significant civil penalties, such as a case where a $120,000 penalty was imposed on an Auckland-based marketing company for sending spam via email and text messages.[12] This is the largest penalty ever imposed for sending spam in New Zealand.

25. Internal Affairs is also the supervisory agency that monitors trust and company service providers for compliance with their obligations under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009. This Act seeks to deter and detect money laundering and terrorism financing, contribute to public confidence in New Zealand's financial system, and bring New Zealand into line with international standards. It includes various enforcement actions including civil penalties of up to $200,000 in the case of an individual, and $2 million in the case of a body corporate.

26. These penalties are imposed by the High Court on the application of the relevant supervisory agency, based on a civil standard of proof and with the Court taking into account "all relevant matters". These include the nature and extent of the act, the likelihood, nature, and extent of any damage to the integrity or reputation of New Zealand's financial system, the circumstances of the case, and whether the agency has been previously found to have engaged in similar conduct.[13]

27. Inland Revenue also has the power to apply civil penalties alongside or instead of criminal penalties. IR applies civil penalties such as late filing or payment penalties and shortfall penalties directly, rather than applying to a court for their imposition.

28. These other regulatory regimes demonstrate the utility of civil penalties as a valuable tool as appropriate in the particular regulatory context.

---

[11] Commerce Commission *Enforcement Response Guidelines*, October 2013, http://www.comcom.govt.nz/the-commission/commission-policies/enforcement-response-guidelines/
[12] *Chief Executive of the Department of Internal Affairs v Image Marketing Group Ltd* [2014] NZHC 139.
[13] Anti-Money Laundering and Countering Financing of Terrorism Act 2009, s 90(4).

International use of civil penalties for privacy breaches

29. Internationally, it is recognised that privacy and data protection regulators need a variety of potential sanctions available, including civil penalties or a fining power, to be able to effectively respond to serious, persistent or egregious breaches and non-compliance. Australian privacy legislation, UK data protection legislation, and the EU General Data Protection Regulation (GDPR) all now include significant penalty provisions. Countries in the Asia Pacific region, have also implemented data protection law including civil penalties or administrative sanctions in their range of enforcement options.[14]

30. The United States Federal Trade Commission, which operates to protect consumers and enhance competition over broad sectors of the economy, can also obtain civil monetary penalties for violations of certain privacy statutes and rules.[15] The FTC has successfully brought enforcement actions protecting the privacy of consumer information against large companies including Google, Facebook, Twitter and Microsoft.[16]

Australia

31. The Privacy Act 1988 (Cth) empowers the Australian Information Commissioner to apply to the Federal Court or Federal Circuit Court for an order that an entity alleged to have contravened a civil penalty provision in that Act pay the Commonwealth a penalty.[17] Civil penalty provisions include:

    a) A serious or repeated interference with privacy (s 13G)[18].

    b) Various civil penalty provisions in relation to credit reporting.[19]

32. If the court is satisfied that the entity or person has contravened the civil penalty provision, it may order the entity or person to pay such penalty as the court determines appropriate. In determining the penalty to be imposed, the Court must take into account all relevant matters, including:[20]

    a) The nature and extent of the contravention.

    b) The nature and extent of any loss or damage suffered because of the contravention.

---

[14] See the Personal Information Protection Act 2011 in South Korea and the Act on the Protection of Personal Information 2003 in Japan.
[15] These include the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and the Telemarketing Sales Rule.
[16] See for example the $22.5 million civil penalty paid by Google to settle FTC charges that it misrepresented privacy assurances to users of Apple's Safari internet browser https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.
[17] Section 80W. Section 79 of the Personally Controlled Electronic Health Record (PCEHR) Act also empowers the Commissioner to apply to a court for a civil penalty in certain circumstances.
[18] The maximum penalty for breaching this provision is 2000 'penalty units' as given value by the Crimes Act 1914 (Cth) – currently a maximum of $420,000.
[19] Part IIIA. These provisions carry a maximum penalty of 500, 1000 or 2000 penalty units, or $105,000, $210,000 or $420,000.
[20] Section 80W(6) of the Privacy Act and s 79(6) of the PCEHR Act.

c) The circumstances in which the contravention took place.

d) Whether the entity (or person) has previously been found by a court in proceedings under the Australian Privacy Act or PCEHR Act to have engaged in any similar conduct.

33. According to the Office of the Australian Information Commissioner (the OAIC), the purpose of a civil penalty order is to financially penalise an entity or person, not to compensate individuals adversely affected by the contravention. The OAIC will not seek a civil penalty order for all contraventions, and "is unlikely to seek a civil penalty order for minor or inadvertent contraventions, where the entity or person responsible has cooperated with the investigation and taken steps to avoid future contraventions."

34. The OAIC has established a range of relevant factors in considering whether a particular interference with privacy is serious and whether to seek a civil penalty order. The OAIC will consider whether one or more of the following factors is present:

a) The interference with privacy is particularly serious or egregious in nature.

b) The entity has a history of serious interferences with privacy.

c) The OAIC reasonably considers the serious interference with privacy arose because of a failure by the entity to take its privacy obligations seriously, or a blatant disregard by the entity for its privacy obligations.

d) The entity failed to take reasonable steps to correct and improve its privacy practices following earlier interferences with privacy.

e) The repeated privacy interferences demonstrate a failure by the entity to take its privacy obligations seriously, or a blatant disregard by the entity for its privacy obligations.

f) The contraventions comprising the repeated privacy interferences are more serious in nature.

g) Interferences with privacy have occurred on a greater number of occasions.

h) The repeated privacy interferences occur within a short period of time.

The OAIC's *Privacy regulatory action policy* emphasises that the use of civil penalties is to punish serious interference, egregious or blatant disregard, and repeated breaches.

35. The level of discretion and judgment available to the OAIC in determining whether to seek a civil penalty order, and whether the interference with privacy is so egregious as to warrant seeking a civil penalty order under s 13G, provides the Australian Commissioner with the necessary flexibility to appropriately administer the Australian privacy legislation.

United Kingdom

36. The United Kingdom Information Commissioner's Office (ICO) has the power to issue civil monetary penalties of up to £500,000 for serious breaches of the Data Protection Act and the Privacy and Electronic Communications Regulations. The Information Commissioner is able to serve a monetary penalty notice if he is satisfied that:

    a) There has been a serious contravention of a data protection principle, and

    b) the contravention was of a kind likely to cause substantial damage or substantial distress, and

    c) the data controller knew or ought to have known that there was a risk the contravention would occur, and that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but failed to take reasonable steps to prevent the contravention.

37. In 2014, the ICO undertook a review of the impact of these civil penalties, in order to assess the extent to which civil penalties influence or improve data protection compliance and practice by organisations. This research was also commissioned in advance of the European Commission's proposals for the EU General Data Protection Regulation.[21]

38. That review identified that the ICO uses civil penalties "as both a sanction and a deterrent against a data controller or person who deliberately or negligently disregards the law", with an overarching goal of promoting compliance and improving public confidence.[22] The research indicated that civil penalties are effective at improving compliance, both directly for offending agencies and as a useful deterrence and incentive for other agencies.

European Union and General Data Protection Regulation (GDPR)

39. The GDPR allows for significant fines on data controllers and processors for non-compliance.[23] The new GDPR fines are described as "rules with teeth and deterrent fines."[24] Guidance around GDPR penalties refers to the importance of administrative fines being "effective, proportionate and dissuasive, leaving the opportunity for early cases of non-compliance to be fined high amounts to set an example for other companies to pay more attention to ensuring compliance."[25]

40. These fines are administered by individual member state supervisory authorities, taking into account the following 10 criteria to determine the appropriate amount:

---

[21] ICO *Review of the impact of ICO Civil Monetary Penalties.*
[22] Above, p 2.
[23] Articles 83 and 84. The GDPR establishes lower level fines of up to €10 million or 2% of the worldwide annual revenue of the prior financial year (whichever is higher) and upper level fines of up to €20 million or 4% of the worldwide annual revenue of the prior financial year (whichever is higher), depending on which article(s) of the GDPR are infringed.
[24] European Commission – press release, Brussels, 24 January 2018.
[25] GDPR Associates, *Understanding GDPR Fines* https://www.gdpr.associates/what-is-gdpr/understanding-gdpr-fines/

a) Nature of infringement: number of people affected, damage they suffered, duration of infringement, and purpose of processing

b) Intention: whether the infringement is intentional or negligent

c) Mitigation: actions taken to mitigate damage to data subjects

d) Preventative measures: how much technical and organisational preparation the firm had previously implemented to prevent non-compliance

e) History: past relevant infringements and past administrative corrective actions

f) Cooperation: how cooperative the firm has been with the supervisory authority to remedy the infringement

g) Data type: what types of data the infringement impacts

h) Notification: whether the infringement was proactively reported to the supervisory authority by the firm itself or a third party

i) Certification: whether the firm had qualified under approved certifications or adhered to approved codes of conduct

j) Other: other aggravating or mitigating factors may include financial impact on the firm from the infringement.

Privacy Commissioner
Te Mana Matapono Matatapu

Appendix B

Background paper – enhancing agency accountability for compliance

1. Amending the Bill to request reporting on steps to compliance

1.1 This paper sets out background information to the Privacy Commissioner's recommendation that the Bill make provision for agencies to report to the Privacy Commissioner on request, at any time, on steps taken by the agency or proposed to be taken to ensure its compliance with the Privacy Act.[1]

1.2 While the Bill's new compliance notice power will enable the Commissioner to respond more effectively to identified issues of non-compliance, this is contingent on a breach of some kind. The extent to which the Commissioner can proactively identify and address systemic compliance issues in the absence of a specific breach or incident is not clearly expressed in the Bill. The amendment to clause 201 is therefore necessary to improve the Commissioner's effectiveness in responding to emerging systemic issues.

1.3 The amendment would improve proactive compliance without unduly increasing agency compliance costs. It would ensure the Commissioner has the necessary flexibility to respond proactively to emerging issues, aligns with international best practice and reflects the revised OECD principles (2013).[2] This new power would also enhance public trust and confidence in effective regulation and the Privacy Commissioner's role to uphold individual privacy rights, particularly in light of the ongoing digital transformation and expanding uses of personal information by both the public and private sector.

1.4 The amendment has a number of benefits. These include promoting a positive compliance culture and reducing the risk of breaches and complaints;[3] normalising agency best privacy practice, and enhancing agency privacy maturity[4]; and promoting public trust and confidence in effective privacy regulation. It would also support responsive privacy regulation, so the Commissioner can address serious risks to privacy before breaches occur and complaints emerge, as well as responding to patterns of non-compliance.

1.5 The proposed approach imposes a lower compliance burden on agencies than the alternative mandatory audit powers used in other jurisdictions, and recommended by the

---

[1] For background discussion, see Privacy Commissioner Report to the Minister of Justice under s 26 of the Privacy Act; Six Recommendations for Privacy Act Reform (February 2017), recommendation 3. https://privacy.org.nz/assets/Files/Reports-to-ParlGovt/OPC-report-to-the-Minister-of-Justice-under-Section-26-of-the-Privacy-Act.pdf

[2] The OECD accountability principle provides that a data controller should be accountable for complying with measures that give effect to the other principles. The OECD basic principles are reproduced in the Privacy Bill, Schedule 9.

[3] This includes strengthening governance of agency decision making and management of activities of agency staff that design and operate systems, to promote compliant behaviour.

[4] Including the take up of Privacy Management Plans and Privacy Impact Assessment tools.

Law Commission in 2011.[5] It is also more flexible than other options such as mandating every agency to produce a Privacy Management Plan.[6] The new provision would have some cost implications for agencies in terms of developing compliance procedures and demonstrating their compliance to the Privacy Commissioner by responding to requests for information. However these costs would largely be offset by reduced compliance failures and the associated resources needed for complaints investigations and settlement.

1.6 The Privacy Commissioner suggests that the proposed amendment can readily be achieved by adding two short sub-clauses to clause 201, along the lines of the following:

201 ~~Privacy officers~~ Agency accountability for ongoing compliance

(1) *An agency must appoint as privacy officers for the agency 1 or more individuals whose responsibilities include –*
   a. *The encouragement of compliance, by the agency, with the IPPs:*
   b. *Dealing with requests made to the agency under this Act:*
   c. *Working with the Commissioner in relation to investigations conducted under **Part 5** in relation to the agency:*
   d. *Ensuring compliance by the agency with the provisions of this Act.*

(2) *Each agency shall take such other steps as are, in the circumstances, reasonable to ensure its ongoing compliance with the Act.*

(3) *The Commissioner may, at any time, require an agency to report to the Commissioner in writing, as the Commissioner may reasonably require, on the steps the agency has taken or proposes to take to ensure its ongoing compliance with the Act.*

1.7 Clause 201 is the existing obligation agencies have to appoint a Privacy Officer, whose responsibilities include ensuring the agency's compliance with the provisions of the Act. The proposed amendment would strengthen this provision to include an obligation on agencies to take other reasonable steps to ensure compliance, and respond to any reasonable request from the Commissioner about the agency's compliance measures that are established or proposed.

2. Why is the amendment necessary?

2.1 Many agencies routinely handle sensitive personal information about individuals and need to do so responsibly in order to avoid privacy harm resulting to the individuals concerned. Agencies should therefore be accountable to the individuals whose information they hold and should be prepared to demonstrate that accountability to the Privacy Commissioner on request.

---

[5] Law Commission *Review of the Privacy Act 1993*, (NZLC R123, 2011) R64. The recommendation was rejected by the former Government on the basis that the Privacy Commissioner's own motion investigation powers could be enhanced.

[6] See Privacy and Personal Information Protection Act 1998 (NSW), s 33; Privacy (Australian Government Agencies – Governance) APP Code 2017.

2.2 The additional provision is within the scope of the key reform in the Bill of strengthening the Commissioner's information gathering powers[7] and is necessary to support the stated overall goal of the reforms in ensuring New Zealand has a privacy regime more focussed on early intervention and prevention of risks rather than after-the-fact remedies.[8]

2.3 Other key reforms in Part 6 of the Bill, mandatory breach notification and the compliance notice power, are intended to promote early intervention and risk management by agencies, rather than the Commissioner relying solely on people making complaints following a privacy breach. However there is a potential gap in the regulatory responses available to the Commissioner under the Bill.

2.4 While the Bill signals a change from a primarily complaints-based or reactive system of oversight, to a system that facilitates proactive oversight of privacy risk, the Commissioner's ability to influence an agency's practices may be targeted primarily to cases where a specific breach has occurred (before a compliance notice can be issued) or a complaint investigated.[9] While the Privacy Commissioner can inquire into matter if it appears the privacy of individuals may be infringed,[10] there is a potential gap as to the extent to which systemic issues can be explored before non-compliance becomes apparent.

2.5 The Privacy Commissioner proposes this be clarified by expressly stating the compliance obligations of agencies in clause 201 of the Bill and providing an explicit basis on which the Commissioner can seek a report about agency practices to manage privacy risk. The amendment would help promote a compliance culture within agencies and create incentives for agencies to develop the necessary proactive approach to privacy management.[11]

2.6 The reform would also enhance public trust and confidence that the Privacy Commissioner can ask agencies to verify about their privacy compliance processes. This is necessary as the accessibility of comprehensible publicly available information from agencies about their privacy practices can be variable.

---

[7] Explanatory Note, p 2. The Commissioner currently has information gathering powers in ss 92 and 93 of the Privacy Act 1993 that allows the Commissioner to demand information from an agency that is relevant to an investigation. The Bill's strengthening of the information gathering power is limited to a technical amendment in clause 92 that will allow the Commissioner to set the timeframe by which the information is to be provided (so that an agency can no longer unilaterally extend the applicable time period).

[8] Cabinet Social Policy Committee, Reforming the Privacy Act 1993, paras 4, 29, 41. https://www.justice.govt.nz/justice-sector-policy/key-initiatives/privacy/

[9] Under the Bill, the Commissioner's ability to make inquiries of the agency in question is tied to a formal investigation, a Commissioner inquiry or circumstances where the Commissioner is considering the issue of a compliance notice: Privacy Bill, clauses 92,129, 203.

[10] Privacy Bill, clause 14(1)(i).

[11] This includes improving the uptake of privacy management tools such as Privacy Impact Assessments (PIA) and Privacy Management Plans (PMP). These tools look into the privacy risks associated with particular projects, can be used as agency wide assessments of current practice, and also demonstrate to staff and stakeholders the steps taken by an agency to uphold the privacy principles and privacy proficiency generally.

3. When would the provision be used?

3.1 The proposed provision would allow the Privacy Commissioner to require an agency to report with sufficient information to demonstrate its compliance with the agency's privacy obligations. This could be useful in response to any suspicion of a risk to privacy from an agency's practices; but is also flexible to allow the Commissioner to respond proactively to emerging issues, within resource constraints.

3.2 The Privacy Commissioner's Office receives a number of enquiries that can raise concerns about an agency's practices but that do not meet the necessary threshold for investigation. It would be useful for the Bill to include provision for the Privacy Commissioner to seek a report on agency compliance measures, as appropriate. This would allow the Commissioner to receive assurance from an agency that privacy risks have been identified and managed proactively to reduce the potential for privacy breaches to arise and privacy complaints to emerge.

3.3 One example where the provision could prove valuable is where an individual believes the agency is collecting more information than is necessary for their lawful purposes, potentially in breach of IPP 1. It can be difficult for an individual to show specific privacy harm has been caused to them from the collection of their personal information in order to trigger a complaint investigation. In cases like these, there is a public interest in the Privacy Commissioner questioning an agency about the compliance of its collection practices, before deciding whether a higher level response is appropriate.

3.4 The proposed amendment would facilitate a relatively low-level enforcement response which is intended to educate agencies and encourage them to establish and maintain their privacy management practices. The existence of a Privacy Commissioner discretion to seek reporting on compliance reminds agencies of their obligations. This approach would be a suitable precursor intervention prior to escalating to a more formal regulatory step as necessary. It would allow the Commissioner to obtain initial assurance where there are potential systemic issues within an agency (that create privacy risk to a large number of individuals).

3.5 The provision would be supported by a published Privacy Commissioner policy on regulatory enforcement responses, outlining the considerations the Commissioner would apply before requiring an agency to report. Much will depend on the circumstances of the case including the potential risk of privacy harm and the responsiveness of the parties involved.

3.6 The additional provision would not need to be used routinely. Most agencies want to comply with the law and put in place the necessary organisational processes to do so. To assist them, OPC conducts education sessions and provides online training modules. OPC aims to inform agencies about privacy enhancing practices to encourage compliance with the Act and to minimise compliance costs. These proactive assistance interventions are sufficient to ensure compliance in most instances.

3.7 An express provision to allow the Privacy Commissioner to seek reporting on compliance will improve privacy outcomes by encouraging the take-up of proactive privacy

management options. There will always be some agencies that operate in breach of the law, or without due regard to the risk of a privacy breach, whether intentionally or not. It is therefore important that the Privacy Commissioner is suitably equipped with flexible compliance and enforcement tools at the right level, in order to respond appropriately to emerging privacy risk. There are particular risks to privacy when agencies adopt new technology or establish new ventures that use personal information to produce products or services or to make efficiency gains.

4. Strengthening the reforms in the Bill

4.1 The intent of the Bill's reforms, as noted in the response to the Law Commission review by the former Government, is that the Privacy Commissioner be able to investigate emerging issues before serious harm occurs and for proactive assessment of agencies' systems and practices where privacy concerns have been identified. The Government response noted that New Zealand needs a privacy regime that will enable the early identification and investigation of, and response to, systemic privacy risks.[12]

4.2 Important reforms in the Bill, such as the compliance notice power (Part 6(2)) and mandatory breach notification (Part 6(1)) will improve the regulatory framework. However, these reforms need to be supported by ancillary provisions that allow the Commissioner to gather information from a variety of sources to inform the appropriate and timely regulatory response in the circumstances. Amending clause 201 would be useful to close a potential gap in the regulatory design of the legislation, and support new features of the Bill.

4.3 Mandatory breach notification is an important development that will inform the Commissioner about privacy breaches as they occur. The Commissioner recommends this be enhanced to allow him to require follow up reporting by the agency in the period after initial notification.[13] However, this new feature of the Bill is directed to oversight of specific privacy breaches, and does not provide for proactive information requests unless grounds are established that warrant an investigation.

4.4 The scope of the new compliance notice power in Part 6(2) of the Bill is focussed on addressing a particular action that is a breach of the Act and, while it can be used to address issues before complaints arise, it does not require an agency to proactively demonstrate that it has appropriate processes and policies in place to generally comply with its privacy obligations. Requiring reporting about compliance practice by an agency may be a useful step for the Commissioner to take prior to issuing a compliance notice, either to confirm whether or not a compliance notice is warranted, or to confirm the matters to be addressed by a compliance notice.

4.5 The proposed amendment would therefore ensure that there is an appropriate "pre-cursor" response option to the new compliance notice power. It would facilitate suitable

[12] Supplementary Government response to Law Commission Review of the Privacy Act 1993 (May 2014) https://www.justice.govt.nz/justice-sector-policy/key-initiatives/privacy/

[13] Recommendation B.6.x.

follow-up steps to a serious breach notification, particularly in response to multiple notifications from an agency.

4.6 The proposed amendment is consistent with existing powers in the Bill to require information from agencies on a confidential basis in investigations or inquiries, but would provide explicit scope for agency reporting on compliance processes more generally, as well as incentivising agencies to proactively manage their privacy risk.

5. Domestic comparisons

5.1 The new provision can be regarded as a moderate intervention, sitting at a fairly low level in the regulatory enforcement pyramid. The Worksafe inspection regime established as part of the Health and Safety at Work Act 2015 provides a comparable example (although the HSW model would sit higher in the regulatory enforcement pyramid than the proposed amendment to clause 201 of the Bill, that is limited to agencies providing compliance reporting on request).

5.2 Worksafe health and safety inspectors carry out workplace assessments. These inspections are proactive planned visits, not usually triggered by a report of serious harm or a health and safety complaint. The function of these inspections and assessments is to monitor and enforce compliance. They operate as a mechanism by which workplaces can demonstrate their compliance with the Health and Safety at Work Act, identify any issues, and work proactively with the regulator to improve their practices.

6. International considerations

6.1 New Zealand's Privacy Act 1993 was drafted in accordance with the OECD's *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*.[14] In the 2013 *Privacy Framework Guidelines and Supplementary Explanatory Memorandum*, the OECD emphasised the importance of agency accountability in protecting individual privacy. The provision proposed would support the privacy legislation's continued alignment with the OECD guidelines.

6.2 The principle of accountability is a cornerstone of the new EU GDPR. Businesses will have to "demonstrate" compliance with the principles. This involves implementing more demonstrable processes and maintaining a proactive approach. The GDPR provides a set of tools to help demonstrate compliance, some of which are mandatory. For example a Data Protection Impact Assessment (DPIA) is mandatory in some circumstances.

6.3 Australia's privacy principle 1 sets out the obligation to manage personal information in an open and transparent way, requiring "such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that ensure the entity complies with the privacy principles and will enable the entity to deal with inquiries or complaints about compliance."[15] Australian Government agencies will soon be required to have a privacy management plan under the Australian

[14] Privacy Act 1993, long title.
[15] Privacy Act 1998 (Cth), Schedule 1.

Government Agencies Privacy Code which commences on 1 July 2018.[16] The Code sets out specific requirements and key practical steps that agencies must take as part of complying with Australian Privacy Principle 1.2, including the requirement that agencies must have a privacy management plan.

6.4 Australian Government agencies are not required to submit their privacy management plans to the Australian Information Commissioner under the Code, but may be required to provide them as part of an assessment, a proactive compliance tool that Australian Commissioner uses to assess whether personal information is being maintained and handled by an entity as required by law.[17] There is a broad discretion for the Australian Information Commissioner to undertake privacy assessments, where this contributes to achieving the goal of promoting and ensuring the protection of personal information, and could include an assessment of an agency's compliance with the Code. The general assessment methodology includes asking the target agency to produce documentation is support of their compliance with the Code, including their privacy management plan.

6.5 It is notable that most other modern data protection authorities (including Canada, Australia, Spain and other European countries) have proactive Commissioner audit powers. The Law Commission recommended mandatory audit powers be included as an element of the New Zealand privacy reforms[18] but this recommendation was not taken up in the government response to the Law Commission's report, nor been included in the Bill.

6.6 The Privacy Commissioner does not call for the recommendation regarding audit powers to be revisited, unless there is a strong call in public submissions that these regulatory powers should now be included, or the Committee considers that these gaps in the regulatory scheme should be re-examined. Nevertheless, the provisions in the Bill need to be enhanced to ensure the regulatory toolbox at Commissioner's disposal allows him to make the appropriate inquiries of agencies about how they propose to comply with their obligations.

---

[16] Office of the Australian Information Commissioner *Privacy (Australian Government Agencies – Governance) APP Code* (2017) www.oaic.gov.au/privacy-law/privacy-registers/privacy-codes/privacy-australian-government-agencies-governance-app-code-2017

[17] Privacy Act 1988 (Cth), s 33C. www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-7-privacy-assessments

[18] NZLC 123, R64.

Privacy Commissioner
Te Mana Matapono Matatapu

Appendix C

Background paper: removing the role of the Director of Human Rights Proceedings in privacy cases

1. This paper provides background information to the Privacy Commissioner's recommendation that the Bill implement the Law Commission's recommendation 55:[1]

> *The role of the Director of Human Rights Proceedings should be removed in privacy cases. The Privacy Commissioner should decide which cases are to proceed to the Human Rights Review Tribunal and act as the plaintiff in those cases, and perform the other roles currently performed by the Director.*

2. This Bill carries over the current model in the Privacy Act that splits functions between the Privacy Commissioner and the Director of Human Rights Proceedings in relation to privacy complaints. If the Commissioner considers a privacy complaint raises issues of importance such that proceedings should be brought in the Human Rights Review Tribunal on the complainant's behalf, then he or she refers the complaint to the Director of Human Rights Proceedings. The Director considers the matter afresh. In recent years the Commissioner has made few referrals and the Director rarely decides proceedings should not be brought.[2] Proceedings are brought in the Director's name, but the Commissioner is liable for any costs awards.

3. The Commissioner supports the Law Commission's conclusion. The current split model was considered necessary twenty-five years ago, but it is no longer justified, in particular given the Bill is being modernised.

This recommendation would promote an efficient and effective complaints process

4. The Law Commission recommended that the Commissioner brings proceedings directly in the Tribunal because it considered the current model "duplicative and inefficient".[3] The Commissioner agrees that reform in this area would reduce unnecessary compliance costs for complainants and other parties when they access the Tribunal, and enhance individual privacy by promoting more effective resolution of complaints.

5. The Director considers a complaint afresh on the same facts and establishes new relationships with the parties. There is scope to reduce duplication of processes by removing the Director's role and allowing the Commissioner to take proceedings directly. At the point of deciding whether to institute proceedings in the Tribunal, the Commissioner already has a relationship with the parties and holds the background to the complaint in-house.

---

[1] NZLC R123 Recommendation 55.
[2] The Commissioner made ten referrals between 1 July 2014 and 31 December 2017. The Director has filed proceedings in seven cases. One decision is outstanding, one was settled before proceedings were filed and in the final case the Director declined to take proceedings after the complainant passed away.
[3] NZLC R123 at 6.33.

6. The Commissioner considers that in addition to duplication, the split model is inefficient given the relative expertise of the two offices. Privacy represents a minority of the Director's workload compared to human rights issues. The Director considers individuals' applications for representation, and represents them in unlawful discrimination complaints under Part 1A (complaints about legislation, government policy or practice) and Part 2 (employment complaints across all sectors and unlawful discrimination by business and non-governmental agencies) of the Human Rights Act 1993. Part 1A complaints are particularly complex. An overview of the balance between privacy and human rights matters in recent years is set out below.

2016/17

7. In the year ended 30 June 2017 the Commissioner referred four privacy complaints to the Director. The Director filed proceedings in respect of three of these complaints but declined in respect of the fourth after the complainant passed away. In respect of Human Rights Act complaints the Director agreed to provide representation in respect of 19 complaints, including under both Part 1A and Part 2 of that Act. [4]

2015/16

8. In the year ended 30 June 2016 the Commissioner referred two privacy complaints to the Director. The Director filed proceedings in respect of one of these complaints and settled the other. In respect of Human Rights Act complaints the Director agreed to provide representation in respect of 17 complaints.[5]

2014/15

9. In the year ended 30 June 2015 the Commissioner referred two privacy complaints to the Director. The Director filed proceedings in respect of both complaints. In respect of Human Rights Act complaints the Director agreed to provide representation in respect of nine complaints.[6]

10. Over these three years, the time taken between the Commissioner referring a complaint to the Director and an outcome (the Director filing proceedings, declining to file proceedings or settling the complaint) ranged from 4 to 19 months, with the average time taken being 9 months.

11. Further efficiency would arise from privacy cases being brought solely by the Commissioner, a privacy specialist. The Commissioner and his staff work entirely on privacy matters. They are obviously familiar with applying the Act and with working with the parties to privacy disputes. This would save time and effort compared to the current system, which requires the Director's office to turn its mind to a privacy case relatively rarely compared to its considerable human rights workload.

---

[4] Human Rights Commission and Director of Human Rights Proceedings Annual Report 2016/17.
[5] Human Rights Commission and Director of Human Rights Proceedings Annual Report 2015/16.
[6] Human Rights Commission and Director of Human Rights Proceedings Annual Report 2014/15.

12. It is also anomalous for the Commissioner not to have control over how the proceedings are argued yet to be liable for the costs.

13. Finally, this recommendation would simplify the process for the parties, who would only deal with one statutory office on their way to the Tribunal. To promote access to justice, legal processes should be as simple as possible for members of the public to understand. The Commissioner would implement appropriate processes to ensure parties are given opportunity to be heard and to settle the matter before proceedings are filed.

Allowing the Commissioner to bring proceedings would be consistent with other reforms under this Bill

Concerns about independence of the Commissioner's dispute resolution function

14. The previous government decided not to accept the Law Commission's recommendation in 2014 and cited the need to protect the Commissioner's dispute resolution function.[7] The Law Commission had considered but expressly rejected that argument.

15. In reviewing the complaints process the Commission took into account concerns held by a minority of submitters about a possible chilling effect on OPC achieving settlements. It ultimately found they were "outweighed by the speedier and more efficient arrangement which would result".[8] It reasoned that it is "far from clear" that the split model makes it easier to achieve settlements and that "it is not immediately apparent why someone should be less ready to settle because the intermediary has functions other than negotiation and persuasion."[9]

16. Bringing proceedings directly in the Tribunal would complement other reforms under this Bill that provide the Commissioner with more efficient and effective enforcement powers, including binding access directions and compliance notices. The Commissioner notes that there is no suggestion that these measures will undermine the integrity of the dispute resolution function. The current Act and the Bill require the Commissioner to use his best endeavours to secure a settlement of a privacy complaint.

OPC will already be increasing its litigation capability

17. The previous government was also concerned about resourcing for litigation within OPC.[10] The Commissioner notes that, given the new ability to issue binding access directions and compliance notices, there is likely to be less need for the Commissioner to bring proceedings in the Tribunal on an individual's behalf than the Director does now. Further, OPC will be required to have the litigation capability to enforce and defend compliance notices in addition to the current requirements, a more substantial volume of work.

---

[7] Office of the Minister of Justice *Reforming the Privacy Act* (Cabinet Social Policy Committee, May 2014)
[8] NZLC R123 at 6.38.
[9] NZLC R123 at 6.31.
[10] Office of the Minister of Justice *Reforming the Privacy Act* (Cabinet Social Policy Committee, May 2014).

18. The Commissioner can appear in any Tribunal proceeding or related proceedings in the courts other than those the Director has brought or decided to appear in at other times.[11] The Commissioner does appear when there is an issue of sufficient interest that warrants the Commissioner's expertise.[12]

19. The Commissioner also appears in cases in the ordinary courts, such as judicial reviews[13] and other matters, including a recent intervention in a Supreme Court case where one of the issues on appeal involved the Privacy Act.[14]

20. The change would be fiscally neutral as any adjustments to the Director's or OPC's funding would balance each other out.

International comparisons

21. Australian and Canadian legislation both provide for the privacy regulator's functions to include the ability to bring proceedings whilst also including a role in conciliating complaints.

Australia

22. The Office of the Australian Information Commissioner (OAIC) has a range of functions to respond to privacy complaints. The Commissioner must make a reasonable attempt to conciliate a complaint if he or she considers successful conciliation is reasonably possible. The Commissioner may also take enforcement and litigation action following an investigation, including commencing proceedings to enforce a determination or an enforceable undertaking, and the ability to apply for an injunction to restrain or direct a person in relation to a specific thing.[15]

Canada

23. The Canadian Privacy Commissioner also has a range of functions to respond to complaints under the Canadian Personal Information Protection and Electronic Documents Act. The Commissioner seeks early resolution and settlement of complaints. He or she can also apply for a hearing in the Federal Court (where various remedies are available) or appear on behalf of individuals who do so.

---

[11] Clause 104 of the Bill and s 86 of the Privacy Act 1993. The Director rarely exercises the right to appear in any case that the Director has not brought. Between 1 July 2014 and 30 June 2017 the Director considered 97 invitations from individuals to intervene in their privacy proceedings and only intervened in two cases. See Human Rights Commission and Director of Human Rights Proceedings Annual Reports.
[12] See, for example, *Koso v Chief Executive of Ministry of Business, Innovation and Employment* [2014] NZHRRT 39. The Commissioner is appearing in five matters that are currently before the Tribunal.
[13] See, for example, *Mitchell v Privacy Commissioner* [2017] NZAR 1706
[14] *R v Alsford* [2017] NZSC 42
[15] Australian Privacy Act 1988.

Drafting

24. The Law Commission's recommendation could be implemented by:

- amending clauses in the Bill that currently provide for the Commissioner to refer complaints to the Director[16] and instead providing the Commissioner with discretion to consider whether proceedings should be instituted;

- amending clause 102 of the Bill to provide the Commissioner with discretion to commence proceedings in the Tribunal;

- substituting further references to the Director for references to the Commissioner under various clauses.[17]

[16] Clauses 84, 87, 96, 98 and 99 of the Bill.
[17] Clauses 94, 95, 103, 104, 108, 204 and 206 of the Bill.