InternetNZ

InternetNZ Submission: Privacy Bill

Justice Select Committee

31 May 2018

InternetNZ

Table of Contents

1. InternetNZ welcomes the Privacy Bill

1.1 InternetNZ is an independent, membership-based charity, which works towards a better world through a better Internet. As part of that mission, we engage on policy issues related to the Internet.

1.2 New Zealanders see privacy as a key Internet issue. In 2016 and 2017, our research showed that 70% of New Zealanders were concerned about threats to personal data online.[1] More recently, stories about Cambridge Analytica have shown how international uses of data can have big effects on New Zealanders.

1.3 Privacy is a human right, and applies online just as it does offline. InternetNZ supports a trustworthy Internet, which protects, respects, and enhances the privacy of New Zealanders.

The Privacy Bill is a welcome update to our law

1.4 We welcome the Privacy Bill as a long-awaited update to New Zealand's current privacy law. Now 25 years old, the current Privacy Act 1993 established privacy rights for New Zealanders, applying to all agencies, whether public or private, and whether large or small. By taking a flexible, principles-based approach, the current law has adapted remarkably well to unforeseen and substantial shifts in technology. The Bill retains those core features, and adopts recommendations from a 2011 review by the Law Commission.

Privacy is a core human right for the information age

1.5 Over the past 25 years, the Internet has fundamentally shifted the ways people use and share information. The first decade of our privacy law saw the broad adoption of desktop computers, of email and web browsers, and of online commerce. The second decade saw the dawn of smartphones and social media. We are more connected, our information more collected, than anyone would have thought possible in 1993.

1.6 InternetNZ's vision is a better world through a better Internet. We know that overall, New Zealanders see the Internet as hugely beneficial, with 88%

[1] "State of the Internet 2017", InternetNZ, <internetnz.nz/state-internet-report-2017>, p 10.

saying positives outweigh the negatives.[2] We also know that privacy and security is the biggest concern about the Internet.[3]

1.7 A better Internet requires robust and usable privacy protections. We welcome this Bill, which updates our law and takes steps in that direction.

1.8 We would welcome the chance to speak to the Select Committee in person. For more information, please contact James Ting-Edwards, via james@internetnz.net.nz or on 0211565596.

Jordan Carter

Group Chief Executive

[2] "2017 Internet research", InternetNZ, <internetnz.nz/2017-internet-research>.
[3] "State of the Internet 2017", InternetNZ.

2. Summary of Submission

The current Bill is a welcome update...

2.1 InternetNZ welcomes the Privacy Bill. To unlock the Internet's benefits, New Zealanders need to trust that their information will be protected. The Bill takes steps towards a robust, workable, and up-to-date privacy law which supports that trust.

2.2 We welcome provisions to enhance privacy protections online, including provisions on breach notification and overseas sharing of data. We also welcome broader changes to the framework, such as the compliance notice power, which will allow a flexible response to new and emerging privacy risks.

...But technology will continue to change privacy needs

2.3 Though we support the Bill, we also believe that it could be improved. In this submission, we highlight key issues for privacy and the Internet. We offer recommendations for further steps to support a robust, workable, and up-to-date privacy framework.

Consider European adequacy and the GDPR

2.4 New Zealand's privacy framework is currently recognised as "adequate" by the European Union (EU). Adequacy substantially simplifies compliance for international and export-focused agencies in New Zealand, but cannot be taken for granted. The European General Data Protection Regulation (GDPR) requires an EU review of our adequacy by 2022.[4] We recommend a review focused on EU adequacy to be completed by mid-2020.

Align breach notification with overseas best-practice

2.5 We welcome data breach notification requirements. Data breaches are a key source of privacy risks, with breaches to May 2018 affecting 10 billion records world-wide.[5] To mitigate risks from breaches, we want a workable and meaningful notifications framework, that aligns with overseas best-practice. To achieve that alignment, to avoid a risk of "notification fatigue" for New Zealanders, and to make obligations workable for agencies, we propose changes to the threshold for notifiable breaches. We attach recommended drafting to implement these changes as **Appendix A.**

We need a privacy framework for the Internet age

2.6 Privacy interests and concerns are deeply connected with changing technology. Beyond the moves in the current Bill, it is critically important to ensure that our privacy framework is and remains up-to-date.

2.7 Over coming years, rapid changes in technology will continue, with large potential privacy impacts. We propose some key changes, which in our view

---

[4] Regulation (EU) 2016/679, of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 ("GDPR") <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>.

[5] Information is Beautiful, "World's Biggest Data Breaches" (2018), http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

would update our framework, and help it to stay up to date. Our proposals are:

a) extending the access right under IPP6, so individuals can request access to the purpose for which their information is held

b) broadening the regulatory toolkit available to the Office of the Privacy Commissioner, allowing a spectrum of responses which recognises that most agencies want to support good privacy practice

c) completing regular reviews of our privacy framework, and implementing changes more frequently, to match rapidly changing technology.

...And an opportunity to discuss potential changes

2.8 Along with others interested in privacy, we are proposing new measures to update and enhance the Privacy Bill. These privacy measures will have implications for every organisation in New Zealand. We think it is important to allow a further phase of engagement on the detail of changes to the Bill. Therefore, we ask that the Committee consult the public on further changes to the Bill before reporting back to the House.

3. Consider steps to keep EU adequacy

3.1 New Zealanders deserve privacy protections that align with international best-practice. While retaining a privacy framework that suits our own context, we should consider what is required to retain adequacy, and what lessons New Zealand might take from the GDPR as a modern data protection law.

Our technology sector benefits from EU adequacy

3.2 In 2012, the European Union awarded New Zealand adequacy status under the European data protection framework.[6] Gaining adequacy was a substantial effort, requiring us to show that while different from Europe's framework, New Zealand's law and broader institutions offered robust protections for privacy interests.

3.3 The benefit of adequacy is easier compliance for New Zealand organisations, particularly those exporting to Europe. Exporting products requires information about customers. This information includes personal data, whether that is an email address, a delivery address, or the network address of a client's computer.

3.4 The alternative to adequacy would be for each New Zealand organisation to enter contracts, or take other steps to meet European requirements. That would be a substantial overhead, which many businesses and other organisations might struggle to meet.

3.5 New Zealand has the opportunity to increase weightless, high-value exports via the Internet. Europe is a leader on privacy standards and a key export market, for which the Government is now seeking a free trade agreement. In that context, retaining adequacy should be a key priority for privacy law reform.

We should not take adequacy for granted

3.6 The GDPR came into effect on May 25, unifying and raising data protection requirements across Europe. The Privacy Bill recognises some of the same concerns, and takes some of the same steps as the GDPR. New measures such as compliance notices, breach notification rules, and controls on offshore sharing improve our framework and strengthen our case for retaining European adequacy.

3.7 Nonetheless, there are protections and requirements under the GDPR which the Bill does not adopt. In particular, the GDPR:

a) requires high standards for up-front disclosure and consent

b) requires a "right to erasure" and a "right to be forgotten"

c) introduces controls on automated decisions

d) requires "privacy by design" in the choice and use of systems.

[6] Office of the Privacy Commissioner, "NZ's 'Adequacy' under the EU Data Protection Directive" (2015), https://www.privacy.org.nz/blog/update-on-nzs-adequacy-under-the-eu-data-protection-directive/

New Zealand needs a plan to retain EU adequacy

3.8 New Zealand's current adequacy status is based on the 1995 Data Directive.[7] Within four years from May 2018, the European Commission will review New Zealand's adequacy against the new and higher GDPR privacy standard.[8] That review will be a holistic assessment of our national laws and institutions.

3.9 To maintain adequacy, we may need further reforms of our law. The four year deadline means any law reforms aimed at retaining adequacy would have to be completed by May 2022 at the latest. The Privacy Bill is an opportunity to consider and address adequacy requirements. However, with uncertainty about the implementation details of the GDPR, some aspects may be better addressed in a separate and targeted review. Retaining adequacy is extremely important to New Zealand.

3.10 We ask for a strong commitment to a targeted and time-bound review focused on retaining European adequacy for New Zealand to be completed by May 2020. This would provide a further 2 years to implement and bring into force necessary changes to ensure that New Zealand maintains it adequacy status.

New Zealand should adapt, not adopt GDPR provisions

3.11 As a modern data protection framework, the GDPR offers useful lessons. But New Zealand's privacy framework is different from Europe's, reflecting our different history, culture, and institutions. Our framework is based on flexible privacy principles and responses to harm, guarded and guided by a Privacy Commissioner. Where the GDPR controls uses of information based on consent and legal basis at the time of collection, our framework does so based on the current purpose for which an agency holds information. These differences mean we cannot simply adopt GDPR rules, but must adapt its lessons to our local context.

3.12 The flexible principles at the core of our privacy framework allow a response to harm, but do not otherwise require compliance or limit innovation. This flexible approach has adapted remarkably well to 25 years of change, and may be a useful approach to emerging interests and concerns. We identify key areas where adapting GDPR approaches could improve our privacy framework.

A new principle for explaining automated decisions?

3.13 The GDPR creates protections for and requirements on automated decisions. This is a developing area, and one where we would not recommend rushing to create specific regulations. Instead, if New Zealand were to consider similar protections to the GDPR, retaining a flexible approach would be important. Extending or creating an information privacy principle would be one way to do this.

3.14 We think the most important response to automated decisions is to allow for accountability, monitoring, and correction of mistakes. "Transparency" of the system or code may not help people to understand or respond to decisions.

3.15 In assessing standards of accountability, it may also be important to assess local context and distinguish public and private sector uses of algorithms.

---

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31 ("Data Directive").
[8] GDPR, Article 45 (3).

One option is to adapt GDPR requirements for access to "meaningful information on the logic" involved in automated decisions into one or more privacy principles, to allow for that flexible response to harm.[9]

Extending protection for data portability

3.16 We support consideration of data portability, as a meaningful protection for consumer choice. As applied to online services, this requires information to be available in a usable, machine-readable format. We think a principle requiring data portability deserves consideration. An alternative, proposed by the Privacy Foundation, is adding a new paragraph (g) to clause 62(1), to require that information an individual has provided be available in a transferable and machine-readable format.

Allow for engagement on new changes to the Bill

3.17 Privacy is a core human right. Along with other submitters, we are proposing substantive changes to improve and update the Bill. It is important that those changes work, and that they have legitimacy.

3.18 We recommend that the Committee undertakes another round of public consultation on new changes to the Bill before reporting back to the House.

Recommendations

3.19 We recommend:

a) a targeted review to consider New Zealand's adequacy status under the GDPR, concluding by May 2020 and implemented by May 2022

b) consideration of a new principle or principles to keep automated decisions explainable and accountable

c) extending protection for data portability, to allow individuals to access and transfer information in a usable and machine-readable format

d) conducting additional public consultation on new changes to the Bill before reporting back to the House.

[9] This is based upon the access right under GDPR Article 15.

4. Deliver best-practice breach notification

We welcome breach notification

4.1 Data breaches, accidental or otherwise, are increasingly important as a privacy concern. Over time, reported breaches have grown in size and frequency. Based on public reports, data breaches have now leaked a cumulative total of over 10 billion records worldwide. [10]

4.2 Notifying breaches to the Privacy Commissioner, and to affected individuals, is vital to monitoring and mitigating resulting privacy risks. Those risks can be substantial, going far beyond the discomfort of being identified. Information can be used for many purposes. Even trivial-seeming information may be combined with other sources, and can play a role in targeted advertising, and in efforts to compromise our accounts and passwords. Once leaked, our data is likely to be accessible around the world, and for a long period of time. As a result, leaks and breaches can pose ongoing risks for the privacy and security of New Zealanders. Notification is part of managing and mitigating those risks.

Align notification rules to overseas best-practice

4.3 New Zealanders deserve best-practice breach notification. Combined with practical concerns, as a small nation with strong international links, it makes sense to align our breach notification rules with overseas best-practice. With that alignment, it will be easier for agencies to comply, and easier to hold them to complying.

4.4 Australia and the European Union are obvious models. Australia is our closest trading partner, and draws on a similar history and institutions. The European Union is a substantial and growing trade partner, and its GDPR framework is likely to lead international practice on privacy and data protection.

4.5 We propose detailed drafting changes to the proposed breach notification rules at **Appendix A**. The aim of this change is to align with overseas models, reduce the risk of notification fatigue, and make notification rules workable for agencies.

An objective "serious harm" threshold for notifying individuals

4.6 The Bill's threshold for notifying individuals requires agencies to make a subjective assessment, focused on future harms. When faced with the urgent situation of a potential breach, agencies may struggle to do this well. The Bill's threshold is also set at a relatively low level. This risks notification fatigue, overwhelming people with information they cannot readily use.

4.7 We propose to raise the threshold for notifying individuals, requiring an assessment of whether serious harm is likely, on an objective "reasonable person" standard. In our view, this change:

a) **aligns** the notification threshold with those in Australia and under the GDPR

b) **allows** agencies to assess whether harm from a breach would be serious before notifying individuals

c) **requires** agencies to make that assessment on an objective standard

---

[10] Information is Beautiful, "World's Biggest Data Breaches" (2018), http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

d) **reduces** the risk of trivial or unhelpful notifications overwhelming individuals.

Allow for technical measures to mitigate privacy risks

4.8 Encryption and other technologies can be used to protect information against unauthorised access. Both the GDPR and Australian breach notification rules recognise that encryption may make a breach less harmful.

4.9 We propose wording changes at 120(1), creating an exception to align with overseas models, and to encourage proactive use of encryption to protect the privacy of New Zealanders.

4.10 This exception only applies to notifying affected individuals or the public. The Commissioner must still be notified of breaches. If the Commissioner views technical measures as inadequate, they could then issue a compliance notice requiring that affected individuals or the public are notified of a breach.

Make it clear that failure to notify breaches privacy principles

4.11 To balance the higher standard for notifying individuals, we propose a stricter standard for situations where notification is required.

4.12 Current wording provides that a failure to notify an individual where required "may" be an interference with privacy. We propose a drafting change at 119(5) so that failing to notify individuals "shall be deemed to" interfere with privacy. This allows the Commissioner to assess steps taken to mitigate a breach, and to issue a compliance notice requiring that affected individuals are notified.

Recognising breaches of genetic and biometric data as serious

4.13 We make these proposals to enable the potential benefits of the Internet, while managing risks to privacy, and risks of notification fatigue. At the same time, we recognise that people's biometric and genetic data is particularly sensitive. Our proposed drafting would deem breaches of biometric or genetic data to be serious ones, requiring notification to individuals. This reflects both the potential harm, and the fact that genetic and biometric information cannot be updated or changed to minimise future risks.

Recommendations

4.14 As set out at Appendix A, we recommend:

a) setting a higher threshold for notifying individuals, as an objective test of whether serious harm is likely

b) clarifying that failure to notify is an interference with privacy

c) recognising and encouraging the use of technology such as encryption to mitigate breaches, while allowing the Commissioner to assess this

d) recognising all breaches of genetic or biometric information as serious breaches, requiring notification to affected individuals.

5. A privacy framework for the Internet age

5.1 Privacy is an increasingly important right to New Zealanders. Shifts in technology mean our personal information is more important, across more areas of life, than ever before. This makes privacy protections increasingly important. Our privacy framework is the key control on how our personal information is collected and used, across business, government and elsewhere.

5.2 We see the need for a small number of minor amendments that could better allow New Zealanders, agencies and the Privacy Commissioner to implement a new Privacy Act in the Internet age. These are to:

a) extend the access right under IPP6, allowing individuals to request access to the purpose for which their information is held

b) provide a modern and broad regulatory toolkit to the Office of the Privacy Commissioner, allowing them flexibility to assist, enable, warn, or prosecute agencies in the service of better privacy protection

c) complete and implement regular reviews of the Privacy Act, on a shorter time-scale which reflects rapid changes in technology.

Consider extending the access right to include purpose

5.3 The Information Privacy Principles (IPP1-12) are at the core of our framework. For individuals, the access right under IPP6 is the basis for all other protections. By requesting access, individuals can see which agencies hold their information, and what information they hold.

5.4 Modern privacy protection is not just about whether information is held, but what it can be used for. Technology makes is easy to retain information, and to apply it for purposes which may go beyond the expectations of the individual at the time information was initially shared. Individuals should know why an agency holds their information, so they can assess whether it is being used in ways that go beyond that purpose.

5.5 We favour a simple and unified framework for access requests, in line with the submission of the Privacy Foundation. Additionally, to monitor the scope of use, the IPP6 access right should be expanded to include the purpose for which an agency holds information.

5.6 We think expanding the access right in this way could usefully increase privacy protection for individuals, without unduly burdening agencies. Knowing what is held, and why it is held, helps individuals to supervise the use of their information. This expanded access right would be relatively easy to pursue, as the Bill gives the Commissioner power to enforce access requests.

Give the Privacy Commissioner a broad toolkit

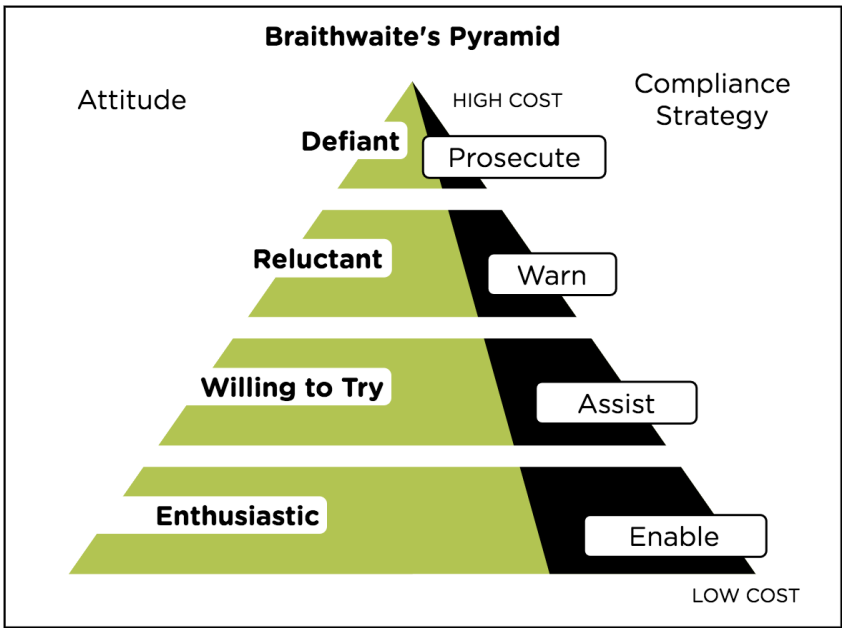
5.7 Both regulatory theory and regulatory law in New Zealand has advanced significantly since the 1990s when the current Privacy Act was enacted.

5.8 The Bill adds welcome new protections and powers, including the new compliance notice power held by the Commissioner. However, the framework under the Bill retains the Privacy Act's focus on complaints and penalties.

5.9 Given the speed of technological changes that can affect privacy, the need for New Zealand organisations to think broadly about privacy, and the implications of new services and technologies, we think that the Office of the Privacy Commission needs a broader, modernised regulatory toolkit. This toolkit should reflect compliance thinking from international experts and also New Zealand Government initiatives, such as the guide *Achieving Compliance: a guide for compliance agencies in New Zealand*.

5.10 Most organisations in New Zealand will be either enthusiastic, or willing to improve their privacy programmes and efforts. They need to be assisted and enabled to do so. (see Figure 1 which summarises the Braithwaite Pyramid, as presented in ***Achieving Compliance***). [11]

Figure 1



5.11 While the Privacy Bill is more than regulatory compliance law, the Office of the Privacy Commissioner has a clear compliance role. We recommend that Committee consider giving the Privacy Commissioner's office additional compliance tools such as formal warnings, and the ability to accept undertakings from agencies.

5.12 Recent New Zealand statutes have empowered a regulator with powers such as accepting undertakings or issuing warnings, for example:

a) Financial Markets Authority Act 2011

b) Health and Safety at Work Act 2015.

5.13 Under a broader compliance framework, the fines that the Human Rights Review Tribunal can impose on an agency who has breached the Act can, and should, go up.

5.14 With a suite of regulatory powers besides taking an agency to the Tribunal, only the most serious breaches should result in fines. Therefore, the civil or criminal fines associated with those cases should go up, and be in line with other regulatory models. As one example, the fine for wilful non-disclosure of financial information to the Financial Markets Authority is NZ$200,000. [12]

5.15 We understand that other submitters such as the Privacy Commissioner, and the Law Commission (in its 2011 report), recommend disestablishing the Director of Human Rights Proceedings. Creating a broader suite of tools for the Commissioner would also complement this proposal.

---

[11] Department of Internal Affairs, "Achieving Compliance" (2011), https://www.dia.govt.nz/diawebsite.nsf/Files/Achieving%20Compliance%20-%20A%20Guide%20for%20Compliance%20Agencies%20in%20New%20Zealand/$file/AchievingComplianceGuide_17July2011.doc

[12] See section 60 of the Financial Markets Authority Act 2011.

Keep our privacy framework up to date

5.16 The current Bill draws on the 1998 "Necessary and Desirable" report and the Law Commission's 2011 review of the Privacy Act. As privacy is increasingly important, and increasingly tied to changing technology, we need more regular and effective reviews to update our privacy framework.

5.17 Effective and modern privacy protection is important, and is not a party political issue. There has been broad Parliamentary support for past improvements to our privacy law. We ask members of the Committee, as the MPs most engaged with these issues, to seek a cross-Parliament commitment to updating our privacy law as technology changes.

Recommendations

5.18 **We recommend that the Select Committee:**

a) consider access to purpose as an extension of the IPP6 access right

b) provide the Privacy Commissioner with a broad toolkit, including options to guide and encourage privacy improvements from agencies, without having to take action through the Human Rights Review Tribunal

c) review the fines within the Bill to see whether they are out of step with fines available to other regulators

d) seek a cross-Parliament commitment to updating our privacy law as technology creates new opportunities and risks.

6. Conclusion

6.1 We welcome the Privacy Bill. In this submission we have made recommendations to support and improve the Bill. Privacy is a core human right, which is vitally important to enabling trust in and on the Internet.

6.2 We would welcome the chance to speak to the Select Committee in person. For more information, please contact James Ting-Edwards, via james@internetnz.net.nz or on 0211565596.

7. Summary of Recommendations

Consider steps to keep EU adequacy

7.1 We recommend:

a) a targeted review to consider New Zealand's adequacy status under the GDPR, concluding by May 2020

b) consideration of a new principle or principles to keep automated decisions explainable and accountable

c) extending protection for data portability, to allow individuals to access and transfer information in a usable and machine-readable format

d) allowing further engagement by consulting with submitters on new changes to the Bill before reporting back to the House.

Deliver best-practice breach notification

7.2 As set out at Appendix A, we recommend:

a) setting a higher threshold for notifying individuals, as an objective test of whether serious harm is likely

b) clarifying that failure to notify is an interference with privacy

c) recognising and encouraging the use of technology such as encryption to mitigate breaches, while allowing the Commissioner to assess this

d) recognising all breaches of genetic or biometric information as serious breaches, requiring notification to affected individuals.

Deliver a balanced framework for the Internet age

7.3 We recommend that the Select Committee:

a) consider access to purpose as an extension of the IPP6 access right

b) provide the Privacy Commissioner with a broad toolkit, including options to guide and encourage privacy improvements from agencies, without having to take action through the Human Rights Review Tribunal

c) review the fines within the Bill to see whether they are out of step with fines available to other regulators

d) seek a cross-Parliament commitment to updating our privacy law as technology creates new opportunities and risks.

Appendix A: Proposed drafting for breach notification

Notifiable privacy breaches and compliance notices

Subpart 1—Notifiable privacy breaches

117 Interpretation

(1) In this subpart,—

affected individual, in relation to personal information that is the subject of a privacy breach,—

(a) means the individual to whom the information relates; and

(b) includes an individual inside or outside New Zealand; and

(c) despite the definition of individual in **section 6**, includes a deceased person—

(i) if a sector-specific code of practice issued under **section 35** specifies that the code applies to information about deceased persons; and

(ii) to the extent that the code of practice applies 1 or more IPPs to that information

biometric information means personal information resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data; *[Drafting Note: cf GDPR, Article 4(14)]*

genetic information means personal information relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question; *[Drafting Note: cf GDPR, Article 4(13)]*

notifiable privacy breach means a privacy breach that a reasonable person would conclude is likely to result in ,—

(a) ~~has caused~~ any of the types of harm listed in **section 75(2)(b)(i) or (ii)** to a significant extent; or

(b) any of the types of harm listed in **section 75(2)(b)(iii)**~~to an affected individual or individuals or there is a risk it will do so~~

or is a privacy breach in respect of an affected individual's or affected individuals' biometric information or genetic information.

[Drafting Note: The rationale here is twofold: (1) to bring the threshold into line with the GDPR and Australia so that only serious breaches are notifiable. Unfortunately, two of the limbs of the interference with privacy test in section 75 (currently section 66 of the Act) do not have any seriousness threshold. That is probably acceptable for ex post facto

consideration of harm, but it is unworkable for an agency trying to decide whether to notify promptly after it becomes aware of a breach. Its ability to assess harm is less at that stage and therefore without an objectively judged seriousness threshold, it will effectively be forced to notify every breach. Therefore, increasing the threshold for notification, but not for interference with privacy generally, is appropriate. Note that section 75(2)(b)(iii) already has a higher threshold because it uses the word "significant". It makes sense therefore to use that word for the threshold for the other two sections (and thereby have recourse to existing New Zealand jurisprudence) even though Australia uses the threshold "serious" (Australian Privacy Act, s26WE(2)) and the GDPR uses the threshold "high" (Article 34.1). (2) It is appropriate to deem breaches involving biometric data or genetic data to automatically be harmful and reportable without any discretion because these are things that an affected individual cannot change (unlike, say a credit card or a password). The potential for harm in the future, even if current harm cannot be identified, is therefore greater.]

privacy breach, in relation to personal information held by an agency,—

(a) means—

(i) unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, the personal information; or

(ii) an action that prevents the agency from accessing the information on either a temporary or permanent basis; and

(b) includes any of the things listed in **paragraph (a)(i)** or an action under **paragraph (a)(ii)**, whether or not it—

(i) was caused by a person inside or outside the agency; or

(ii) is attributable in whole or in part to any action by the agency; or

(iii) is ongoing.

(2) For the purposes of this subpart, the meanings of **access**, **disclosure**, and **loss** are not limited by the use of those words or the meanings ascribed to them elsewhere in this Act.

Compare: 1956 No 65 s 22B

118 Agency to notify Commissioner of notifiable privacy breach

An agency must notify the Commissioner as soon as practicable after becoming aware that a notifiable privacy breach has occurred.

119 Agency to notify affected individual or give public notice of notifiable privacy breach

(1) An agency must notify an affected individual as soon as practicable after becoming aware that a notifiable privacy breach has occurred, unless **subsection (2)** or an exception in **section 120** applies.

(2) If it is not reasonably practicable to notify an affected individual or each member of a group of affected individuals, the agency must instead give public notice of the privacy breach.

(3) Public notice must be given—

(a) in a form in which no affected individual is identified; and

(b) in accordance with any regulations made under **section 213.**

(4) If **subsection (2)** or an exception in **section 120** is relied on, the agency must notify the affected individual or individuals at a later time if—

(a) circumstances change so that **subsection (2)** or the exception no longer applies; and

(b) at that later time, there is or remains a risk that the privacy breach will cause any of the types of harm listed in **section 75(2)(b)** to the affected individual or individuals.

(5) A failure to notify an affected individual under this section ~~may~~ shall be deemed to be an interference with privacy under this Act ~~(*see*section 75(2)(a)(iv))~~.

[Drafting Note: The word "may" introduces an unhelpful degree of uncertainty. Provided the definition of notifiable privacy breach has an appropriate threshold, then all such breaches should be deemed to be interferences with privacy as that term is used in the Bill/Act. This has an important flow on effect in terms of the proposed changes where an agency must report to the Privacy Commissioner but need not report to affected individuals if the agency considers that the breach has been rectified. If, once he or she receives the notification, the Privacy Commissioner disagrees with the agency and considers that not reporting would cause harm (and is therefore an interference with privacy), the Commissioner under these proposals would then be able to issue a compliance notice requiring disclosure under section 124.

Note however that section 124 should be amended to make it clear that this form of interference with privacy can be the subject of a compliance order]

120 Exceptions to obligations to notify affected individual or give public notice of notifiable privacy breach

(1) An agency is not required to notify an affected individual or give public notice of a notifiable privacy breach if:

(a) the agency had, prior to the privacy breach occurring, implemented appropriate measures that a reasonable person would conclude render the personal information that is the subject to the privacy breach unintelligible to any person who is not authorised to access it; or *[Drafting Note: cf Australian Privacy Act s26WF, GDPR Article 34.3(a)]*

(b) the agency has, after the privacy breach has occurred, implemented appropriate measures that a reasonable person would conclude result in it being unlikely that harm of any of the types referred to in paragraphs (a) and (b) of the definition of **notifiable**

privacy breach, will occur; or *[Drafting Note: cf Australian Privacy Act s26WF, GDPR, Article 34.3(b)]*

(c) ~~if~~ the notification or notice would be likely to—

~~(a)~~

(i) prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand; or

~~(b)~~

(ii) prejudice the maintenance of the law by any public sector agency, including the prevention, investigation, and detection of offences, and the right to a fair trial; or

(d) endanger the safety of any person; or

~~(d)~~

(e) reveal a trade secret.

[Drafting Note: The objective here is to avoid unnecessary disclosure to affected individuals of breaches that have been rectified to the extent that it is not likely that significant harm will be caused. This is consistent with the GDPR (Article 34.3) and the Australian Privacy Act (section 26WF). This exception is subject to the safeguard that notice must always be given to the Privacy Commissioner. If the Commissioner considers that significant harm will still occur, he or she may issue a compliance notice under section 124 ordering notification to affected individuals (assuming that discussion with the agency does not result notification being initiated voluntarily).]

(2) An agency is not required to notify an affected individual or give public notice of a notifiable privacy breach—

(a) if the individual is under the age of 16 and the agency is satisfied that the notification or notice would be contrary to that individual's interests; or

(b) if, after consultation is undertaken by the agency with the individual's health practitioner (where practicable), the agency is satisfied that the notification or notice would be likely to prejudice the physical or mental health of the individual.

(3) If an agency decides not to notify an affected individual for either of those reasons, the agency must—

(a) consider whether it would be appropriate to notify a representative instead of the individual (if a representative is known or can be readily identified); and

(b) before deciding whether to notify a representative, take into account the circumstances of both the individual and the privacy breach; and

(c) if the agency decides it is appropriate to notify a representative and has identified a representative, notify that person.

(4) The agency must advise the Commissioner as soon as practicable if—

(a) the agency relies on **subsection (1)** and does not notify an affected individual or give public notice of the breach; or

(b) the agency—

(i) relies on **subsection (2)** and does not notify an affected individual or give public notice of the breach; and

(ii) cannot or decides not to notify a representative of that individual.

(5) In this section, **representative**,—

(a) for an affected individual under the age of 16, means his or her parent or guardian:

(b) for an affected individual aged 16 or over, means an individual appearing to be lawfully acting on that individual's behalf or in that individual's interests.

Compare: 1982 No 156 s 6

121 Requirements for notification

(1) A notification to the Commissioner under **section 118** must—

(a) describe the notifiable privacy breach, including—

(i) the number of affected individuals (if known); and

(ii) the identity of any person or body that the agency suspects may be in possession of personal information as a result of the privacy breach (if known); and

(b) explain the steps that the agency has taken or intends to take in response to the privacy breach, including whether any affected individual has been or will be contacted; and

(c) if the agency is relying on **section 119(2)** to give public notice of the breach, set out the reasons for relying on that section; and

(d) if the agency is relying on an exception to notification of affected individuals in section 120, state the exception relied on and set out the reasons for relying on it; and

(e) state the names of any other agencies that the agency has contacted about the privacy breach and the reasons for having done so; and

(f) give details of a contact person within the agency for inquiries.

(2) A notification to an affected individual under **section 119** or a representative under **section 120(3)** must—

(a) describe the notifiable privacy breach and state whether the agency has or has not identified any person or body that the agency suspects may be in possession of the affected individual's personal information (but must not include any particulars that could identify that person or body); and

(b) explain the steps taken or intended to be taken by the agency in response to the privacy breach; and

(c) where practicable, set out the steps the affected individual may wish to take to mitigate or avoid potential loss or harm (if any); and

(d) confirm that the Commissioner has been notified under **section 118**; and

(e) state that the individual has the right to make a complaint to the Commissioner; and

(f) give details of a contact person within the agency for inquiries.

(3) A notification to an affected individual must not include any particulars about any other affected individuals.

(4) In order to comply with the requirement under **sections 118 and 119** that notification must be made as soon as practicable, an agency may provide the information required by this section incrementally. However, any information that is available at any point in time must be provided as soon as practicable after that point in time.

122 Offence to fail to notify Commissioner

(1) An agency that, without reasonable excuse, fails to notify the Commissioner of a notifiable privacy breach under **section 118** commits an offence and is liable on conviction to a fine not exceeding $10,000

(2) It is not a defence to a charge under this section that the agency—

(a) did not consider the privacy breach to be a notifiable privacy breach, if, in the circumstances, it was reasonable for the agency to have done so; or

(b) has taken steps to address the privacy breach.

123 Publication of identity of agencies in certain circumstances

(1) The Commissioner may publish the identity of 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 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.

Since section 75(2) is a critical component of the breach notification regime, it is included below for ease of reference.

75 Interference with privacy of individual

(1) In this Act, an action of an agency is **an interference with the privacy of an individual** in any of the circumstances set out in **subsection (2) or (3)**.

(2) An action of an agency is an interference with the privacy of an individual if the action breaches,—

(a) in relation to the individual,—

(i) 1 or more of the IPPs; or

(ii) the provisions of an approved information sharing agreement; or

(iii) the provisions of an information matching agreement or **section 179 or 181**; or

(iv) **section 119**; and

(b) the action—

(i) has caused, or may cause, loss, detriment, damage, or injury to the individual; or

(ii) has adversely affected, or may adversely affect, the rights, benefits, privileges, obligations, or interests of the individual; or

(iii) has resulted in, or may result in, significant humiliation, significant loss of dignity, or significant injury to the feelings of the individual.

….

Compare: 1993 No 28 s 66