Privacy Commissioner
Te Mana Matapono Matatapu

REPORT TO THE MINISTER OF JUSTICE UNDER SECTION 26 OF THE PRIVACY ACT

SIX RECOMMENDATIONS FOR PRIVACY ACT REFORM

Introduction

1 Section 26 of the Privacy Act requires the Privacy Commissioner to carry out periodic review of the operation of the Act, to consider whether any amendments are necessary or desirable and to report those findings to the Minister of Justice. This current review examines developments in the five years since the last review of the Act, that make it necessary or desirable to amend the Act to ensure it is fit for purpose in the current and future environment.

2 In conducting the review I have considered the requirements of section 14(c) of the Act (to consider any developing general international guidelines relevant to the better protection of individual privacy) as well as my specific functions under section 13 of the Act including s 13(1)(e) (public registers), s 13(1)(n) (monitoring developments in data processing and computer technology) and s 13(1)(o) (reporting on proposed legislation or policy that may affect the privacy of individuals).

3 Privacy law reform has been under consideration since 1998 with the release of the Privacy Commissioner's comprehensive *Necessary and Desirable* report (and four update reports 2000-2008), followed by the thorough and wide-ranging Law Commission review (2008 - 2011) and the government's detailed response.[1] These reviews and the government response form the basis for the proposed modernisation of the Privacy Act.

4 The following table outlines the timeframe of reform since the Act was passed in 1993:

1993-1998	**Privacy Commissioner's report "Necessary and Desirable" under s26**	Period of the first Commissioner's review Necessary & Desirable (1998)
2000-2008	**Privacy Commissioner's Supplements to Necessary and Desirable**	1st supplement (2000) 2nd supplement (Jan 2003) 3rd supplement (Dec 2003) 4th supplement (May 2008)
2008-2011	**Law Commission privacy law review**	NZ Law Commission review of the Privacy Act NZLC 123 (2011) including public registers NZLC 101 (2008)
2011, 2012 2014	**Government responses to reform recommendations**	Cabinet approval for new information sharing amendments (2011); Government response to other Privacy Act recommendations (March 2012); and supplementary government response in detail (May 2014)
2013	**Part 9A added to Privacy Act – information sharing**	Implements the Law Commission's 2011 ministerial briefing on information sharing
2013	**All of government approach to privacy**	Role of Government Chief Privacy Officer established within DIA
2011-2016	**Privacy Commissioner review "Six recommendations for Privacy Act reform" under s 26**	Period of this s 26 review

[1] Supplementary Government Response to Law Commission report on Review of the Privacy Act 1993 (May 2014).

5 While the Act has been the subject of thorough and cumulative review, in light of further rapid changes in information technology and data science, and significant developments in international legal frameworks,[2] it has become necessary to address further matters of reform to ensure that the new privacy framework will be fit for purpose in the current environment as well as being adequately future focussed to anticipate foreseeable developments.

6 A lot has changed since the Law Commission's review. Important developments since 2011 that impact on the operation and adequacy of the privacy legislation include developments in data science and information technology, and new business models built on data driven enterprise. These developments have highlighted the importance for both the public and private sectors to optimise trust in the digital economy. While the Act's principles-based privacy regulation is inherently flexible, this new environment is revealing or confirming gaps and pressure points that add to those identified or considered in previous reviews. There are also apparent gaps and weaknesses in the Act's enforcement framework that need to be addressed if the reforms proposed are to introduce an effective and modernised form of privacy regulation.

7 The international context has also seen significant developments, in particular the adoption of revised privacy laws in Europe that will come into force in 2018, and these should now be taken into account in preparing revisions to New Zealand's privacy law.

Summary of recommendations for Privacy Act reform

8 I recommend the following matters should be included in the proposed modernisation of the Privacy Act:

8.1 **A right to data portability**: introducing a right to personal information portability (also known as a right to data portability), a new consumer right that is a feature of the EU General Data Protection Regulation (that will come into force in 2018) to suport and strengthen the fundamental right of access to information and to enhance consumer choice;

8.2 **Controls on re-identification**: including protections against the risk that individuals can be unexpectedly identified from data that has been purportedly de-identified;

8.3 **A new power to require demonstrations of agency compliance:** empowering the Commissioner to require agencies to demonstrate their compliance with the Act by reporting on the agency's privacy management programme or plan. This is a necessary measure to realise the policy intent of the reforms to enable the Commissioner to proactively identify and respond to systemic issues,[3] and complement other elements of the reforms to ensure workability of the proposed new enforcement framework including the compliance notice power and mandatory breach notification obligation, and reflect the importance of agency accountability for compliance, as recommended by the OECD guidelines;[4]

8.4 **New civil penalty**: providing for the Commissioner to seek the imposition of a suitably significant civil penalty in the case of a very serious or repeated breach of the Privacy Act. This will address a gap in the Act's enforcement framework (noting the enactment of civil penalty powers in the Australian Privacy Amendment Act 2012 (Cth), and the adoption in Europe of significant fining powers for non-compliance of up to €20 million or four per cent of a company's global revenue);

[2] In particular, the European General Data Protection Regulation (GDPR) adopted in April 2016, to come into force in May 2018 to replace the current data protection directive 95/46/EC.
[3] Supplementary Government Response to Law Commission report on Review of the Privacy Act 1993 (May 2014).
[4] OECD Privacy Framework Guidelines (revised 2013).

8.5 **Adjustments to criminal offences**: amending the scope of the defences available in respect of the criminal offences for obstructing the Commissioner in the exercise of any power under the Act (section 127 (a)) or failing to comply with a lawful requirement of the Commissioner under the Act and (section 127(b)). This will improve the efficiency and effectiveness of the Commissioner's investigation processes – three reform options are identified below and my preferred option is to make these offences strict liability;

8.6 **Proceeding with public register reform**: as recommended by the Law Commission, repealing the public register privacy principles and related provisions in Part 7 of the Act due to their lack of utility, enhancing provision for the suppression of personal information and confirming the Commissioner's privacy complaints jurisdiction in relation to breaches of public register access provisions.[5]

Recommendations for amendments to the Privacy Act 1993

Recommendation 1: A right of personal information portability

9 **I recommend that the Act include a right of personal information portability.**

10 A right of portability will allow individuals to request an agency to provide them their personal information in a suitable electronic format. This will reduce the current friction in transferring services to another provider. In my Office's latest survey of public attitudes, in response to a question about how important people considered portability of their personal information, we found a majority of the public consider the ability to transfer personal information between social network or cloud services as important.[6]

11 Facebook users, for example, can download a zip-file archive containing their Facebook history that includes a wide range of personal information, including information on any purchases made via Facebook including payment data, Internet protocol addresses, details of deleted friends, a facial recognition identifier and much more.[7]

12 This portability right should at a minimum entitle the individual concerned to rights comparable to those contained in article 18 of the new General Data Protection Regulation (the "GDPR"). This is prompted by the significant international development of the adoption by the EU of the GDPR. This is a new form of consumer entitlement that has arisen since the Law Commission's review of the Act and therefore was not considered as a potential additional right or principle as part of that review.[8]

13 I consider the benefits of including this new entitlement in the Act include:

13.1 helping to ensure existing access and use principles remain meaningful in a pervasive digital environment;

13.2 strengthening consumer choice in relation to information service providers in the digital environment and helping to prevent provider lock-in;

[5] Law Commission *Public Registers: Review of the Privacy Act Stage 2* (NZLC R 101, 2008).
[6] Our 2016 survey asked "*When you decide to change online service providers (e.g. an online social network or cloud service provider), how important is it for you to be able to transfer personal information that was stored and collected by the old provider to the new one?" https://privacy.org.nz/news-and-publications/statements-media-releases/public-attitudes-to-data-sharing-cautious-but-shifting-survey/*
[7] EU Privacy Reg Data Portability May Affect Controllers
Bloomberg Law: Privacy & Data Security (30 March 2016) https://www.bna.com/eu-privacy-reg-n57982069251/
[8] See Law Commission *Review of the Privacy Act 1993* (NZLC R 123, 2011) ch 3 for the new matters considered in the review.

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

13.4 preserving NZ's status, and comparative trading advantage, as a country recognised as providing an adequate level of data protection, in the face of any post-GDPR review of that status.

Discussion

14 It is proposed that an amendment to the Act confer upon individuals a 'portability' right to personal information held about them by agencies. This will allow individuals to request that an agency transfer their personal information, in an electronic format that remains usable with another agency. This is comparable to number portability (regulated by a determination under the Telecommunications Act 2001) that enables a customer to switch telecommunications providers while retaining the same telephone number, bringing efficiency and other benefits in the telecommunications sector, and reducing barriers to competition.

15 For example, the portability right can enable individuals to take their transaction histories with them when they switch to a new bank, telecommunications company or internet service provider. The right would also be relevant in relation to online cloud services that provide storage and access to personal information, digital photo albums and videos and allow individuals to request a download of their personal information that they can carry with them to a new provider or service.

16 The proposed right of personal information portability will broadly correspond to the new 'Right to Data Portability' contained in article 18 of the EU General Data Protection Regulation. The GDPR was adopted in April this year, after four years legislative consideration, and will come into effect in May 2018. 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.[9]

17 The identified problem that the new right seeks to address was described by the European Commission as the difficulty an individual can experience in attempting to transfer personal data from an application or service to a different provider, essentially locking consumers in to a particular application or service and acting as a barrier to competition:[10]

> There is also no explicit right for the individual to extract his/her own personal data (e.g. his/her photos or a list of friends) from an application or service in a format that may be processed further, so that the individual may transfer data to another application or service. With increasing use of certain online service, the amount of personal data collected in this service becomes an obstacle for changing services, even if better, cheaper or more privacy friendly services become available. This could mean the loss of contact information, calendar history, interpersonal communications exchanges and other kinds of personally or socially relevant data which is very difficult to recreate or restore. Even where possible, re-entering the data manually into another service can be a major effort. This situation effectively creates a lock-in with the specific service for the user and makes it effectively very costly or even impossible to change provider and

[9] Available cost/benefit assessment of the EU reforms (including the portability right) includes London Economics "Implications of the European Commission's proposal for a general data protection regulation for business" (Final report to the Information Commissioner's Office, May 2013) https://ico.org.uk/media/1042341/implications-european-commissions-proposal-general-data-protection-regulation-for-business.pdf; European Commission Staff Working Paper, Impact Assessment, 2012 http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf

[10] European Commission Staff Working Paper, Impact Assessment, 2012.

benefit from better services available on the market. Portability is a key factor for effective competition, as evidenced in other market sectors, e.g. number portability in the telecom sector.

18 Lock-in is a privacy problem in that it signifies a loss of an individual's autonomy and control and can render the meaningful exercise of the fundamental right to access one's own personal information illusory.

19 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. Principles seeking to empower individuals to control the use of their information, and allow consumer choice, are rendered ineffective if individuals are locked into relationships with information services providers because they cannot effectively extract personal information and seamlessly move to another provider.

20 The new right 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. Privacy law seeks to empower individuals to maintain control over their personal information. When individuals sign up with a service provider, they may have a choice. They might research how that provider will use their information and the services provided. As time goes by an individual may wish to choose another provider. A new provider may offer a better service or price or the individual may have lost trust in the first provider. Individuals should be able to switch services, especially in a world where service providers may change business models or discontinue products.

21 Currently however, barriers to extracting and transferring information may mean that individuals are effectively locked in. The individual may not want to lose the effective use of the personal information already amassed. They may not want or be able to 'start from scratch'. Consumer lock-in is seen as a competition problem. However, it is also 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.

22 The adoption of the GDPR is a development in privacy law of global significance. It is widely perceived as the most stringent and the most influential privacy law in the world: the 'gold standard'. It harmonises the information privacy law of a trading bloc of 510 million of the world's most affluent people. The law purports to apply not only to European businesses but also to businesses processing the information of EU residents: such as NZ businesses directing their products or services to European consumers.

23 New Zealand's privacy law has been formally recognised by the European Commission as providing an adequate level of data protection to meet the requirements of existing EU law.[11] NZ is one of only 5 countries outside Europe to have received such formal recognition,[12] and other countries in the Asia-Pacific region including Japan and Singapore are seeking to emulate the European model with South Korea recently expressing a desire to achieve EU adequacy status. The recognition of the adequacy of New Zealand's privacy law provides a legal basis for EU businesses freely to send data to NZ for processing (and earning the EC's recognition its informal characterisation as 'NZ's first free trade agreement with the EU'). The formal recognition will be carried over to the new GDPR regime. However, it will be subject to ongoing review and with the more stringent EU standards

[11] New Zealand's adequacy status is noted as a major advantage to New Zealand business in the government response to the Law Commission's review of the Privacy Act: Office of the Minister of Justice *Reforming the Privacy Act* (Cabinet Social Policy Committee, May 2014) at [38].

[12] http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm. In addition, the EU Commission has also adopted a decision recognising the adequacy of the protection provided by the EU-U.S. Privacy Shield (12 July 2016).

applying from 2018 – including the data portability right – there will be some risk of NZ's status being questioned in the future if our law is seen as falling below prevailing EU expectations.

24 The drafting and scope of a NZ right may appropriately differ from the EU right. However, the objective would be to produce a right that is interoperable with the GDPR (and any other emerging international approaches). In other words, a NZ 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 NZ provider just as NZ consumers might benefit from the new GDPR right in dealing with an EU-based business.

25 Europe is not the only economy promoting data portability. The White House has also been active in seeking to increase data portability since 2010 and has just begun a new project to further explore the benefits.[13]

26 In New Zealand, portability has also been suggested as a Privacy Act reform by academic Gehan Gunasekara.[14]

Recommendation 2: Controls on re-identification

27 **I recommend that the Privacy Act include protections against the risk that individuals can be unexpectedly identified from data that has been purportedly de-identified (anonymised).**

28 Additional provisions are needed to ensure that the opportunities and benefits of greater data use can be optimised, without undue risk to individual privacy, and public trust and confidence. As noted in Vodafone's recent survey on big data:[15]

> Finding a way to take advantage of the social and economic benefits that big data offers while protecting the rights of freedoms of individuals is one of the most important challenges we face today. The collection and analysis of data could change our lives for the better but this will only happen if we understand individuals' privacy concerns and put them at the heart of big data initiatives.

29 The issue of identifiability and advances in re-identification was noted in the Law Commission's 2010 Issues Paper and 2011 Final Report as an emerging issue.[16] Since the Commission's review, there have been a number of high profile instances overseas where the re-identification risk has been raised or has actually eventuated, leading to privacy harms and to the de-railing of public sector initiatives. Some re-identification examples are set out in the Appendix.

30 Re-identification is an important issue in light of the government's stated objectives of improving efficiency and outcomes through greater use and re-use of data. The New Zealand Data Futures Partnership (the "DFP") has been tasked with making recommendations to government to limit the increasing risks of the re-identification of individuals from de-identified (anonymised) information, and that the DFP is due to report back with its findings in 2017.

---

[13] https://www.whitehouse.gov/blog/2016/09/30/exploring-data-portability

[14] Gehan Gunasekara: Big Data is becoming capable of manipulating our lives New Zealand Herald (13 December 2016) http://www.nzherald.co.nz/technology/news/article.cfm?c_id=5&objectid=11765242

[15] Matthew Kirk, Chairman of the Advisory Board, Vodafone Institute of Society and Communications, Vodafone Big Data Survey 2016 http://www.vodafone-institut.de/wp-content/uploads/2016/01/VodafoneInstitute-Survey-BigData-Highlights-en.pdf

[16] Law Commission *Review of the Privacy Act 1993* (NZLC IP 17, 2010) at [3.24]; *Review of the Privacy Act* 1993 (NZLC R 123, 2011) at [2.46].

Discussion

The context for reform

31 The need for controls in the Act on re-identification is becoming urgent as enhanced access to and use of de-identified (anonymised) personal information is increasingly sought for a variety of public good purposes, to improve service provision and to gain public sector efficiencies. Where personal information has been disclosed in de-identified form it can be freely used and disclosed. However advances in technical understanding and computing power now make it impossible to guarantee that de-identified information will not be re-identified.

32 Public trust and confidence is a critical consideration in this context. It is vital, for the public sector and in the wider public's interest to ensure that, when personal information is anonymised, anonymity is preserved and maintained. I am concerned any significant loss of public trust could jeopardise the ability to sustain social license in the widespread use of personal information along with the various public benefits from that use.

33 There is a compelling public interest in deriving greater value from public datasets. However, successfully leveraging the benefits of data analytics to inform public policy, create economic benefits and to serve citizens, fundamentally depends on maintaining public trust and confidence.

34 Data sharing is more readily accepted where personal information is anonymised and aggregated. Individuals' confidence in the use of de-identified information is in part determined by their belief that they will not be able to be re-identified or singled out from the crowd. But the lack of an explicit prohibition on the re-identification of individuals from aggregated personal information opens up a gap in the Act and risks undermining public confidence in the robustness of de-identified datasets.

35 The Act requires reform to ensure that agencies holding personal information take adequate steps to de-identify it before using or releasing it in "anonymised" form and ensure that there are adequate re-identification controls on third party recipients of de-identified personal information. I note that the Australian government has recently announced legislative reforms, prohibiting the re-identification of de-identified personal data through the use of both criminal and civil penalties.[17]

36 In the New Zealand context, the Act provides for the use and re-use of de-identified (anonymised) personal information in privacy principles 10(f) and 11(h) including for the statistical and research purposes. But the risk of re-identification of de-identified (anonymised) information may render a number of important privacy protections ineffective, damage trust, and hinder safe and accountable information sharing in the public and private sectors.

37 Greater sharing of anonymised datasets derived from personal information and the growing sophistication of data analytics poses challenges to the Act's current framework. Sensitive information about individuals can now be derived from combining and manipulating datasets from a variety of sources, including datasets that were de-identified prior to their release.

38 A number of examples that demonstrate the risks involved in releasing de-identified datasets are noted in the Appendix. These include the recent example where the Australian Department of Health announced it had removed a dataset from data.gov.au following an alert made in the public interest from the Department of Computing and Information at

[17] Privacy Amendment (Re-identification Offence) Bill 2016, currently before the Australian Senate. http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1047.

Melbourne University that it was possible to decrypt some service provider ID numbers. The dataset did not include names or addresses of service providers and no patient information was identified but given the potential to extract some doctor and other service provider ID numbers, the Department of Health immediately removed the dataset from the website to ensure the security and integrity of the dataset.

39 This example and others in the Appendix, as well as the vigorous academic debate on the issue,[18] demonstrate that de-identification no longer represents a 'silver bullet' for privacy protection. While de-identification measures applied by agencies that have collected or compiled datasets prior to release remain highly significant for the protection of the privacy of the individuals, additional safeguards against re-identification are essential to maintain proper protection and accordingly public trust in innovative data use.

40 There are therefore two matters to be addressed to ensure the Act remains fit for purpose in the current dynamic data use environment being:

40.1 adequate controls on re-identification by recipients of de-identified data to protect the privacy of the individuals in de-identified datasets; and

40.2 clear expectations that an agency holding personal information must take adequate steps to de-identify it before using or releasing it in de-identified form.

Controls on re-identification

41 I recommend that the Privacy Act should include a new privacy principle that limits the re-identification of previously de-identified or anonymised personal information, except in limited circumstances. A new privacy principle would reassure people that they have a means of redress if they suffer harm as a result of being re-identified from supposedly anonymous data. This would act as a necessary incentive to data holders and users to maintain the integrity of the de-identified data set.

42 I consider the addition of a new privacy principle is the most effective and flexible option to address the risk of privacy harm, in a manner that is consistent with the overall scheme of the Act, having considered other options. These include:

42.1 amending principles 10 and 11 to specify how re-identified information may be used;

42.2 issuing a code of practice under Part 6 of the Act; and/or

42.3 creating a new criminal offence to penalise re-identification in certain circumstances, as is proposed in Australia.

Clarifying de-identification obligations

43 As well as new controls on re-identification, effective de-identification (anonymisation) remains vitally important. De-identification is a crucial first step that significantly reduces the

[18] Anonymization and Risk – Rubinstein and Hartzog, August 17, 2015 Rubinstein and Herzog (September 2015) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2646185
Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006 Dispelling the Myths Surrounding De-identification, Ann Cavoukian and Khaled El Emam https://fpf.org/wp-content/uploads/2011/07/Dispelling%20the%20Myths%20Surrounding%20De-identification%20Anonymization%20Remains%20a%20Strong%20Tool%20for%20Protecting%20Privacy.pdf https://fpf.org/wp-content/uploads/2010/07/The_Deidentification_Dilemma.pdf
Cavoukian and Castro "Setting the Record Straight: De-identification Does Work" (June 2014); Arvind Naryanan and Edward W. Felten of Princeton presented a rebuttal, (July 2014); https://iapp.org/news/a/on-why-we-need-to-map-the-de-identification-middle-ground/ NIST (the National Institute of Standards and Technology in the US Department of Commerce) released a paper by Simson Garfinkel in October 2015 "De-identification of Personal Information".

risk that personal information will be used or disclosed for unauthorized or malicious purposes.

44 I therefore recommend the Act include a provision clarifying the obligations on agencies that de-identify datasets containing personal information. For example, clarifying the need to take reasonable precautions in the circumstances to limit the identification of individuals included in a dataset (similar to the principle 5 standard to take adequate security measures) would help ensure that the de-identification is sufficiently robust to protect privacy interests. This could be accompanied by Privacy Commissioner guidance.

Recommendation 3: An additional power to require demonstrations of compliance

45 **I recommend that the Privacy Act include an additional power to require an agency to demonstrate its ongoing compliance with the Act.**

46 This power would allow the Commissioner to require an agency to demonstrate its ongoing compliance by:

46.1 establishing a privacy management programme or plan that is adequate for their purposes;

46.2 requiring a report to the Commissioner on steps taken to achieve compliance with that requirement; and/or

46.3 publicly reporting on its position with regard to its privacy management programme.

47 The three key reasons for my recommendation are to:

47.1 realise the policy intent of the reforms to enable the Commissioner to proactively identify and respond to systemic issues,[19]

47.2 ensure the workability of the proposed new enforcement mechanisms, in particular, the compliance notice power and mandatory breach notification obligation, and

47.3 reflect the importance of agency accountability for compliance, as recommended by the OECD guidelines.[20]

48 My proposal is an additional express function or power that would mean the Commissioner can inquire into the adequacy of an agency's privacy management processes, so that any significant gaps and weaknesses can be proactively addressed and the risk of future breaches mitigated.[21] The aim of the recommendation is to improve and incentivise compliance with the Act and to reduce the risk of systemic breaches. It could be used in a range of situations.

49 As it would not be limited to situations of non-compliance, it could be used proactively as a monitoring tool to provide my Office with additional information about privacy practices to complement other information sources, in order to focus on emerging problems or issues and to respond appropriately, such as through guidance, education, media engagement and own motion investigations.[22] For example, it would allow the Commissioner to focus on or

[19] Supplementary Government Response to Law Commission report on Review of the Privacy Act 1993 (May 2014).
[20] OECD Privacy Framework Guidelines (revised 2013).
[21] An alternative option would be to make privacy management plans mandatory, as is the case in New South Wales; however I do not consider that option to be necessary or desirable. The proposed option to require an appropriate demonstration of compliance is a more flexible approach.
[22] Currently the Commissioner's information sources include complaints, breach notifications, media reports, enquiries, consultations with other oversight bodies, and from international contacts.

highlight privacy compliance in a particular sector, in relation to a particular issue or technology, or on a particular aspect of compliance.

50 The power I am proposing would be discretionary and used in limited cases. In terms of resourcing implications for OPC, suitable criteria and a protocol would be developed in relation to its exercise. I predict that the power would usually be triggered in response to the suspicion of a risk to privacy by a specific agency's practices, or in response to a more general privacy risk, for example by agencies that deal with high volumes of personal information or highly sensitive data.

51 Overall, I expect the benefits of including the additional power to include:

51.1 promoting a positive compliance culture and reducing the risk of breaches and complaints;

51.2 facilitating responsive regulation by enabling the Commissioner to address serious risks to privacy to supplement 'after the event' redress triggered by a complaint;

51.3 promoting and normalising the development of privacy management plans and role-modelling best practice, enhancing uptake and privacy maturity; and

51.4 strengthening governance of agency decision making and management of activities of agency staff that design and operate systems, to promote compliant behaviour.

52 The proposed power would have cost implications for agencies in terms of time spent preparing plans, any necessary systems changes and demonstrating their compliance to the Commissioner. However we expect these costs would largely be offset by reduced compliance failures and the associated resources needed for complaints investigations and settlement.

Discussion

Fulfilling the intent of reforms to enable the Commissioner to proactively identify systemic issues

53 The new power I recommend is necessary to fulfil the stated overall goal of the reforms to ensure New Zealand has a privacy regime more focussed on early intervention and prevention of risks rather than after the fact remedies.[23] The intent of the reforms as noted in the government response to the Law Commission review was that the 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, noting that New Zealand needs a privacy regime that will enable the early identification and investigation of, and response to, systemic privacy risks.

54 While the new compliance notice power will enable me to respond to identified issues of non-compliance, the current scope of my investigation powers (that depend on a breach of some kind) will limit the extent to which I can proactively identify and address systemic compliance issues in the absence of a specific breach or incident. The additional new power to require positive demonstrations of compliance is therefore necessary to ensure that I can effectively identify, investigate and respond to systemic issues.

55 There is a strong case for requiring agencies to demonstrate how they address privacy risks and any evident inadequacies in their policies, processes and/or operating systems, to reduce the likelihood of privacy breaches. It is in everyone's interests, including the agencies themselves, that agencies have robust systems for managing personal

[23] At [41].

information.[24] Where agencies are pre-emptive and actively plan and prioritise privacy management, they save resources and reduce the potential for complaints and harm to both individuals and the agency (such as reputational damage from poorly handled or high volumes of complaints).

56 However, the current New Zealand regulatory model embeds a reactive approach to breaches and complaints. This means that, rather than having a strategic, proactive approach to privacy management and protection, privacy compliance policies can be ad hoc, and vary in quality and application.

57 There are occasions when the issues raised in a complaint reflect matters of systemic compliance rather than a specific privacy breach.[25] My Office has experience of agencies that are consistently uncooperative regarding privacy investigations or are regularly complained about - but the absence of sufficiently serious privacy harm on an individualised basis means the privacy interference threshold may not be reached.[26]

58 The existence of an explicit power to require an agency to develop and/or report on its privacy management framework would help to raise the bar of privacy performance for some agencies that are lagging behind. My rationale is that the introduction of an additional power of this sort would encourage those agencies that on occasion take a blasé attitude to OPC's recommendations to adopt them more readily, and lead to agencies being more willing to reach settlements and to address systemic problems to improve their privacy practices generally.

Addressing the current gap in the reforms

59 The absence of a power to inquire into the adequacy of an agency's compliance may have an adverse impact on the effectiveness and efficiency of the Act's proposed new enforcement framework and limit the workability of the new enforcement powers in some circumstances. The new power I recommend is therefore a necessary component of the modernised Act. This is to ensure the workability of the new enforcement framework as currently proposed. An effective privacy regulator needs a range of regulatory tools to be able to respond appropriately to emerging privacy risks. This requires a variety of measures in the Act, including those that enable the Commissioner to effectively and efficiently pursue broad systematic improvements in information handling procedures.

60 The Law Commission's review concluded that the Privacy Commissioner should have further powers, noting that the office should not be perceived as a "toothless tiger".[27] The Law Commission recommended that the Commissioner should have both compliance notice powers and mandatory audit powers, and that agencies should have mandatory breach notification obligations.[28]

61 The government response accepted the majority of the Law Commission's recommendations, including new compliance notice powers and mandatory breach notification obligations. However, the recommendation for mandatory audit powers was rejected on the basis that the Commissioner's own motion investigation powers could be enhanced.[29] However, the proposed reforms to the Commissioner's investigation powers

[24] See Law Commission *Review of the Privacy Act 1993* (NZLC R 123, 2011) at [6.89].
[25] Anecdotally it would seem that some agencies would rather face the risk of Human Rights Review Tribunal proceedings as they arise than take proactive steps to improve overall privacy performance and reduce potential complaints.
[26] There are occasions when naming the agency or referring a case to the Human Rights Review Tribunal is not an appropriate escalation and a broader range of regulatory options would be helpful.
[27] Law Commission *Review of the Privacy Act 1993* (NZLC R 123, 2011) at [6.65].
[28] Law Commission *Review of the Privacy Act 1993* (NZLC R 123, 2011) R63, R64, R67-79.
[29] Office of the Minister of Justice *Reforming the Privacy Act* (Cabinet Social Policy Committee, May 2014) at [5.2], [34].

are limited and do not extend as far as proactive enquiries in the absence of a suspected breach.[30]

62 The new compliance notice power is not enough on its own to address compliance issues. That power will expand the range of regulatory responses available to the Commissioner following a breach of some kind, and will require an agency to take steps to rectify any non-compliance. However, that new power does not explicitly enable the Commissioner to proactively require an agency to demonstrate that it has appropriate processes and policies in place to support its general compliance with its obligations under the Act. An ability to require agencies to demonstrate their compliance would therefore fill some of the gap in the regulatory toolbox currently at the Commissioner's disposal.

63 An express recognition in the new Act that the Commissioner can require agency demonstrations of compliance would complement the other new powers, for example it would provide a practical example of the type of concrete steps the Commissioner may require an agency to take to fulfil a compliance notice, and the type of potential regulatory response to repeated and unexplained serious breach notifications.

64 Other data protection authorities (including in Canada, Australia, Spain and other European countries) have mandatory audit or prior approval powers. Privacy audits investigate the flows of personal information within an organization and determine whether the organisation implements appropriate privacy principles in its management of these data flows. These audits are one way of increasing privacy protections in the age of big data and social networking.[31]

65 The Law Commission recommended the Commissioner have mandatory audit powers as an element of the New Zealand privacy reforms;[32] however that recommendation was not accepted. That omission means that a gap remains in the scheme of the Act in terms of monitoring compliance and verifying internal privacy management practices. It is therefore necessary to address this to ensure that there is an appropriate "pre-cursor" power to the new compliance notice power, as well as providing a range of appropriate response powers to the new mandatory breach notification obligation. Requiring a positive demonstration of compliance by an agency would be a useful step 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.

66 For example, where I receive regular complaints about a practice that may raise a risk of future non-compliance but does not meet the threshold for investigation (for example because the breach has not resulted in a particular privacy "harm" under s 66 of the Act), to decide whether a compliance notice should be issued to address any systemic issues, a useful initial step might be to require an agency first to demonstrate its compliance so that I am informed as to the state of the agency's privacy management programme.

67 The power to require an agency's demonstration of compliance by producing evidence of its privacy management programme may also be a suitable response to a repeated or unexplained serious breach notification to identify the areas of systemic weakness or process steps required to be addressed in an eventual compliance notice.

[30] The specific enhancements proposed are (a) increasing the maximum penalty for non-compliance with a lawful requirement of the Commissioner from $2,000 to $10,000 and (b) amending the process for extensions of time to comply with any Commissioner's requirement to produce information in relation to an investigation.
[31] Alan Toy *Privacy Audits: Expectations and Implementation* University of Auckland, PhD thesis (May 2016).
[32] Currently the Commissioner has "voluntary" audit powers by virtue of s 13(1)(b) of the Act.

68 There are also examples under the current enforcement framework that illustrate the need for an additional power (that would not be addressed by the new compliance notice power). For example:

68.1 where I become aware of a new practice or technology that has implications for privacy, I have limited powers to proactively investigate how early adopters are addressing compliance issues and whether any risks to individual privacy are being adequately managed; or

68.2 where an agency has deficient or inefficient privacy complaints handling processes, I have limited ability to inquire into the agency's management of privacy requests and complaints, unless the agency fails to comply with a statutory demand (s91(4)) or obstructs my investigation process (s 127(a)) or otherwise refuses or fails to comply with my lawful requirement (s 127(b)).

69 There are other examples where the power to require an agency to demonstrate its compliance would be a useful adjunct power to my function (s 13(1)(m)) to inquire into any practice that appears may infringe an individual's privacy or to investigate any action that is or appears to be an interference with the privacy of an individual (s 67). For example:

69.1 where I receive regular notifications of repeated similar data breaches from an agency or a sector that indicate inadequate security safeguards;

69.2 where an agency is repeatedly investigated for interfering with the privacy of individuals but makes little effort to improve its systems or practices to address underlying compliance issues; and

69.3 where an investigation by an overseas Privacy or Data Protection Commissioner raises compliance issues or concerns that could usefully be addressed proactively in New Zealand.

A workable alternative to mandatory audit power

70 I consider that the identified gap in regulatory options can largely be addressed by including a power to require a demonstration of compliance, as an alternative to mandatory audit powers. This alternative is more flexible, less resource intensive (both for the agency concerned and for the Commissioner) and would impose a lower burden on agencies than a mandatory privacy audit power.

71 Requiring an agency to demonstrate its compliance by providing the Commissioner with its privacy management planning and policies is a different approach to a privacy audit:

71.1 Accountability remains with the agency to address compliance, rather than falling on the Commissioner to verify or critique compliance through exercising an audit function.

71.2 It requires the agency to provide evidence of its privacy management programme to the Commissioner, in sufficient detail to demonstrate its approach to compliance, but does not go so far as requiring a transactional compliance audit against privacy standards.

71.3 Agencies may find privacy audits provide real value, however they would not be compelled to adopt them or be subjected to a privacy audit under the new power being proposed. Rather, the obligation is to produce sufficient evidence of internal privacy management practice to ensure adequate processes and systems to address foreseeable compliance issues.

OECD Privacy Framework – a new emphasis on agency accountability

72 International best practice is influential in the options for design of the Act's modernised framework and the revised OECD Guidelines support the approach of requiring agencies to be able to demonstrate their compliance with their obligations.

73 I consider inclusion of the new power necessary to adequately reflect the 2013 revision of the Guidelines to the OECD Privacy Framework, a development that post-dates the Law Commission's review of the Privacy Act[33] and now includes an increased emphasis on agency accountability for compliance. To be accountable, an agency has to be able to demonstrate genuine compliance rather than merely reacting to breaches or complaints investigations as these arise. Without adding a new power to require appropriate demonstrations, this aspect of the OECD Guidelines will not be addressed.

74 In the 2013 updated Privacy Framework Guidelines and Supplementary Explanatory Memorandum, the OECD emphasised the importance of agency accountability in protecting individual privacy.[34] The Guidelines introduce the concept of privacy management programmes as the core operational mechanism through which agencies implement privacy protection. According to the Guidelines, an accountable agency should have a privacy management programme in place that is tailored to the structure, scale, volume and sensitivity of its operations and provides for appropriate safeguards based on privacy risk assessment:[35]

> PART THREE: IMPLEMENTING ACCOUNTABILITY
>
> 15. A data controller should:
>
> a) Have in place a privacy management programme that:
>
> i. gives effect to these Guidelines for all personal data under its control;
>
> ii. is tailored to the structure, scale, volume and sensitivity of its operations;
>
> iii. provides for appropriate safeguards based on privacy risk assessment;
>
> iv. is integrated into its governance structure and establishes internal oversight mechanisms;
>
> v. includes plans for responding to inquiries and incidents;
>
> vi. is updated in light of ongoing monitoring and periodic assessment;
>
> b) Be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines; and
>
> c) Provide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects.

75 To be accountable, an agency has to be able to demonstrate genuine compliance rather than merely reacting to breaches or complaints investigations as these arise, or having a pro forma policy in place that is not widely known or followed by staff.[36] Whether an agency would need to develop a full privacy management programme or a simpler high level

[33] The desirability of consistency with the revised OECD Privacy Guidelines is noted in the government response: Office of the Minister of Justice *Reforming the Privacy Act* (Cabinet Social Policy Committee, May 2014) at [38].
[34] Section 14(c) of the Act requires the Commissioner to consider any developing general international guidelines such as the OECD guidelines that are relevant to the better protection of individual privacy. The OECD principles, including the accountability principle, are contained in Schedule 5A to the Privacy Act.
[35] OECD guidelines Part 3.
[36] The OECD Supplementary explanatory memorandum at p 24 emphasises the accountability gains for an agency when a Commissioner requests that an agency demonstrate compliance under paragraph 15(b): "Establishing the capacity and effectiveness of a privacy management programme, even in the absence of a personal data security breach or allegation of noncompliance, enhances the accountability of [agencies]."

privacy plan will depend on the privacy risks and implications of the agency's activities and operations, consistent with a risk-based approach. The requirement would be scalable according to the particular circumstances of the agency.

Utility of privacy management planning

76 Privacy management programmes are a tool for agencies to demonstrate that they have taken reasonable steps to uphold the privacy principles, and as evidence of a culture of privacy awareness and proficiency within the agency. Adoption would also assist agencies with the management of their compliance obligations in terms of specific provisions of the legislation:

76.1 a privacy management programme would provide practical evidence of:

76.1.1 reasonable security safeguards and necessary steps to prevent unauthorised use or disclosure of personal information (information privacy principle 5); and

76.1.2 reasonably practicable steps to prevent an employee doing an act contrary to the privacy principles as serving to limit liability for the acts of an employee (s126(4));

76.2 an agency's demonstration of compliance could be part of 'a satisfactory assurance against the repetition of any action that is the subject matter of the complaint or the doing of further actions of a similar kind by the person concerned' under s74.

77 This approach could also provide a useful model for orders made by the Human Rights Review Tribunal as an outcome of Privacy Act proceedings. For example, the Tribunal might make an order requiring an agency to develop or improve a privacy management programme or plan that the Privacy Commissioner could then review or monitor.[37]

Recommendation 4: Including a civil penalty provision

78 **I recommend that the Act empower the Commissioner to apply to the High Court for a civil penalty to be imposed (up to $100,000 in the case of an individual and up to $1 million in the case of a body corporate) in the case of serious breaches.**

79 This is consistent with Australian law and with other comparable New Zealand regulatory frameworks.[38]

80 In light of international trends and current conditions, privacy enforcement sanctions no longer appear adequate to deal with serious breaches. Additional civil enforcement sanctions for serious breaches of privacy are needed to ensure that the Act is fit for purpose and maintains equivalence with data protection laws in other comparable jurisdictions, as well as other New Zealand regulatory regimes.

81 While the proposed new compliance notice power will empower the Commissioner to respond to instances of non-compliance by requiring the agency concerned to take specified steps in order to meet its compliance obligations, the civil penalty provisions are also required to provide an appropriate regulatory response to the most egregious breaches of the Act, such as those committed intentionally or recklessly, and that affect a large number of people or compromise sensitive information, or could result in significant privacy impacts.

[37] This would expand on the current range of orders made by the Tribunal, for example, compulsory training orders.
[38] For example, s 45 Unsolicited Electronic Messages Act 2007.

82 Examples of monetary penalties imposed by the United Kingdom Information Commissioner (who is empowered to impose fines of up to £500,000) include:

82.1 The British Pregnancy Advice Service (BPAS) being fined £200,000 after a serious breach of the Data Protection Act revealed thousands of people's details to a malicious hacker. The personal data was not stored securely and a vulnerability in the website's code allowed the hacker to access the system and locate the information.[39]

82.2 The Kent Police force being fined after sensitive personal details of a woman who accused her partner of domestic abuse were wrongly disclosed to the suspect.[40] The breach was considered sufficiently serious in the circumstances to warrant a penalty of £80,000 in light of the amount of information disclosed (contents of a mobile phone), the sensitivity of the information and the potential consequences.

82.3 An online holiday insurance company being fined £175,000 after IT security failings let hackers access more than 5,000 customer records, including credit card and medical details.[41]

82.4 A £400,000 fine being issued against a telecommunications company for security failings that allowed a cyber attack to enter its systems and collect substantial personal data.[42]

83 Civil sanctions were not considered in detail in the Law Commission's 2011 review of the Act, although the Commission noted the comparatively large number of tools available to the UK Information Commissioner including a monetary penalty notice that can be imposed directly by the UK Commissioner (as illustrated above), as well as other enforcement measures including criminal prosecution, enforcement notice, application for an enforcement order, and compulsory audit, along with associated enforcement tools including an information notice, an assessment notice and a search warrant.[43] The Law Commission's preferred approach was not to go so far in New Zealand in terms of enforcement powers, opting for enhancements by way of compliance notice and mandatory audit powers. The Commission did not expressly consider judicially imposed penalties as an alternative to fining powers.

84 The government response to the Law Commission's review noted that other jurisdictions rely on the imposition of heavy fines to ensure compliance, including Australia's maximum penalty of A$1.7 million for repeat and serious privacy breaches. The response preferred a more moderate package of reforms and that New Zealand should not currently consider imposing fines for privacy breaches until the impact of the reforms has been determined. Although it noted the Australian penalty provision, the response discounted the option of "fines" without expressly addressing the option of judicially imposed penalties. However, in relation to the proposed criminal offence to support the new mandatory breach notification obligation, the government response noted that this would be reconsidered in light of the Law Commission's forthcoming review of pecuniary penalties.

[39] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/03/british-pregnancy-advice-service-fined-200-000/
[40] https://ico.org.uk/media/action-weve-taken/mpns/1623962/kent-police-mpn-20160421.pdf
[41] https://ico.org.uk/media/1043368/staysure-monetary-penalty-notice.pdf
[42] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/
[43] Law Commission *Review of the Privacy Act 1993* (NZLC R 123, 2011) at [6.66].

85 That review, the Law Commission 2014 report on the use and design of civil penalties in different regulatory contexts, concluded that pecuniary penalties are a legitimate regulatory tool when used appropriately.[44]

Discussion

86 Enforcement under the Privacy Act is primarily by way of Human Rights Review Tribunal proceedings brought either by the Director of Human Rights Proceedings or by aggrieved individuals. The outcome of proceedings may result in awards of compensation and other enforcement orders made by the Tribunal.[45] The law reform proposals include the Commissioner being empowered to issue compliance notices in relation to breaches of the Act, however that new power is focussed on improving compliance and does not include any provision for penalising past non-compliance, even in serious cases.

87 The Privacy Act contains targeted criminal offences that penalise a failure to comply with any lawful requirement of the Commissioner (s 127(b)). New criminal offences will also be added to address failures to comply with the new mandatory breach notification compliance notice, and access order obligations. However, there is currently no generic provision for penalising egregious conduct that does not fall under one of the specific offences.

88 Further, 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 is relatively low (either $2,000 or $10,000 in the Act, regardless of whether the defendant is an individual or a corporate entity). Offences are targeted at specific egregious acts such as making false statements, impersonation or destroying information, rather than providing a means of responding to significant privacy breaches more generally.

89 Otherwise, the compensatory nature of the Act's remedies is of limited effect in deterring egregious or blatant breaches by agencies. For example there is no power under the Act for the Tribunal to award exemplary damages. The only practical option available for the Commissioner to deter egregious breaches is to publicly report on these.[46]

90 The principles of responsive regulation suggest that compliance is most likely to be achieved where a regulatory regime is enforced by way of a hierarchy (or pyramid) of interventions that range from lower level "soft" options, up to harder orders and penalties that progressively increase in response to the seriousness of the issue.[47]

91 The Productivity Commission found evidence in its 2014 inquiry into regulatory practice that regulators can be constrained in effectively operating a responsive compliance strategy, where they do not have the range of enforcement tools to enable them to move up and down the pyramid, reporting the following comment from one submitter:[48]

> Good operation of regulators cannot overcome the inherent flaws in poor regulatory design. In these cases the outcomes intended by Parliament will never be achieved because the regulators have never been provided with the tools to effectively achieve these outcomes.

[44] Law Commission *Pecuniary Penalties: guidance for legislative design* (NZLC R133, 2014). In this later report, the Law Commission carried out a comprehensive review of the various considerations and the desirability of consistency when creating monetary penalties in legislation that are imposed by a court in regulatory contexts.
[45] Tribunal orders include declarations, restraining orders, performance orders (including training orders) and any other relief the Tribunal thinks fit (s 85(1) Privacy Act).
[46] The Law Commission considered whether the Tribunal should be able to award exemplary or punitive damages where a breach is intentional or in flagrant disregard of the plaintiff's rights, but recommended against any such power. Law Commission *Review of the Privacy Act 1993* (NZLC R123, 2011) R62.
[47] Law Commission *Pecuniary Penalties: guidance for legislative design* (NZLC R133, 2014) at [5.23]. The regulatory enforcement pyramid (Ayres & Braithwaite 1992) is discussed by the Productivity Commission in its report *Regulatory Institutions and Practice* (Final Report 2014) at 56.
[48] At 59.

92 Internationally, the trend is towards privacy and data protection regulators having a variety of sanctions in order to respond effectively and meaningfully to the range of breaches and non-compliance that arise. This includes the potential for large civil sanctions to be imposed for those rare, sufficiently serious cases that require them.

93 In Australia, 2014 amendments to the Privacy Act 1988 (Cth) empower their Commissioner to seek a significant civil penalty order (up to AU$1.7m for companies or AU$340,000 for individuals). The Australian Commissioner will consider seeking a civil penalty order where:

93.1 the interference with privacy is particularly serious or egregious in nature (e.g. a breach results in significant adverse consequences or substantial detriment or affects a large number of people);

93.2 the agency has a history of serious breaches; or

93.3 the agency failed to take its compliance obligations seriously or acted with blatant disregard for the law.

94 In Europe, privacy authorities can directly impose a range of sanctions including fines. UK examples have already been noted. The revised EU Regulation (that will come into force in 2018) includes provision for privacy authorities to impose administrative fines to sanction violations of data protection laws. A two-tiered sanctions regime will apply. Breaches of the significant provisions can lead to fines of up to €20 million or four per cent of global annual turnover. For other breaches authorities can impose fines of up to €10 million or up to two per cent of annual worldwide turnover for enterprises.

95 The New Zealand privacy enforcement framework now has a notable gap in the available options for regulatory response as non-compensatory civil sanctions are not currently provided for. Addressing this by including civil penalties (imposed by the High Court on the application of the Commissioner) is consistent with decisions already taken to strengthen the regulatory framework, noting the proposed inclusion of new compliance obligations such as mandatory breach notification and compliance notices.

96 In New Zealand, civil penalties are an increasingly common feature of commercial regulation and are available, for example, under the Unsolicited Electronic Messages (Spam) Act 2007, the Financial Markets Conduct Act 2013, the Financial Advisers Act 2008 and the Commerce Act 1986. [49]

97 Including a civil penalty provision in the Act (like the Australian model) appears to best align with New Zealand's approach and use of civil penalties as a regulatory mechanism. On that basis I prefer this over the alternative option of a power for the Commissioner to directly impose administrative fines (subject to appeal).

98 The overall benefits of modernising the enforcement framework by adding provision for civil penalties include:

98.1 incentivising compliance and deterring non-compliance through an appropriate spectrum of escalating enforcement responses;

98.2 enhancing flexibility and efficiency of enforcement action;

98.3 broader impact of high profile proceedings on compliance behaviour generally; and

[49] Civil or pecuniary penalties are imposed by the High Court under the authority of a statute for a breach of that legislation. The primary purpose of such a regime is to secure compliance with the statutory requirement and to penalise non-compliance.

98.4 keeping parity with the enforcement powers available to overseas privacy regulators for purposes of cross border co-operation and investigations.

Recommendation 5: Reform of criminal offences for obstructing the Commissioner

99 **I recommend the narrowing of the defences available in respect of the criminal offences for obstruction of the Privacy Commissioner or a failure to comply with a lawful requirement of the Commissioner (section 127(a) and (b)).**

100 Section 127 of the Privacy Act contains criminal offences attracting a maximum fine of $2,000 (proposed to be increased to $10,000) if a person (whether a company or an individual):

100.1 *without reasonable excuse*, obstructs, hinders, or resists the Commissioner in the exercise of powers under the Act (s 127(a)); or

100.2 *without reasonable excuse*, refuses or fails to comply with any lawful requirement of the Commissioner (s 127(b)).[50]

101 Current experience of agencies obstructing statutory investigation processes has shown that the "reasonable excuse" defence means that the offences are not operating satisfactorily. A person or agency who fails to comply with the Commissioner's lawful requirements can employ various excuses including a mistaken belief that they need not comply with the requirement.

102 The Law Commission considered and recommended new offences in its review of the Privacy Act, but did not consider the adequacy of elements of the current offences. The government response opted to increase the maximum penalties for these offences, but did not otherwise propose any amendments.

103 I have identified three reform options for narrowing defences:

103.1 replacing the "reasonable excuse" defence with the defence of "lawful justification or excuse" (option 1), or

103.2 recasting these offences as strict liability (option 2) – my preferred option, or

103.3 providing the option for the Privacy Commissioner to seek a pecuniary penalty order in relation to these offences as an alternative to prosecution (option 3).

Discussion

104 The criminal offences play an important role in incentivising agency co-operation with the Commissioner's statutory investigation and complaints process and deterring obstructive behaviour that may hamstring the Commissioner's ability to take appropriate action. For example, an efficient investigation into an interference with an individual's privacy depends on prompt compliance with notices given under s 91 requiring information to be produced (on a strictly confidential basis). Any obstruction or failure to comply by an agency can have a negative impact on the timeliness and efficiency of an investigation which is not in the public interest.

105 I have observed that some agencies either wrongly assume that they do not need to engage with my investigations process due to the perceived special circumstances of their

[50] See also s 114F of the Act, added in 2010, that provides a reasonable excuse defence to the offence of failing to comply with a transfer prohibition notice. No prosecutions have yet been brought under this provision.

business or profession, or they simply do not recognise that the Privacy Act applies to them or to their activities.

106 As already noted I have identified the following options for reform of s 127(a) and (b) including:

106.1 replacing the "reasonable excuse" defence with the defence of "lawful justification or excuse" (option 1);[51] or

106.2 recasting these offences as strict liability (option 2) – my preferred option;[52] or

106.3 providing the option for the Privacy Commissioner to seek a pecuniary penalty order in relation to these offences as an alternative to prosecution (option 3).[53]

107 I note that the comparable offences in the Ombudsmen Act 1975 (s 30) and the Human Rights Act 1993 (s 143) adopt the "lawful justification or excuse" defence[54] rather than the "reasonable excuse" defence. There are good policy reasons, given the statutory inter-relationships, for the Privacy Act to align with the Ombudsmen Act and Human Rights Act (option 1). One consideration however is whether this alignment would be sufficient given the scope of the Act's application across the public and private sector. Experience of the Ombudsmen Act offence is that this acts purely as a deterrent and its existence alone is sufficient to ensure compliance in the public sector.[55] Experience under the Privacy Act however is that on occasion these offences require prosecution to highlight and deter instances of obstruction and non-compliance.

108 In light of that experience, my preferred option is therefore option 2 – recasting these offences as strict liability. Examples of a "strict liability" approach include s 41 of the Statistics Act 1975, s 117 of the Mental Health (Compulsory Treatment) Act 1992 and s 102 of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009. This approach is also consistent with the Act's proposed new strict liability offence for failing to comply with an agency's new breach notification obligation that will require the Commissioner to be notified about material and serious breaches.

109 A third option is to create an alternative civil penalty provision that would enable the Commissioner to pursue a civil penalty on the civil standard of proof against an agency that obstructs the Commissioner's investigation, rather than prosecuting the defendant as a criminal matter. A model for this approach is the Employment Relations Act. This option has the advantage of flexibility in responding to non-compliance via civil enforcement rather than criminal enforcement, and can be better suited to proceeding against corporate actors.

[51] A "lawful excuse" is one supported by the law (*Carpenter v Police* [1969] NZLR 1052). A lawful excuse may also include an honest, or honest and reasonable, mistaken belief in facts, which if true, would provide a defence, although usually it does not include a belief in legal right based on a mistake of law.
[52] While offences of strict liability do not include mens rea as a necessary ingredient of the offence and it is therefore unnecessary for the prosecution to prove that the defendant intended the action in question, there is a narrower defence of "total absence of fault" where the defendant can prove they were not at fault (on the balance of probabilities).
[53] S 134A Employment Relations Act 2000: "(1) Every person is liable to a penalty under this Act who, without sufficient cause, obstructs or delays an Authority investigation, including failing to attend as a party before an Authority investigation (if required). (2) The power to award a penalty under subsection (1) may be exercised by the Authority (a) of its own motion; or (b) on the application of any party to the investigation." Maximum penalties are $10,000 in the case of an individual or $20,000 in the case of a corporation: s 135(2).
[54] See also Reserve Bank of New Zealand Act s 66C; Employment Relations Act, s 134A; Anti-Money Laundering and Countering Financing of Terrorism Act, s 96; Serious Fraud Office Act 1990, s 45.
[55] Mai Chen "New Zealand's Ombudsmen Legislation: the Need for Amendments after almost 50 years" (2010) 41 VUWLR 723 noting at 752 that the s 30 offence has never been used.

Recommendation 6: Proceeding with public register reform

110 **I recommend that the public register privacy principles (and related provisions) in Part 7 of the Act should be repealed and in their place the Act should provide for:**

110.1 the suppression of personal information in public registers in appropriate circumstances, where there is a safety risk, by way of application to the Privacy Commissioner;

110.2 complaints to the Privacy Commissioner in relation to breaches of access conditions as provided in each public register enactment.

111 I consider it timely to address the recommendations in the Law Commission's report on public registers (2008) in conjunction with modernisation of the Act. Part 7 of the Act is a product of its time and is in need of a fundamental overhaul.

112 Public registers are registers or databases of information to which the public has some specific statutory right of access (for example the electoral rolls, land registers, company registers and occupational registers). The legislative regulation of public registers is via a combination of the individual statutes that set up each register, the four public register principles in Part 7 of the Privacy Act (in relation to those public registers listed in Schedule 2), and Part 6 of the Domestic Violence Act that allows people under protection orders to apply to each registrar for their personal details to be suppressed.[56]

113 Part 7 of the Act sets out four public register privacy principles and related provisions, that apply to certain public registers listed in Schedule 2, and was included in the Act to meet the perceived need in the early 1990s (when the internet was in its infancy) to provide a minimum set of safeguards for public registers, that were predominantly paper-based at that time. Over time, these minimum safeguards are increasingly unnecessary due to the evolution of electronic registers and the inclusion of relevant privacy safeguards directly in the statute establishing the relevant public register, as recognised by the Law Commission in its report.

114 The Law Commission's recommendations included a high level proposal for repeal of the public register privacy principles (the "PRPPs") and review of existing public registers (R1), as well as a number of specific practical and targeted recommendations addressing particular issues with public registers (R5-13).

115 In its consultation, the Law Commission found little support for continued use of the PRPPs.[57] I support their repeal as the PRPPs no longer have any utility and do not act as any practical check on the availability, dissemination or reuse of public register information in the current digital environment and more relevant safeguards are now included in the legislation governing the particular public register.

116 The Law Commission recommended a comprehensive review of the existing public registers.[58] While that may have been a desirable policy objective in 2008, I do not believe that such a review remains necessary or desirable. Since 2008, numerous public register statutes have been amended or are in the process of amendment. My Office is consulted and provides guidance on proposed amendments to public register statutes as they arise. This provides the opportunity to address public register reform with the agencies concerned and in my view has proved effective to improve the quality and consistency of the design of public register statutes.

[56] Law Commission *Public Registers – Review of the Law of Privacy Stage 2* (R 101, 2008).
[57] Law Commission *Public Registers – Review of the Law of Privacy Stage 2* (IP3, 2007) at [263].
[58] 55 enactments are listed in Schedule 2 as containing public register provisions.

117 I recommend continuing and formalising this approach. Given the variety of purpose and information in public registers, functional oversight is better dealt with statute by statute rather than via the PRPPs (a practice that has led to the PRPPs no longer having any continuing useful or practical role).

118 Part 7 of the Act should therefore now be repealed. In its place, the Act should provide for any specific privacy safeguards, such as the suppression of personal information in cases requiring the protection of personal safety. The case for enhancing available suppression mechanisms is supported by research carried out by my Office last year in the local government sector.

Discussion

119 The four public register privacy principles apply to certain public registers of information set up under other enactments that are listed in Schedule 2 to the Act (55 enactments are currently specified as containing one or more public register provisions). The PRPPs purport to limit the way that public registers can be searched, and how information from public registers can be re-sorted or combined for commercial purposes, and to limit the ability to charge more than a reasonable charge for public register information. However they no longer provide an adequate basis to regulate public registers and there are few penalties for misuse of information obtained from a public register.[59]

120 I consider Part 7 of the Act is now overdue for reform. These public register provisions have not been substantively updated since they were first introduced and have largely become ineffective due to the way that registers are now organised and made available. The need for public register reform was canvassed in the Law Commission issues paper and report dedicated to the issue, as well as the earlier 1998 recommendations of the Privacy Commissioner.[60] While the detailed government response to these recommendations was deferred until other aspects of privacy law reform had been progressed, public register reform should now be included in the proposed modernisation of the Act.

121 As I submitted to the Data Futures Forum in 2014,[61] New Zealand has a robust legal framework for managing personal information but there are some key areas where reform is needed to improve this framework so that it is fit for purpose to maximise the benefits and opportunities for New Zealand in the use and re-use of data. One area that I suggested for reform, to better support the four values of the Data Futures Forum (Value, Inclusion, Trust and Control) is to update the regulation of public registers.

Law Commission's recommendation for repeal of PRPPs and review of public registers

122 The core Law Commission recommendation was for a fundamental reform, it being to repeal the PRPPs and related provisions in Part 7 of the Act and primarily regulate public registers through their establishing statutes (Law Commission recommendation 1). This recommendation proposed a systematic review of each public register against a standard set of criteria with a view to future regulation being appropriately a matter for each statute that establishes a public register. However, this recommendation for a systematic review had significant resource implications to implement, and in my view such a review is now unnecessary as a precondition to repeal of the PRPPs.[62]

[59] See John Edwards "Public registers and privacy" NZLJ (May 2007) 146.
[60] Privacy Commissioner *Necessary and Desirable – Privacy Act 1993 review* (1998) Part VII, recommendations 91, 98, 99.
61 https://privacy.org.nz/news-and-publications/reports-to-parliament-and-government/new-zealands-data-future-a-view-from-the-privacy-commissioner/
[62] The Law Commission's proposal at para [5.19] was for a dedicated review team of 6 staff and a manager to conduct the review over 12 months at a cost of $800,000.

123 As a practical matter, my Office is consulted on substantive amendments to the establishing statutes as they arise so that appropriate privacy safeguards are included.[63]

124 A survey of the Schedule 2 public register enactments added or amended since the Law Commission recommendations in January 2008 shows that progress has been made in improving the quality of the public register provisions in relation to existing or new registers, supporting the case for repealing Part 7. Sample amendments include:

124.1 The Births, Deaths, Marriages, and Relationships Registration Amendment Act 2008 inserting new s73 – 75G relating to the access register of requests for access to source documents;

124.2 Financial Service Providers (Registration and Dispute Resolution) Act 2008 establishing a register of financial service providers;

124.3 Insurance (Prudential Supervision) Act 2010, adding s 227 establishing a register of banned persons;

124.4 Health and Safety in Employment Amendment Act 2013, adding s 19ZZB-19ZZD in relation to the register of industry health and safety representatives;

124.5 Financial Reporting Amendment Act 2014, adding s 36N in relation to the register of approved persons;

124.6 Te Ture Whenua Maori Bill, clause 270, in relation to the Maori Land Register.

125 In light of the improvements that have been achieved since the Law Commission's report, and as an alternative to the Law Commission's proposal for a global review of all public registers, I support including an explicit function of the Commissioner in the Act to review any public register (whether or not a Schedule 2 register) and to publicly report my recommended amendments to the relevant statute that may be necessary to give protection or better protection to the privacy of the individual. An update of my function to monitor public registers (s 13(1)(e)) would allow me to undertake a more systematic review programme and prioritise any remaining areas where amendments to existing public register provisions are desirable. The new function could also promote best practice criteria to be used in drafting these provisions.[64] I recommend that the replacement function should be along the following lines:

> to monitor the establishment, operation and use of public registers[65] and to publicly report on the need for or desirability of taking legislative, administrative or other action to give protection or better protection to the privacy of the individual.

126 This new function could usefully be accompanied by a new or amended Cabinet Office Circular that requires agencies to consult with my Office when proposing new or amended public register provisions.

[63] The Legislation Design and Advisory Committee guidelines on process and content of legislation (2014) at [7.3] recommend seeking advice on legislative proposals for public registers from the Privacy Commissioner, the Ministry of Justice and the Government Chief Privacy Officer.
[64] Current guidance for agencies is available from OPC's website: https://privacy.org.nz/news-and-publications/guidance-resources/drafting-suggestions-for-departments-preparing-public-register-provisions/
[65] Public registers should be defined to include both the registers currently listed in Schedule 2 and other public registers not currently included.

Law Commission's specific recommendation relating to suppression

127 The Law Commission made specific recommendations about enhancing the protection of the personal details of vulnerable individuals where disclosure on the register would put their safety at risk, and improving processes for protecting the personal details of individuals who have protection orders under the Domestic Violence Act 1995 (recommendations 5-8).

128 Implementing these recommendations would represent tangible and practical privacy enhancements and should be included in the proposed modernisation of the Act. In my submission to the Department of Internal Affairs earlier this year in relation to access to births, deaths, civil unions and name change information I noted the following:

> there is not currently a central point to contact to request suppression where an individual may appear on multiple public registers. The law expects a great deal from individuals in expecting them to know what registers they are on and who to contact. While that central contact agency currently does not exist, the Department could play a role in making it easier for individuals to seek suppression from other registers where personal safety is concerned. At the very least, the Department could provide a list of contact points for other register suppression mechanisms, or pass suppression requests on to the registrars of those registers.

129 The case for enhancing available suppression mechanisms is supported by research carried out by my Office last year. Our survey of local authorities indicated highly variable levels of opt-out under the suppression mechanisms provided by the Local Government (Ratings) Act 2002 and low numbers of opt-outs under the Domestic Violence Act 1995 regime.[66] The results of this survey indicate that current suppression mechanisms may not be operating as intended in the local government sector and warrant re-assessment.

130 Of 78 local authorities surveyed about numbers of ratepayers seeking suppression of their personal details from the ratings database, 41 responded with percentages of residents seeking suppression ranging from 25% in the case of one local authority, nearly 15% in the case of another, between 5-10% in the case of six local authorities, and less than 5% in relation to the other authorities surveyed, with the majority of those under 2%. While one large city reported 20,000 residents had sought suppression of their personal details, another reported no applications had been received at all.

131 Only six local authorities reported applications under the Domestic Violence Act for the suppression of personal details from Council administered public registers and numbers of recorded applications were very low – only 11 applications were recorded as having been received (in total) by these authorities in the period 2012-2014.

132 These survey results indicate a lack of consistent practice in the use of the current suppression mechanisms and support the Law Commission's recommendation for a single uniform protective mechanism for most public registers, and a role for the Commissioner in considering applications for suppression.

66 The Domestic Violence Regulations 1998, reg 6, requires a protected person to make a separate application in respect of each such register. However, if those public registers are administered by the same agency, the protected person may make a single application to that agency in relation to those public registers.

Privacy Commissioner
Te Mana Matapono Matatapu

APPENDIX

RECOMMENDATION 2 – CONTROLS ON RE-IDENTIFICATION

CASE EXAMPLES ILLUSTRATING RE-IDENTIFICATION PROBLEMS AND RISKS

Latanya Sweeney's challenge to anonymised health care data (1997)

1 A famous and early example of anonymisation failing was demonstrated by Dr Latanya Sweeney.

2 The Massachusetts Group Insurance Commission decided to release anonymised health data on state employees. Its aim was to help health researchers to improve healthcare. Obvious identifiers such as name, address and social security number were removed from the data. The Massachusetts Governor at the time, William Weld, assured the public that the Group Insurance Commission had protected patient privacy by deleting identifiers.

3 A graduate student in computer science at MIT, Latanya Sweeney, requested a copy of the data, and got to work. She knew that Governor Weld resided in Cambridge, Massachusetts, a city of 54,000 residents and seven ZIP codes. For $20, she purchased the complete electoral rolls for Cambridge. These included the name, address, ZIP code, birth date and sex of every voter. Only six people in Cambridge shared Governor Weld's birthdate. Only three of those six were men, and of them, only he lived in his ZIP code. Dr Sweeney had the Governor's detailed health records, including diagnoses, prescriptions and details of hospital visits, delivered to his office. Sweeney's exercise demonstrates the risks involved in linking de-identified datasets with other datasets that contain linking information and the identity of an individual to derive personal information.

4 Latanya Sweeney has continued to research in this area, and has revealed that our intuitive beliefs about how easy it is to identify an individual from a supposedly anonymous set of data are often misplaced. Among her findings she has demonstrated that 87% of the US population can be identified by birth date, sex and ZIP code alone. This is particularly startling when you keep in mind that the average ZIP code has a population of around seven and a half thousand.[67]

5 As more datasets are linked together there are an increased number of vectors for identifying a target. So, while you might not have information about a target's birthday, you might know what they studied at University. Or how many children they have, or whether they've ever been convicted of an offence.

The Netflix Prize dataset (2008)

6 The re-identification of the Netflix Prize dataset by Arvind Naryanan in 2008 took de-identified data about 500,000 Netflix subscribers and matched it with publicly available information to uncover sensitive information about them, including their political preferences.[68]

7 Narayanan and Shmatikov showed that the set of movies a person had watched could be used as an identifier. Netflix had released a dataset of movies that some of its customers had watched and ranked as part of a competition. Although there were no direct identifiers

[67] To put that in the New Zealand context, the average population of a Statistics New Zealand mesh block is about 90. For the next largest statistical unit, the "area unit", the average population is 2100.
[68] Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset) http://arxiv.org/pdf/cs/0610105.pdf

in the dataset, the researchers showed that the movies watched could be linked to a user profile from the Netflix database to a single user profile in the Internet Movie Data Base (IMDB).

Scott Peppet and the Internet of Things (2014)

8 Scott Peppet, a professor of law at Colorado School of Law, wrote in a 2014 paper on the Internet of Things that researchers at MIT recently analysed data on 1.5 million cell-phone users in Europe over 15 months and found that it was relatively easy to extract complete location information about a single person from an anonymised dataset containing more than a million people. In a stunning illustration of the problem, they showed that to do so required only locating that single user within several hundred yards of a cell-phone transmitter sometime over the course of an hour four times in one year. With four such known data points, the researchers could identify 99 percent of the users in the dataset. As one commentator on this landmark study put it, for sensor-based datasets "it's very hard to preserve anonymity".

United Kingdom's care.data initiative derailed (2014)

9 As well as the risk to individuals, the ability to identify individuals within a large dataset can jeopardise the dataset's objectives. This is a feature of debates in the UK over the government's decision to make detailed NHS data available to researchers through its care.data initiative.

10 Privacy campaigners pointed out that where the details of treatments were in the public domain, such as then Labour leader Ed Milliband's nose operation to cure a sleep apnoea[69], or then Deputy Prime Minister Nick Clegg's wife's broken elbow[70], it will be possible to identify the individual and 'read across' their broader NHS record.[71] Well known medical science commentator, and advocate for greater use of data in public policy Ben Goldacre summed it up in the Guardian with the title "Care.data is in chaos. It breaks my heart." As he put it: "When you're proposing to share our most private medical records, vague promises and an imaginary regulatory framework are not reassuring."[72]

11 The public outcry forced the government to delay the launch of care.data. An online tool developed by a private company was shut down and a Parliamentary select committee inquiry was initiated.

Celebrity taxi hacks (2014)

12 In 2014, the New York City Taxi and Limousine Commission released a dataset of the 173 million taxi trips taken in New York City in the previous year. In an attempt to de-identify the dataset, the Commission replaced the taxi medallion numbers and driver licence numbers with a one-way cryptographic hash. Users of the dataset discovered the hash algorithm and were able to reverse the pseudonymisation, uncovering the identity of the taxi drivers and also celebrity passengers such as Bradley Cooper, by correlation with time stamped celebrity photos of celebrities in taxis that showed the taxi medallion number.

13 This provides an illustration of how an individual's identity, pattern of behaviour, physical movements and other traits can be extrapolated from apparently anonymised datasets. There are unanticipated sources of data that might correlate with information in the dataset.

[69] http://www.telegraph.co.uk/news/politics/ed-miliband/8666354/Ed-Miliband-undergoes-successful-nose-operation.html
[70] http://www.telegraph.co.uk/news/election-2010/7633714/General-Election-2010-Nick-Cleggs-wife-fractures-elbow-in-shopping-fall.html
[71] https://medconfidential.org/2015/medconfidential-response-to-nhs-england-response-to-sky-news-nhs-security-story-and-research-by-the-oxford-internet-institute/
[72] http://www.theguardian.com/commentisfree/2014/feb/28/care-data-is-in-chaos

Australian Department of Health dataset vulnerability (29 September 2016)

14 The Australian Department of Health announced it had removed a dataset from data.gov.au recently following an alert made in the public interest from the Department of Computing and Information at Melbourne University that it was possible to decrypt some service provider ID numbers.

15 The Department of Health makes the high-value datasets it holds publicly available to enable researchers, the not-for-profit sector and health industries to extract the most value from government data. This is helping to improve health outcomes for all Australians and is popular in the university, research and health-related communities.

16 The dataset did not include names or addresses of service providers and no patient information was identified. However, as a result of the potential to extract some doctor and other service provider ID numbers, the Department of Health immediately removed the dataset from the website to ensure the security and integrity of the dataset.

17 It was reported that no patient information had been compromised, and no information about the health service providers has been publicly identified or released and that the Office of the Australian Information Commission had been made aware of the issues and is currently investigating the matter and providing independent oversight.

18 The Department of Health also reported it is undertaking a full, independent audit of the process of compiling, reviewing and publishing this data and this dataset will only be restored when concerns about its potential vulnerabilities are resolved.