Regulatory Impact Statement: Supplementary Government Response to Law Commission's report "Review of the Privacy Act 1993"

Agency Disclosure Statement

1. This Regulatory Impact Statement (RIS) has been prepared by the Ministry of Justice.
2. Privacy-related risks have changed as technological advancements have come to dominate the way in which personal information is captured, stored, and shared by public and private sector agencies within and across borders. The capacity for harm to individuals has accelerated as a result; both in terms of the numbers affected and how they are affected.
3. We have aimed for a package of privacy reforms that sends strong signals about the importance of privacy of personal information. Early intervention rather than after-the-fact responses are a focus of the proposed privacy reforms.
4. It is expected that proposed amendments to privacy settings will create some costs to businesses and public sector agencies. These costs, however, should help to reduce future breaches and associated costs, and improve the trust of clients. Given the broad scope of the Privacy Act, it has been difficult to assess the costs of some of the proposals as the impacts of the proposals may affect agencies differently.
5. As with the advice in 2012 with respect to the Government's interim response to privacy reform, analysis of options has been constrained by lack of empirical evidence about the direct and indirect economic costs and benefits of privacy law settings to individuals, businesses and Government. We are constrained by the lack of data on the scale and nature of privacy breaches in the current environment of voluntary reporting to the regulator and voluntary notification to individuals.
6. When the Law Commission's report came out in June 2011, opinion was divided as to whether significant privacy breaches were are real possibility. Since then, significant data security breaches have occurred in both the public and, to some extent, the private sectors, reinforcing the strength of the Commission's recommendations. We have considered options for responding to the Law Commission's recommendations that range from retaining the status quo to supporting the Law Commission's proposals. Other options we consider build on approaches being progressed overseas to respond to many of the same issues, and modifications of the Law Commission's proposals to take into account a broader canvas of checks and balances than were considered by the Law Commission.
7. In estimating the costs and benefits of the options and preferred proposals, we have had to rely on judgments. Our key judgement is that the law already effectively requires agencies to operate privacy systems and that the proposals in the paper therefore make marginal costs in regard to existing obligations.
8. In addition, each privacy breach is unique, which causes difficulties when attempting to estimate 'average' costs. The context is everything. The costs to businesses of mandatory notifications to individuals in serious cases of privacy breaches for example – one of the proposals – would depend on the nature of the breach, the number of individuals involved, the level of harm sustained, and so on.

9. Social impacts are also difficult to quantify. All of the proposals suggested are expected to improve the protection afforded to individuals and limit harm done to them when a serious breach occurs. Quantifying this is difficult, however, due to the lack of empirical evidence about the scale of harm occurring now, except when a major breach is exposed.

10. The key judgements we have made about the impacts on agencies are included in relevant sections in the RIS. Assumptions about costs for the Office of the Privacy Commissioner are included in Appendix 1.

11. In assessing the limitations of current privacy settings and developing its recommendations, the Law Commission undertook extensive consultation in its review of New Zealand's privacy law. Our proposals were developed in response to the Law Commission's recommendations through public sector consultation, targeted discussions with representative private sector agencies, and review of international approaches and movements.

12. Cabinet is asked in the accompanying paper to agree to:

- policy decisions for a new Privacy Bill, building on the recommendations of the Law Commission
- increased funding for the Office of the Privacy Commissioner
- the Minister of Justice presenting to the House of Representatives the Supplementary Government Response to the Law Commission's report on *Review of the Privacy Act 1993.*

13. The draft Bill will also go through a Select Committee process including public submissions. We propose also that an exposure draft of the proposed Bill be released to encourage businesses and other agencies to test the detailed approach to implementing the policy decisions.

David King
General Manager
Civil and Constitutional
Ministry of Justice

Date 13/03/14

Executive summary

1. New Zealand's privacy regime was established in the early 1990s. In that era a regime based on individual complaints was appropriate because breaches tended to impact on single individuals.
2. Since then information technology has developed significantly. Today large amounts of data can be stored, retrieved and transmitted digitally. This enables businesses and government to operate more efficiently and effectively in delivering services.
3. In this environment privacy breaches can impact on large numbers of individuals rather than single individuals.
4. Consequently a regime more focused on early identification and prevention of privacy risks, rather than after the fact remedies, is required.
5. This is the approach recommended by the Law Commission and is in line with international trends.
6. Key proposals create stronger incentives for agencies to identify and prevent privacy risks early and give a stronger role to the Privacy Commissioner (the Commissioner) through:
    - 6.1. mandatory reporting of privacy breaches – a two tier regime requiring:
        - for material breaches – notification to the Commissioner
        - for serious breaches – notification both to the Commissioner and the affected individuals when there is a real risk of harm
    - 6.2. enhanced own motion investigations – strengthening the Commissioner's existing powers to investigate emerging issues before serious harm occurs and for proactive assessment of agencies' systems and practices where privacy concerns have been identified, by increasing the penalty for non-compliance with requests for information from the Commissioner and allowing urgent requests to be made; and
    - 6.3. compliance notices – the power to issue compliance notices for privacy breaches as a result of a complaint, own motion inquiry, data breach notification or other avenue.
7. While these proposals will ensure the Commissioner has adequate tools to address privacy risks, there will be safeguards around their use to minimise compliance costs and the primary role of the Commissioner will remain to facilitate compliance and work with agencies.
8. These proposals are seen as having benefits for business and the public sector by giving the public the confidence to provide information to them. They are also seen as in line with developing international expectations for doing business worldwide, with one exception; other jurisdictions use large fines to get agencies to take notice. Our penalty-related proposals are moderate by comparison.
9. The costs involved for agencies as a whole are marginal as they are required to have privacy systems in place currently, and the Commissioner will only have resources to use the new tools in relatively limited circumstances.
10. We are also proposing amendments that will:
    - 10.1 streamline the complaints resolution process to build trust in the system and increase efficiency and effectiveness
    - 10.2 clarify the law and impose new obligations relating to cross-border flows of information to support New Zealand businesses to operate effectively internationally

10.3 fix gaps in the privacy regime, clarify the law and make compliance easier.

11 The Act currently gives the regulator limited (generally complaints-based) powers, which means that OPC is not always notified when breaches occur - our assumption is that early warning of difficulties and the use of tools such as compliance notices and own motion inquiries would assist a regulator to detect emerging and systemic issues early on, and help agencies avoid more significant future breaches.

12 The Office of the Privacy Commissioner's (OPC) current baseline is $3.2 million per annum which has remained static since 2007. OPC has sustained increasing demand for core services and is under financial pressure despite significant productivity improvements. OPC will need to be adequately resourced to perform its current functions before it can implement the proposals arising from the Privacy Act review. Once it is resourced at a sustainable base level, new functions can then be added to its responsibilities. It is recommended OPC be resourced:

12.1 to a sustainable baseline under current settings through an operational baseline increase of $0.336 million in 2013/14, $1.923 in 2014/15, and $1.722 million on-going from 2015/16;

Status Quo

13 New Zealand's privacy framework is established in the Privacy Act 1993 (the Act). The Act regulates what can be done with information about individuals and has wide-reaching implications – it applies to every 'agency', including Government, businesses, and voluntary sector and non-Government organisations.

14 The Act does not address the privacy issues associated with the cross-border flows of data, goods and services that are now routine for private sector businesses and some public sector agencies.

15 There are two main features of the Act, which are discussed below.

The Act is based on principles

16 The Act generally requires agencies to handle personal information in accordance with 12 information privacy principles. The principles are designed to govern personal information at all points of its lifecycle, from its collection to destruction. The principles are intended to be flexible enough to enable agencies to develop their own information-handling policies, tailored to the needs of the agency and its users or customers. The principles can be overridden by any other enactment.

The Act is designed to address harm primarily affecting single individuals

17 The privacy principles are designed to prevent harm occurring to individuals, and under the Act the Commissioner has an important role to play in educating agencies about their responsibilities and providing guidance in how to meet them.

18 However, the principal function of the Commissioner under the Act is to address breaches of privacy through a complaints based system. Under this system, individuals who consider their privacy has been breached and have not been able to achieve a successful remedy from the agency concerned may complain to the Commissioner. In the first instance the Commissioner attempts to achieve a mediated outcome. Where such an outcome is not possible the Commissioner may ask the Director to consider taking proceedings to the Human Rights Tribunal. These proceedings may result in damages which address specific harm to individuals.

19 Under the Act currently, there is limited ability to address wider issues raised by a complaint. Currently the Commissioner can only make recommendations in regard to such matters, and has limited ability to act where wider concerns with systems or procedures are identified or where organisations are unwilling to comply.

Problem definition

20 The Act has never been comprehensively updated although the privacy environment has changed significantly. The following broad problems with New Zealand's privacy framework have been identified:

Technology changes mean that breaches impact a large number of individuals

21 The 20 years since the Act was passed has seen extensive technological advances, for example the rise of the internet, social media, business to business and business to consumer electronic commerce. Large amounts of data are regularly stored, retrieved and transmitted digitally. International commerce and the related transfer of private information internationally is now more important than ever for a strong New Zealand economy.

22 As a result of these technology changes, the risk profile of privacy breaches has changed. It is now possible for large amounts of harm to be caused for large numbers of individuals by a single breach, rather than harm to a single individual.

23 When the Law Commission's report came out in June 2011, it was theoretical whether large scale breaches would occur, and what the impact would be. Since then, significant data security breaches have occurred in both the public and, to some extent, the private sectors, reinforcing the strength of the Commission's recommendations (for example mandatory data breach notifications).

24 A number of issues have been identified as a result of technological developments. Over the past four years there has been:

24.1 increasing demands on OPC services:

- a 36% increase in complaints to OPC
- a rise from 3 to 107 breach notifications to OPC from private and public agencies
- single breaches each involving thousands of clients - for example:
  - the Ministry of Social Development's insecure kiosks alone meant that 529,000 clients were potentially vulnerable
  - ACC's "Pullar" breach in March 2012 involved 6,700 client records

24.2 increasing concern about private sector privacy systems in the context of a regulator that has little knowledge about or control over those systems, while financial and other personal information is increasingly stored and transmitted electronically

24.3 a proliferation of under-developed public sector privacy systems, as outlined in the Chief Government Information Officer's Review of "Publicly Accessible Systems" and associated February and May 2013 papers to Cabinet

24.4 a loss of public trust in agencies and how they secure and use personal information – an October 2012 Colmar Brunton poll undertaken soon after a Ministry of Social Development privacy breach, for example, revealed that 60% of respondents did not trust government departments to protect their personal information

24.5 continuing breaches by agencies.

25 The costs of breaches are significant. Key information collected by agencies in both the public and private sectors is financial: income, assets, debts, and expenditure. Personal information about violence, abuse, injury, ill-health, family issues, and children is also collected by some government agencies. The costs of privacy breaches include:

25.1 costs to consumers such as financial losses; loss of dignity; negative psychological impact and emotional distress; time diverted towards, and financial cost associated with, recovery efforts; and the opportunity for identity theft

25.2 costs to agencies such as negative publicity; loss of client confidence and trust, loss of clients; profit and stock market losses; and costs associated with consumer redress, recovery and legal fees

25.3 social and economic costs associated with people less willing to provide personal information to public and private agencies, making assistance and commerce more difficult. If people are unwilling to seek the assistance to which they are entitled, there will be social and community costs. If commerce suffers, economic growth suffers too.

26 Given the changed risk profile as a result of technology, the real prospect of breaches and their significant consequences, it is socially desirable for most privacy breaches to be avoided rather than addressing the harm caused by breaches as is the primary focus of the current Act. Therefore, the key problem with the current regime is that there are insufficient incentives for agencies to identify and address privacy risks before breaches occur.

27 It might be argued that the recent privacy breaches have themselves raised the importance of privacy and strengthened the reputational incentives on agencies to address privacy risks. This RIS assesses the status quo on the basis that there are now stronger incentives. However, the judgement is that the key problem remains because experience with regulatory regimes suggest that memory of failures fade over time, the attraction of short term gains that risk long term reputation dominate, and poor practice reasserts itself without wider incentives to pay on-going attention to privacy risks.

28 The key challenge then is to identify and assess options that will better enable privacy risks to be identified and addressed earlier by agencies.

Principles based approach

29 As noted above, the Act is based on principles which allow agencies the flexibility to apply the Act in the way that best fits their circumstances.

30 However, a consequence of retaining this flexibility is that the Act does not provide the certainty of "bright line" rules. The Law Commission's Review identified that the flexibility of the Act's principles also means that there can be a lack of prescription and different interpretations and applications of those principles by agencies. The Law Commission recommended more focus on education and guidance for agencies. This was supported by the May 2013 Cabinet paper on the Chief Government Information Officer's Review of "Publicly Accessible Systems" which identified "room for improvement in the support provided to agencies to aid compliance with information security and privacy standards, through the provision of clear and coherent guidance and advice".

31 This lack of prescription may be particularly important given the technological changes identified above. The Law Commission recommended a number of recommendations to fix gaps in the privacy regime, clarify the law and make

compliance easier. The Government agrees with the majority of these recommendations.

The Law Commission Review

32 The Law Commission undertook a four stage policy overview to assess privacy values, changes in technology, international trends, and their implications for New Zealand civil, criminal and statute law.

33 On 21 March 2012 the Government tabled its interim response to the Law Commission's review of the Act. The Government has accepted the majority of the Law Commission's recommendations.

34 Appendix 2 lists all the Law Commission's recommendations addressed in the Supplementary Government Response and their status in this RIS.

35 Attached as Appendix 3 is a table summarising the status of all of the Law Commission recommendations responded to in the interim, and in this supplementary, Government response.

Objectives

36 The 2012 interim Government response identified the importance of retaining aspects of the Act that work well while making it easier to navigate and understand. Without explicitly developing objectives for the privacy reforms at that stage, preliminary high level decisions were taken in the context of:

36.1 a generational shift in technology

36.2 public expectations about security of personal information

36.3 how business (government and private) is conducted today, both domestically and internationally.

37 Subsequent analysis of the problem definition with respect to the privacy regime and options for addressing that, including analysis of the Law Commission's recommendations, has determined that the desired aim of the reform of privacy is sound privacy, balanced law so that:

37.1 individuals have confidence that information shared with private and public sector agencies will be adequately protected

37.2 as a result of that confidence, public and private sector agencies are able to access the information they need from the public to provide goods and services as effectively and efficiently as possible.

38 These aims are consistent with the approach taken in the interim Government response, the Law Commission recommendations, and international trends.

Regulatory impact analysis

39 Changes to the regulatory regime would have to be made by legislative amendment. The only other viable alternative is for OPC to issue guidance material to either supplement existing legislation or as an alternative to additional regulation. Guidance and education material recommended by the Law Commission is already being developed by OPC.

40 The proposed reforms in this supplementary Government response reflect the decisions already made by Government in its initial response including agreement to replace the current Privacy Act with a new Act and agreement to retain a principles-based approach to the regulation of privacy.

41 The detail in this RIS focuses on the extent to which current gaps and weaknesses in the privacy status-quo can be addressed through the implementation of the

outstanding recommendations or through alternative options. A critical issue is whether the package of proposed amendments creates the best balance of privacy protection, voluntary compliance, and complaint resolution at the lowest level, to ensure that people are protected without overregulation. Overregulation creates unnecessary burdens and costs on businesses and government. The package of reforms proposed here aims to find that balance.

42 In the analysis that underpins this RIS, each possible option for responding to identified problems or gaps is evaluated for its ability to align with our objectives and for its impacts. The Government's recommended approach in this RIS only includes the option considered to be the most optimal in this respect. The recommendations categorised in the fourth cluster of reforms are less significant and of a more technical nature compared with those in the other clusters. For this reason, more analysis is shown in the RIS with respect to the first three clusters. In these, the options considered are:

42.1 the status quo

42.2 the recommendation(s) of the Law Commission

42.3 the Government's recommendation, which is one of the following:

- agree with the Law Commission's recommendation(s)
- reject the recommendation(s) and retain the status quo
- agree to a modification of the recommendation(s)
- propose a completely new approach
- defer.

43 The Government's recommendations have been developed and assessed using an intervention logic approach taking into account these assessment criteria:

43.1 the problems/issues

43.2 our objectives

43.3 what regulatory and non-regulatory options could be considered to address the problems and achieve our objectives

43.4 the likely impacts (costs/benefits) of each option including:

i. economic, including compliance impacts

ii. fiscal

iii. cultural

iv. environmental (none)

v. social[1]

43.5 international comparisons

---

1 All of the Government's recommendations will have social impacts in that they aim to enhance protection and confidence for individuals without impinging on the capacity of business and government to work effectively. Any drag on the operation of business and government would have social impacts as well as economic, such as reduced ability to employ more staff. All of the Government's recommendations are expected to enhance social protection and confidence compared with the status quo and, in some cases, compared with the Law Commission's recommendations.

43.6 how it would contribute to the overall package of reforms in balancing the protection of individuals on the one hand and the burden on agencies on the other

43.7 risks – where risks are identified, these are identified in red text.

44 For the first three clusters of more significant recommendations, a 'traffic light' approach is used, in this way, to aid understanding:

- denotes that the relevant regime does not meet objectives and does not result in the best outcomes
- identifies that the relevant regime only goes part-way to address the problem and meet objectives, and results in mixed outcomes
- indicates the preferred regime for addressing the problem, meeting objectives, and achieving good outcomes.

1. Enabling the Privacy Commissioner to better identify, investigate and address emerging privacy risks proportionately

The public's trust and confidence in the collection, use and storage of personal information is fundamental for good business and government. People expect information to be used efficiently, but within acceptable limits.

Status quo and problem identification

As discussed earlier, the combination of the Commissioner only being able to make recommendations, a lack of prescription in our privacy laws and limited powers of the regulator mean that breaches are common and there are few incentives in law for agencies to avoid future breaches. The technological advances of the past 20 years are critical for government and business to operate effectively. The increased reliance on technology has, however, increased the risks around privacy breaches.

International norms reveal that the four components of the privacy risk reduction package are: (i) breach notification to the privacy commissioner and to affected individuals; (ii) privacy commissioner audits or investigations; (iii) privacy commissioner compliance notices or orders; and (iv) either financial penalties for non-compliance or enforcement through a court of law, or both.

Key international jurisdictions (such as Australia, the UK, and Canada) shape these four components in different ways but they are always part of a packaged approach to set the bar for agency compliance with solid privacy standards. Most jurisdictions (federal and state or provincial) already provide for (or have Bills going through the House to provide for) mandatory reporting to a privacy commissioner and to affected individuals of breaches at risk of causing serious harm to individuals. All provide the commissioner with the power to undertake audits or own motion investigations where there is just cause (such as a complaint or a breach has already occurred) and to command access to the information required to undertake that investigation. In all jurisdictions compliance notices or orders can be used to enforce change, and these are supported by penalties or court action for non-compliance.

In New Zealand, breach notification is currently voluntary, own motion investigations are provided for and compliance notices and associated penalties are not provided for in the current law.

Addressing the problem and potential outcomes

The Government proposes to address compliance and enforcement weaknesses so that the Privacy Commissioner can better identify, investigate and address emerging privacy risks, proportionately. Doing so should mean that individuals have more confidence about sharing their personal information with agencies.

These proposals are:

a. a two-tier approach to mandatory breach notifications including:
   - the requirement to notify the commissioner of any material breach
   - the requirements to notify the commissioner and the individuals concerned where there is a real risk of harm

b. strengthened own-motion investigation powers including giving discretion for the Commissioner to require urgent compliance with information requests

c. compliance notices issued by the commissioner following a complaint or an investigation to require agencies to stop doing specific acts or to change their practices

d. penalties for non-compliance with a request for information.

At the same time, the intention is to support the Privacy Commissioner's role in complaint resolution at the lowest level and stopping breaches from occurring.

A. Mandatory breach notifications

Options	Description	Impacts
Status quo	Voluntary notification to the Privacy Commissioner and/or to individuals, if a breach occurs.	• The Commissioner's guidance material combined with voluntary reporting are not enough currently to help avoid breaches. • We only know about the breaches that are reported in the media, and these tend to be significant public sector breaches. • The Commissioner's powers to help prevent breaches are weak because there is no requirement for OPC to be informed of problems, and so it cannot help rectify those difficulties or help agencies avoid future breaches. • Future harm cannot be minimised. • Early detection is not incentivised. • Individuals' trust in the system is undermined by regular breaches. • The status quo is inconsistent with the proposed EU Data Protection Regulation which introduces a data breach notification requirement.
Options	**Description**	**Impacts**
Law Commission recommend-ations	**Recommendations**: 67 to 79 Require mandatory breach notices where a serious breach occurs; a high threshold. Agencies must notify the individual and the Commissioner if the breach is serious. Non-notification is grounds for a complaint to the Commissioner and could ultimately lead to Tribunal proceedings and damages.	• Notification to the Commissioner and to affected individuals would enable an opportunity for the Commissioner to help avoid future breaches and for the agency to provide redress where harm has occurred. Improved confidence and trust of individuals as a result. • Consistent with the proposed EU Data Protection Regulation and would signal to overseas jurisdictions that our privacy laws are robust. • Mandatory breach notification is potentially costly for agencies in the short term if new systems need to be implemented, but has the potential for longer term savings for an agency if client confidence is maintained and system issues are addressed. • The scale and cost of the notification process for each breach is influenced by the nature of the issue, the level of harm to individuals, and the number of individuals affected. Actual costs are currently not possible to estimate. • Potentially an increased volume of complaints to OPC, which is difficult to estimate and cost. If there was a 25% increase over current volumes, costs for OPC may increase by up to $0.560 million p.a., using 2011/12 figures as the baseline for the number of complaints and the average cost per complaint. Volumes could be mitigated by the introduction of rec 60 about representative complaints.

		• Risk: the potential volumes of complaints, and the scale of the mitigation impact of recommendation 60, are difficult to estimate.	
Govt recommend-ation	**Modified** recommendations of the Law Commission – Reasonable steps to notify the: • Commissioner of material breaches • Commissioner and affected individuals of breaches where there is a real risk of harm. Recommendation 79 suggests that OPC create new guidance material, and the Ministry of Justice has undertaken to discuss this with OPC once Government has accepted other relevant recommendations. *Exceptions* – agencies will not need to notify breaches if the agency believes, on reasonable grounds, that there are public interest grounds mitigating against notification that outweigh the public interest in notification e.g. where notification is likely to prejudice the security or defence of New Zealand or its international relations, or where notification could make matters worse for vulnerable people. If a non-notified privacy breach becomes public, agencies would have to satisfy the Commissioner (and, if necessary, the Human Rights Review Tribunal) that an exception applied. *Penalty* fine of up to $10,000 upon conviction of failure to notify Commissioner of either tier one or tier two breaches.	• The lower threshold for reporting would enable OPC to be more proactive in promoting compliance, to work with agencies to educate and raise awareness of good practice *before* serious breaches occur, and to detect systemic problems. • Potential to help avoid more serious breaches that would otherwise be accompanied by higher costs to agencies and added harm to individuals. • Improved confidence and trust of individuals to a higher degree than other options. • Whether the fine should be a civil penalty rather than a criminal offence can be determined in the context of the Government Response to the Law Commission report on the Law Relating to Civil Penalties (final report due in 2014).	
Mandatory breach notifications - summary	On balance, the option of regulating for the reporting of all material **and** serious breaches has the most potential to meet the Government's objectives of bolstering the privacy protection and confidence of individuals while assisting agencies (Government and private) to avoid more serious and costly future breaches. It is consistent with a balanced and fair approach that aims to minimise harm. There are risks relating to the difficulties in estimating the potential increase in the volumes of complaints; each of which is a cost to OPC.		

B. Compulsory audits or strengthened own motion investigation powers

Options	Description	Impacts	
Status quo	The Commissioner can undertake an own motion inquiry into any matter if it appears to the Commissioner that the privacy of an individual is being, or may be, infringed. The Commissioner has compulsory information-gathering powers and can summon witnesses. Every person commits an offence and is liable to a fine of $2,000 if they fail to comply with the lawful requirements of the Commissioner.	• Emerging and systemic issues cannot easily be identified.	
Law Commission recommend-ations	**Recommendations**: 64, 65 Allow compulsory audits where there are good reasons. The Commissioner could (i) undertake the audit; (ii) require the agency to self-audit or (iii) commission an audit. Good reasons include: reasonable grounds to believe an agency's systems are inadequate; the agency handles particularly sensitive information; or the agency is engaging in a new or untested practice.	• Early identification of issues within an agency. A means of identifying and investigating more serious issues. • Signals to business and government agencies to consider the security of their systems – but, rightly or wrongly, people have the sense that audit is something that happens after the event, and that occurs within an agency, whereas we need a mechanism that can look across the sector as well as within an agency, and in a proactive manner where possible. • The likely volume of audits is difficult to estimate and cost. If the number was to be five times higher than the status quo, and increase in scale, the costs would increase from $0.280 to $1.400 million p.a. • The Law Commission did not recommend who should bear the costs of the audits. • Risk: likely volume of audits difficult to estimate.	
Government recommend-ation	**Modified** status quo: • give the Commissioner the discretion to decrease the time for agency compliance with the Commissioner's evidence power from the maximum of 20 working days • increase the offence penalty for offences for not complying with requests for information from $2,000 to a maximum of $10,000.	• Strong signals to agencies to proactively consider the security of their systems. • OPC would continue to have discretion about which investigations to progress, ensuring proportionality of response. Likely to achieve the same purpose as the LC recommendation. • OPC can work with an agency to improve privacy systems alongside the issuing of a compliance notice requiring changes to an agency's systems or behaviours. • Should improve confidence and trust in how agencies use personal information.	

Govt recommend-ation *(cont)*	OPC to publish a protocol about how it will go about conducting the own-motion inquiries, to ensure transparency.	• If the number of investigations was to double and increase in scale (as is expected), the cost to OPC of own-motion inquiries would increase from $0.280 to $0.700 million p.a. This is expected to include any additional costs relating to establishing a protocol about the own-motion inquiry process. • If the Commissioner issues compliance notices requiring upgrade of information systems, this could require significant capital expenditure. OPC's experience to date, however, is that compliance largely relates to enforcing rules, checks, and balances that are already in place but not used, rather than introducing new systems. • OPC meeting the costs of these investigations would guard against overuse of power. • Risk: the volume and scale of inquiries is difficult to estimate.
Compulsory audits - summary	The best outcomes for individuals, agencies and for OPC, on balance, are likely to result from a combination of strengthened powers for OPC to compel the provision of information and for it to work with an agency alongside the issuance of a compliance notice. Strengthened own motion powers would build on the Commissioner's focus on facilitation and resolving issues at the lowest level, and enable a cross-sector view. The audit option potentially poses significant financial risks for agencies. The key risk is that the number and scale of own-motion inquiries under the proposed regime is difficult to estimate, but will impact on cost.	

C. Compliance notices

Options	Description	Impacts
Status quo	The Commissioner relies on voluntary compliance because she cannot require agencies to change their practices. She has limited ability to act where wider concerns with systems or procedures are identified through the complaints process or other avenues, or where agencies are unwilling to comply.	• There is limited capacity to prevent breaches or minimise harm. The Commissioner does not currently have the power to respond where there has been: - repeated non-compliance - a failure to alter practices despite assurances during the settlement process - a breach, and there is an opportunity to minimise the harm to individuals. • Business and government agencies are not compelled to address any weaknesses in their privacy systems. • Individuals are not adequately protected.

Law Commission recommend-ation	**Recommendation**: 63 This recommendation would give the Commissioner the power to issue a compliance notice for privacy breaches, either in response to a complaint or through an own-motion inquiry. There would be the right to challenge the notice through the Tribunal. Non-compliance would be an offence under the Act.	• OPC not expected to incur additional costs from issuing compliance notices per se, as a compliance notice would replace some of the current 'closing letters' from an investigation. • Risk: a departure from the current voluntary compliance regime incurs a risk of impacting on conciliation. Agencies may become more adversarial, and there may be a perception of reduced incentives for the OPC to settle complaints. • More appeals might be expected during a transitional period, which will then drop off. Costs relating to appeals may be up to an additional $0.070 million in 2014/15 and $0.140 million in 2015/16. • Businesses are not expected to incur additional compliance costs as, in OPC's experience, compliance largely relates to enforcing rules, checks and balances that are already in place but not used, rather than implementing new systems. • Individuals are more protected, with improved confidence and trust in the use of their information by agencies.
Government recommend-ation	**Agree** with the recommendation of the Law Commission. Adopt.	• To mitigate possible adversarial responses, the legislation can emphasise that conciliation is the overriding objective, and compliance notices are to be used as a backstop if conciliation is not successful. • The OPC could issue guidance outlining how, and when, compliance notices will be issued.
Compliance notices - summary	Compliance notices are considered to be a potentially significant factor in preventing future breaches and minimising harm to individuals; important objectives for privacy settings and weaknesses of the status quo. This is because they place enforceable requirements on agencies to change their practices for the better. This option is accompanied with a risk however that, for a transitional period, the currently non-litigious settlement process becomes more litigious.	

2. Clarifying business obligations when private information is transferred across borders

Cross-border transfers of personal information are increasing in both number and complexity. Cross-border transfers of personal information fall into two main groups. Cross-border outsourcing is where an overseas provider holds and processes information on behalf of a New Zealand agency. Cross-border disclosures occur where a New Zealand agency discloses information to an overseas agency and the overseas agency then uses the information for its own purposes.

Status quo and problem definition

Cross-border outsourcing

There are gaps in current privacy law dealing with cross-border outsourcing. In some situations no agency is responsible for protecting the privacy of the data. Currently, a New Zealand agency remains liable for information it outsources to an overseas service provider. However, this liability depends on how the service provider uses the information. If the overseas service provider uses or discloses the information for *its own purposes* the New Zealand agency is no longer liable. For example, if the service provider used the information for its own purposes and had a data breach, the New Zealand agency would not be liable. An individual in New Zealand harmed by the data breach would be unable to bring a complaint against either the New Zealand agency or the overseas service provider (the service provider is not subject to New Zealand law).

In addition, the relevant provision is poorly drafted and difficult to find in the Act. We consider it is likely that some agencies may be unaware of their obligations regarding outsourced information.

Cross-border disclosures

Once information has been disclosed to an overseas agency there is no guarantee the information is subject to adequate privacy standards. Currently, a New Zealand agency can disclose information to an overseas agency if the disclosure complies with the Information Privacy Principles. There are no further obligations on the New Zealand agency to ensure the information will continue to be subject to adequate privacy standards in the overseas jurisdiction. This means that New Zealanders' personal information can be disclosed to an agency in a jurisdiction with no or inadequate privacy law. As with cross-border outsourcing and individual would not be able to bring a complaint against the overseas agency as the overseas agency is not subject to New Zealand law.

Cross-border enforcement and international privacy rules

More generally, current privacy law does not adequately address how New Zealand cooperates with other jurisdictions with respect to privacy violations. Nor does it enable New Zealand agencies to formally adopt international privacy rules that reduce the compliance costs associated with the cross-border transfer of information.

Addressing the problem and potential outcomes

The proposals are:

a. cross-border outsourcing – clarify in law that an agency that outsources personal information services to an overseas provider is accountable for what happens to that information, and is responsible for any breaches of privacy by the service provider

b. cross-border disclosures – a new privacy principle requiring disclosing agencies, with some exceptions, to take reasonable steps to ensure that the information will be subject to acceptable privacy standards in the foreign country; the Act will provide guidance on reasonable steps. One of the exceptions will be that agencies can provide information offshore so long as clients authorise an agency to do so in the full knowledge that the standards of the privacy laws in the offshore country may or may not be adequate

c. cross-border enforcement cooperation – provide the Commissioner with the powers to share relevant information with overseas privacy enforcement authorities, provide assistance to overseas authorities in relation to possible violations in their privacy laws, engage in mutual assistance with overseas counterparts, and cooperate with other authorities and stakeholders

d. cross-border privacy risks – undertake further work to determine whether the APEC cross-border privacy rules may provide a mechanism to reduce the compliance costs of businesses trading in multiple jurisdictions.

A. Cross-border outsourcing

Options	Description	Impacts
Status quo	There is a gap in current law regarding outsourcing of personal information: where a NZ agency sends information to an overseas provider for storage and processing, such as Cloud and offshore data processers. Agencies are generally accountable for such information. However if the overseas provider uses the information for its own purpose (not the purpose of the outsourcing NZ agency), then the NZ agency is no longer deemed to 'hold' the information.	• A NZ agency is not accountable for the overseas provider's breach of NZ privacy laws. A person in New Zealand whose privacy is breached by the overseas provider would have no redress in New Zealand under the Privacy Act. • The risk of impact actually occurring may be partially mitigated by the potential reputational damage to an NZ agency if their overseas provider misuses personal information. Some NZ agencies will already be ensuring they deal with reputable overseas providers and that there are adequate systems in place to prevent the provider misusing the information.

Law Commission recommend-ations	**Recommendations:** 107, 109. Clarify that an agency that outsources personal information services (such as storage and processing) is accountable for what happens to that information, and is responsible for any breaches of privacy by the service provider. This approach would clarify that a New Zealand agency remains accountable under the Privacy Act for what happens to information outsourced to an overseas service provider.	• Increased protection for individuals when their information is outsourced to an overseas service provider. Individuals will have more confidence that their personal information is protected and they will be more inclined to provide the private information needed by the agencies. • We are unable to quantify the costs for agencies as this will depend on how agencies currently deal with outsourcing. For example, whether an agency already ensures that the information will be appropriately protected (some agencies already do this as a matter of sound business practice, but others may not). We have assumed the costs will be minimal as the proposal is closing a discrete gap and is also clarifying existing legal obligations that are not clearly expressed in the Privacy Act. We acknowledge that some NZ agencies may have to take additional steps to ensure they have systems in place to mitigate against a situation where the overseas agency uses the information for its own purposes in breach of the outsourcing arrangements. It is unclear how many agencies will be impacted by the proposal and to what extent, given the broad application of the Privacy Act. • The benefit of closing this legislative gap and clarifying existing legal obligations is improving the safeguards applying to personal information and increasing protection for individuals. We consider that this outweighs the costs for businesses. • Agencies will be incentivised to ensure they outsource information to reputable companies with adequate privacy systems as the law will clearly state that the NZ agency is accountable if the overseas service provider breaches the Privacy Act. • Guidance material will provide agencies with suggestions as to how to mitigate risks when they outsource information overseas to higher-risk jurisdictions (as per recommendation 108). • NZ businesses are likely to benefit from New Zealand's laws being more closely aligned with those of likeminded trading partners such as Australia and the EU. We are unable to quantify this benefit but closer alignment is likely to facilitate trade with these countries, • There are no identified risks.	
Non-regulatory option	OPC clarification of, and guidance about, agency accountability	• Does not address the current statutory gap where a NZ agency is not responsible if the overseas provider uses the outsourced information for its own purposes. • There would be no statutory incentive for NZ businesses to deal with overseas providers that will protect the privacy of the outsourced information.	

		• Some NZ businesses will already be ensuring they deal with reputable overseas providers and that there are adequate systems in place to prevent the provider misusing the information. They are likely to continue to do this. • There would be no remedy available for an individual whose privacy had been breached by an overseas provider using the information for its own purpose (rather than in accordance with the outsourcing arrangements).	
Government recommend-ation	**Agree** to recommendations of Law Commission. Adopt.	• As for the Law Commission's recommendations.	
Cross-border outsourcing - summary	Ensuring that agencies are always responsible for what happens to personal information that they outsource is expected to improve information protection and mitigate against potential breaches. We consider that the potential for increased costs to businesses should be outweighed the proposal's benefits. This proposal will: • ensure that New Zealand's privacy practices are consistent with overseas jurisdictions • support New Zealand businesses to operate effectively internationally, based on the confidence and trust of individuals • encourage and facilitate compliance with good privacy practice. There are no identified risks.		

B. Cross-border disclosures

Options	Description	Impacts	
Status quo	No provisions in law regarding cross-border disclosures of information: when NZ agencies send personal information overseas to a foreign agency for the foreign agency's own use.	• Individuals are unprotected in the modern global approach to business, work and play. • A 2011 OPC survey of international disclosures, however, found that most responding agencies already had controls to protect the security of information in transit and to ensure that overseas organisations could not pass the information onto unauthorised third parties or use it for different purposes.	
Law Commission recommend-ations	**Recommendations:** 110-112. NZ agencies sending personal information overseas should be required to take reasonable steps to ensure that the information is subject to acceptable privacy standards.	• New compliance costs for agencies sending information overseas, as they will need to do a risk assessment.	
Government recommend-ation	**Agree** with recommendations of the Law Commission and propose that, **in addition**, the Act should: • establish a new privacy principle requiring NZ agencies to take reasonable steps to ensure that information disclosed overseas will be subject to acceptable privacy standards in the foreign country • provide guidance on reasonable steps and a list of acceptable jurisdictions • provide exceptions e.g. agencies can provide information offshore so long as clients authorise an agency to do so in the full knowledge that the standards of the privacy laws in the offshore country may or may not be adequate.	• As for Law Commission's recommendations, with additional guidance on what is reasonable and acceptable. • Public confidence in cross-border information flows is essential for New Zealand's effective participation in global markets. • Including exceptions will help to reduce compliance costs to businesses. We are unable to quantify the costs to agencies as this will depend on a variety of factors such as whether the agency discloses information overseas as part of its day-to-day business, if so, whether these disclosures are subject to contractual terms etc. • The Commissioner will have the power to publish a list of overseas frameworks that constitute acceptable privacy standards. This will help to mitigate the compliance costs to agencies. • Doing due diligence on the privacy standards of additional jurisdictions is a time-consuming job. OPC may require an additional FTE to take on this role, potentially costing $0.140 million p.a. for two years. There is a risk that this role may take longer than two years. • NZ businesses are likely to benefit from New Zealand's laws being more closely aligned with those of likeminded trading partners such as Australia and the EU. We are unable to quantify this benefit but closer alignment is likely to facilitate trade with these countries.	

Cross border disclosures - summary	Requiring agencies to take reasonable steps to ensure acceptable privacy standards of overseas jurisdictions, before sending personal information to those jurisdictions, is an important expectation in today's global and networked environment. The proposal will: • ensure that New Zealand's practices are consistent with other jurisdictions • support New Zealand businesses to operate effectively internationally, based on the confidence and trust of individuals • encourage and facilitate compliance with good privacy practice. There are no identified risks other than a small risk that the estimated costs of compiling a list of 'privacy safe' jurisdictions may increase, if the task takes longer than four years.

C. Cross-border enforcement cooperation

Options	Description	Impacts	
Status quo	a. No provisions to support the Commissioner to engage in cooperative relationships with other jurisdictions, although s72C allows consultation with overseas privacy enforcement authorities about specific complaints.	• Restricts ability to build goodwill across jurisdictions that can be drawn on to help resolve complaints.	
Law Commission recommend-ations	a. **Recommendation**: 114. Enable the Commissioner to: • share relevant information with overseas privacy enforcement authorities • provide assistance to overseas authorities in relation to possible violations of their privacy laws • engage in mutual assistance with overseas counterparts • cooperate with other authorities and stakeholders.	• Cooperation and mutual assistance creates goodwill that can be called on when we need to resolve New Zealanders' cross-border complaints. • Will help resolve issues for individuals as well as business and government agencies. • Broader cooperative powers would be a useful response to the particular challenges of enforcing privacy protection in an online environment.	
	b. **Supplement** Tribunal's procedural powers to deal with cross-border privacy complaints.	• Potentially simplifies cross-border proceedings between Australia and New Zealand. There are links to existing Ministry of Justice work on implementing the Trans-Tasman Proceedings Act. • The recommendation relates to all aspects of the Tribunal's work not just privacy matters; and so further work needs to be done to consider the broader impacts.	

Government recommend-ation	a. **Agree** with recommendation of the Law Commission. Adopt.	• How mutual assistance with overseas counterparts will operate is under consideration. There are no identified risks. • Legislative amendment is required to ensure New Zealand: - is consist with the international community; - can take advantage of developments in cross-border enforcement; and - Is in a position to provide reciprocal assistance.	
	b. **Defer.** Tribunals will be considered for inclusion in the trans-Tasman evidence regime and under the Trans-Tasman Proceedings Act 2010 (TTPA) once it comes into force. The HRRT is one of many NZ tribunals to be considered for inclusion.	• The aim is to ensure that the proposal is suitable across all areas of the Tribunal's jurisdiction and that a consistent approach is taken to implementation of the Trans-Tasman Proceedings Act 2010.	
Cross border enforcement cooperation - summary	Enabling the Privacy Commissioner to work cooperatively with overseas jurisdictions can only benefit individuals in today's environment in which cross-border flows of information are routine. There are no identified risks from this proposal. The recommendation to enable the Tribunal to deal with cross-border privacy complaints is deferred to be incorporated into a wider piece of work.		

D. APEC cross-border privacy rules

Options	Description	Impacts	
Status quo	No provisions in law relating to cross-border privacy rules.	• Businesses trading in multiple jurisdictions face significant compliance costs when they need to comply with many sets of rules across a number of jurisdictions.	
Law Commission recommend-ations	**Recommendation**: 115. Include a provision allowing for the adoption of a cross-border privacy rules system in New Zealand – to come into force at a time to be determined by Order in Council. Aimed at implementation of APEC's cross-border privacy rules system for businesses.	• Businesses trading in multiple jurisdictions would incur fewer compliance costs if they were enabled to comply with only one set of rules across many jurisdictions • Regulation many not be required for this purpose, however.	
Government recommend-ation	**Agree** that APEC's rules system could benefit businesses trading in multiple jurisdictions by allowing them to comply with one set of rules across all jurisdictions. **Disagree** with the mechanism. Some constitutional concerns about implementing legislatively a non-binding international arrangement that does not have treaty status and can be changed quite easily. Most APEC economies are exploring administrative approaches to implementing the privacy rules, and	• Not clear whether legislative change is required. • Government will consider further how APEC cross-border privacy rules could be implemented. • By not proceeding immediately, businesses do not obtain the potential benefits (reduced compliance costs) associated with APEC cross-border privacy rules.	

	New Zealand should follow this lead. The OPC is comfortable exploring this approach.		
APEC cross border rules - summary	Propose further work to determine whether APEC cross-border privacy rules may provide a mechanism to reduce compliance costs and other benefits, and if so, how to implement the cross-border privacy rules. There are no identified risks.		

3. Streamlining the complaints process

The Law Commission agrees that the privacy complaints resolution system is already reasonably effective and efficient and, on the whole, aims to keep resolution at the lowest levels.

Status quo and problem definition

A problem area, however, relates to complaints from individuals that an agency has decided not to give them access to their personal information. Currently, if the Commissioner cannot settle an access complaint, the Commissioner may decide to refer the complaint to the Director of Human Rights Proceedings. The Director will then consider whether the case should be considered by the Human Rights Tribunal. Tribunal proceedings are adversarial and court-like, and it is not an appropriate forum for resolving access complaints. Where the complainant is a party to the proceedings, the proceedings must be conducted in a way that prevents the complainant from seeing the material at issue until the Tribunal has made a determination. This raises natural justice issues.

Prompt access to personal information is a key component of international privacy laws and, in Australia and Canada, is addressed through both state/provincial laws as well as federal. Compliance notices can be used, and are enforced through financial penalties and/or court action.

Addressing the problem and potential outcomes

The proposal is to improve complainant access to their own information by giving the Commissioner the power to issue compliance notices requiring the release of the information to the individual concerned. This will streamline the complaints resolution process so that it is as efficient and effective as possible. The changes will enhance complainants' confidence that their complaints can be resolved quickly and efficiently.

A. Access determinations

Options	Description	Impacts	
Status quo	Currently complainants do not have access to the information in dispute and it is difficult for them to argue their case. Only the Tribunal makes access determinations.	• These access cases make up about half of the OPC's complaints workload and about half of the cases that are referred to the Tribunal. • The cost of the Tribunal is estimated at, on average, about $6,300 per case. Eighteen access cases were considered in 2011/12.	
Law Commission recommend-ations	**Recommendations**: 56-59. Would give the Commissioner the power to make enforceable decisions on access complaints about what information should be released and which withheld. OPC's determination would be binding on the agency, unless there was an appeal to the Tribunal.	• Improved outcomes for individuals. Would enhance complainants' confidence that their complaints can be resolved quickly and efficiently. • More efficient and effective process. Tribunal savings of up to $0.100 million p.a., if no longer required to make determinations on access cases. Would add little to the OPC costs of already handling the access case prior to escalating to the Tribunal. Proposed that these savings be absorbed into processing other complaints more quickly by the Tribunal. • Provides scaled response following investigation. • OPC can have greater oversight to identify and resolve systemic issues.	
Government	**Agree** with the	• As above. There are no identified risks.	

recommend-ation	recommendations of the Law Commission. Adopt.	• Within an environment which enables compliance notices, also discussed in the first cluster of proposals, there would be strengthened Commissioner powers to seek an assurance that the action which led to the breach will not be repeated, making conciliation more meaningful for the parties.	
Access determin-ations - summary	Enabling the Commissioner to make access determinations instead of relying on the Tribunal would improve efficiency, reduce costs, improve the trust of and outcomes for individuals, and ensure natural justice. There are no identified risks.		

B. Role of the Director of Human Rights Proceedings

Options	Description	Impacts	
Status quo	If the Commissioner is unable to settle complaints, it is referred to the Director to consider whether it should proceed in the Tribunal	• Director considers the matter afresh and appears in the Tribunal as the prosecutor • Director has expertise and experience in appearing before the Tribunal	
Law Commission recommend-ations	Recommendation: 55. The role of the Director should be removed in privacy cases and given to the Commissioner to streamline the complaints resolution process	• This would result in the duplication of resources and expertise. The Director would need to be retained for other (human rights) cases, and the Commissioner would need to develop increased expertise with respect to the (few) privacy cases. • The primary conciliation role of the Commissioner would be maintained. • The continued separation of compliance and litigation functions ensures that parties can freely engage in conciliation; •	
Government recommend-ation	**Reject**. The role of the Director in privacy cases should be retained.	• As above • There are no identified risks	
Summary	The status quo should remain to ensure the best outcomes for all parties to a privacy complaint. Opportunities to streamline the complaints resolution process are outweighed by disadvantages.		

4. Fixing gaps and making compliance easier

The Law Commission concluded that the Act is fundamentally sound.

Status quo and problem definition

The problem is the lack of clarity and the use of difficult language in the Act. Businesses, government agencies and individuals can have difficulty understanding their obligations and rights.

Addressing the problem and potential outcomes

A number of minor and technical improvements to the Act are recommended including some to improve clarity about intentions, definitions, thresholds and roles. A new purpose clause is proposed that balances privacy interests with the ability to effectively use information. Drafting improvements are also suggested to improve the clarity and workability of the principles.

This raft of less significant recommendations is considered in the following table.

Very few of these recommendations are expected to have a financial or economic impact. Any changes to the approach and scope will also have social implications, because privacy is inherent in this day and age in the way we interact, do business, work, and play. Any legal changes to protect people's privacy, however minor, will become part of New Zealand's social fabric that helps make people's lives better.

Where expected and specific impacts can be identified, they are included in the following table.

Less substantive proposals to fix gaps in the Privacy Act and to make compliance easier

No	Recommendation	Government recommendation	Discussion and impacts
3	The Privacy Act should have a new purpose section, as drafted by the Law Commission.	**Modify**	• A purpose clause would help to reduce the current variability of interpretation of the Act. The section proposed by the Law Commission is highly specified, regulatory and interventionist. As such, it is not consistent with the balance that this tranche of reforms is aiming for between protecting people's privacy and allowing business and Government to conduct business efficiently. • A modified purpose section is proposed to better acknowledge the need for protection of individuals through the good handling practices of agencies, which can be supported in a range of ways (regulatory and non-regulatory).
6	Causes of action under the Privacy Act should survive the complainant's death.	**Reject**	• A common law dictum is that personal action dies with the person. Actions for defamation and sedition are, for example, excluded from the Law Reform Act 1936 and an estate cannot sue for exemplary damages. The corollary is that a person's estate cannot be sued for a wrong committed by the deceased. • The proposed rejection of the recommendation reduces implications and costs for the estate and is more consistent with other legislation.
12	Principle 2(2) should be amended by adding a new exception covering situations where an agency believes, on reasonable grounds, that non-compliance is necessary to prevent a serious threat to the health or safety of any individual. *Principle 2 relates to the source of personal information*	**Agree**	• Would add another layer of protection for individuals.
17	Section 45 should be amended to provide that an agency shall not enable access to information that is requested under principle 6(1)(b) if the agency has reasonable grounds for believing that the individual concerned is making the request under duress.	**Agree**	• Would allow agencies to withhold information if there are reasonable grounds to believe a request for information is made under duress from another person. • Would increase public confidence that information will be used and disclosed appropriately.

No	Recommendation	Government recommendation	Discussion and impacts
18	Section 66(2) should be amended to provide clearly that failure by an agency to comply with the requirements of section 45 is an interference with privacy. Section 66(2) defines and lists interference with privacy. Section 45 requires agencies to be satisfied of the identity of a requester of information.	**Agree**	• There is no reason why the list of administrative provisions listed in section 66(2) should not include section 45. • Would enhance good business practices and relationships. • Might increase compliance costs to ensure business systems are adequate or, in many cases, might merely require the implementation of rules about using existing systems. • The number of complaints may increase.
19	"Authorise" should be defined in section 2 as excluding situations in which an individual's agreement is obtained under duress.	**Reject**	• The proposed amendment to section 17 should protect individuals under duress. A concurrent redefinition of 'authorise', to exclude agreement gained under duress, is not necessary. • The term 'authorise' is used in a variety of ways in the Act and starting to add exclusions will not adequately capture all the ways it is used.
22	Section 27(1)(d) should be amended so that an agency may refuse access if disclosure of the information would be likely to present a serious threat to public health or public safety, or to the life or health of any individual.	**Agree**	• Current provisions only relate to the physical safety of an individual. Widening this to refer to all types of 'health' would encompass mental as well as physical safety, align with principles 10 and 11, and be consistent with Australia's privacy principles. • The extent of individual protection would be broadened.
23	A new provision should be added to section 29, allowing agencies to refuse access where disclosure of the information would create a significant likelihood of serious harassment of an individual.	**Reject**	• Additional regulations will be unnecessary once recommendation 22 above is implemented, as harassment will be covered.
25	A new provision should be added to section 29 allowing agencies to refuse access where disclosure of the information requested would disclose information about another individual who is a victim.	**Agree**	• This amendment would enhance the protection of individuals and ensure that information requested only applies to the requester. • Would contribute to public confidence that their information will be used and disclosed appropriately. • Would contribute to the Government goal of providing more support to victims and help reduce re-victimisation.

No	Recommendation	Government recommendation	Discussion and impacts
27	A new provision should be added to section 29, allowing agencies to refuse access if the same information, or substantially the same information, has previously been provided to the requestor. 'Vexatious' grounds are already covered.	**Reject**	• Instead, propose additional guidance and education from the Privacy Commissioner and the Office of the Ombudsmen as an alternative to regulation. • Would contribute to good business practices and relationships.
28	Section 35(3)(b)(i), which provides that a private sector agency may charge for correction of personal information, should be deleted.	**Agree**	• Agencies are obliged to ensure that information is accurate before it is used. If private agencies agree to correct information, however, they can charge for it. • The cost of ensuring accuracy should fall where the obligation rests, which would contribute to good business practices and relationships. Individuals would be more likely to volunteer up-to-date information. • Would increase compliance costs. Difficult to cost, as the potential for increased volumes of requests is not known, and data on the revenue gathered by agencies for this purpose is not gathered.
29	Complexity of the issues raised by a personal information request should be added to the grounds in section 41(1) on which an agency may extend the time limit for responding to a request.	**Agree**	• Not having enough time to carry out due process, including checks and balances, can be a contributing factor in privacy breaches. • This proposal would enhance public confidence that their information will be used and disclosed appropriately after due deliberation. The number of breaches and harm to individuals may decrease.
33	An exception for the use of unique identifiers for statistical and research purposes should be added to principle 12(2).	**Agree**	• This would contribute to good business practices and enable, through the gathering of statistics, Government monitoring of the impacts of privacy law.
35	Principle 1 should be amended to allow individuals to interact with agencies anonymously or under a pseudonym, where it is lawful and practicable to do in the circumstances. *Principle 1 relates to the purpose of collection of information.*	**Agree**	• Potentially encourages individuals to provide information that they otherwise would not.

No	Recommendation	Government recommendation	Discussion and impacts
36	The Act should apply to the Parliamentary Service, but only in respect of its departmental holdings. Information held by the Parliamentary Service on behalf of Members of Parliament should not be covered by the Act.	**Defer**	• Consultation with the House of the Clerk and Parliamentary Services concluded that this recommendation should not proceed in isolation from a wider consideration about how privacy information issues should be dealt with in respect of the House of Representatives and members of Parliament. • It is proposed to defer making a decision on this recommendation while further consultation is undertaken with the Office of the Clerk and Parliamentary Services, which may include consideration of non-regulatory options.
37	The Ombudsmen should be deleted from the list of entities that are excluded from the definition of "agency".	**Modify**	• All organisations should be subject to the Act unless there is a good reason to the contrary. • The Act does not currently apply to the Ombudsmen, but the Ombudsmen Act already contains sufficient protections with respect to the handling of personal information. • The Ombudsmen are the last line check on the exercise of executive power and should not be subject to investigation by an agency such as the Commissioner that is itself subject to the Ombudsmen's jurisdictions. • The proposal is, instead, to amend the Ombudsmen Act so that information on how they deal with personal information must be included in their annual report. • This approach would ensure improvements in public confidence that their information will be used and disclosed appropriately.
40.1	Section 54 should be amended to allow the Commissioner to grant exemptions from principle 9. *Principle 9 requires agencies not to keep information for longer than necessary.*	**Agree**	• The introduction of this approach would allow flexibility for one-off circumstances. • This type of proportionality would help to reduce compliance costs for agencies and engender good business practices.
40.2	Section 54 should be amended to allow the Privacy Commissioner to grant exemptions from principle 12. *Principle 12 relates to unique identifiers.*	**Reject**	• It is difficult to see how the allocation and use of unique identifiers could be a one-off occurrence. In light of a lack of problem definition, the exemption to principle 12 does not appear necessary.

No	Recommendation	Government recommendation	Discussion and impacts
41	Section 54 should be amended to require the Privacy Commissioner to report annually on exemptions applied for and granted under section 54, and to maintain on the Commissioner's website a list of all current exemptions.	**Agree**	• Section 54 allows the Commissioner to authorise the collection, use or disclosure of personal information that would otherwise be in breach of some of the principles. One-off exemptions should be transparent. Although not required by statue, the OPC does already report on exemptions in their annual report.
42	Section 55 should be amended to provide that principles 6 and 7 do not apply in respect of personal information held by or on behalf of the Auditor-General, and in connection with the Auditor-General's statutory functions. The principles would continue to apply with respect to information about staff.	**Agree**	• The work of the Auditor-General involves gathering information about risk and behaviour which can be personal and sensitive. Confidentiality is important to gain full disclosure. • Would provide consistency with information provided to, inter alia, commissions of inquiry and the Ombudsmen. Would contribute to public confidence that their information will be used and disclosed appropriately.
43	Section 56 should be amended to state expressly that the exemption applies to all of principles 1 to 11. *Section 56 exempts personal information relating to domestic affairs from the privacy principles.*	**Agree**	• The rationale is that individuals should not have to comply with the Act in relation to everyday domestic activities such as taking photos of friends or keeping records of family expenditure. This amendment would recognise the special nature of domestic relationships. • The wording of section 56 only refers to personal information that is collected or held. It is not clear whether it applies to disclosures. Being explicit that it applies to all of the principles would make this clear. Would improve clarity about the scope of the section.
44	Section 56 (above) should be amended to provide that it applies to information collected or held "solely" (rather than "solely or principally") in connection with household affairs.	**Agree**	• This would close an existing loophole.
45.1 and 45.2	Section 56 should be amended to provide that it does not apply to misleading or unlawful conduct. *Section 56 provides an exemption from the requirements of the Act for information collected and held for domestic affairs.*	**Agree**	• The proposed amendment would mean that an exemption with respect to personal information would not apply if it had been obtained unlawfully or through misleading conduct. • Would be useful in providing a civil remedy for intimate covert filming and for some matters involving the use of the internet. • Would contribute to public confidence that their personal information will be used and disclosed appropriately.

No	Recommendation	Government recommendation	Discussion and impacts
52	Codes of practice should continue to be developed by the Commissioner, but should require approval by the Governor-General in Council.	**Defer**	• Defer to a future review. The status quo is working well, and already includes constitutional safeguards such as referral to the Regulations Review Committee for examination.
53	The Governor-General in Council should be able to reject a proposed code, but not to amend it.	**Defer**	• Defer as above.
60	The Act should specifically provide that representative complaints are permitted.	**Agree**	• The Act currently contemplates representative complaints but is not clear that they are allowed. This proposal would provide the clarity needed to allow representative complaints. • Would help to increase efficiency by encouraging 'pooling' of multiple complaints.
61	The chairperson of the Human Rights Review Tribunal should be a judge at the level of a District Court Judge.	**Reject**	• Appointing either a sitting or retired District Court Judge would impose significant costs with little evidence of a problem or of benefits. There is no evidence that previous Chairs have been subject to political interference or lacked the skills to fulfil the required functions. • The number of District Court Judges is capped at 156. Appointing a sitting District Court Judge would mean removing a Judge from a District Court.
62	The Human Rights Review Tribunal should not be empowered to order exemplary damages	**Agree**	• Exemplary damages are anomalous and should not be legislated for without good reason. No evidence of a problem. No policy reason to change current legislative prohibition.
66.1	There should be a new offence of intentionally misleading an agency.	**Agree**	• The proposed offence is not currently covered by the Crimes Act or the Privacy Act. • Would contribute to public confidence that their information will be held and used appropriately.

No	Recommendation	Government recommendation	Discussion and impacts
66.2	There should be a new offence of knowingly destroying documents.	**Agree**	• The proposed offence is not currently covered by the Crimes Act or the Privacy Act. • Would contribute to good business practices and relationships with people and support agencies to handle personal information effectively through its lifecycle. Would contribute to public confidence that their information will be held and used appropriately.
87	The Public Records Act 2005 should require the Chief Archivist to consult the Commissioner when preparing standards about access to archived records.	**Reject**	• The proposed consultation already happens as a matter of good practice, and so a problem does not exist. Additional regulation is not required and would not accord with the Government's principle of less regulation being better regulation.
89	Section 16 of the Criminal Disclosure Act 2008 should contain a provision that, in deciding whether information is relevant for the purpose of section 13(2) of that Act, consideration must be given to the extent to which it relates to the private affairs of another individual. This would then mirror the withholding grounds in the Privacy Act under section 29(1)(a).	**Reject**	• This is already covered by sections 13 and 16(1)(k) of the Criminal Disclosure Act 2008. Section 16(1)(k) allows withholding of information where disclosure of the information would be contrary to the provision of another Act. Section 13 provides for only 'relevant' information be able to be disclosed. • Additional regulation is not considered to be required.
97	A new exception to principle 11 should be created that would expressly permit an agency to report any reasonably held suspicion or belief that an offence has been or may be committed. *Principle 11 relates to limits on use of information.*	**Agree**	• Would assist law and order, and assist Government in delivering good social outcomes.
117	Principle 12 should be amended to encourage measures to control the public display of unique identifiers, as a response to the problem of identity crime. *Principle 12 relates to the use of unique identifiers.*	**Agree**	• This would contribute to public confidence that their information will be used and disclosed appropriately.
119	Section 14 should be amended to provide that, in exercising his or her functions, the Privacy Commissioner must take account of Māori needs and cultural perspectives, and of the cultural diversity of New Zealand society.	**Agree**	• While a desire for privacy appears to be universal among human beings, the ways in which privacy is understood can vary between cultures (e.g. individual vs collective interests). • Would contribute to good business practices and relationships with people from Māori and other cultures, and help to develop trust that information is used in ways that would not disempower or diminish mana.

No	Recommendation	Government recommendation	Discussion and impacts
120.1	Principle 4 should be amended to provide that, in considering whether the collection of personal information is unfair or unreasonably intrusive, the age of the individual concerned must be taken into account. *Principle 4 relates to the manner of collection of personal information.*	**Agree**	• Would demonstrate sensitivity to vulnerability, and contribute to public confidence.
122	Section 14(b) should be amended to refer to New Zealand's international obligations concerning the rights and best interests of the child.	**Reject**	• The obligations are already taken into account. UNCROC is considered in developing New Zealand legislation and there is no need to specifically refer to obligations under UNCROC in legislation • Other legislation referring to the 'best interests of the child' includes the Care of Children Act 2004 which elevates the best interests of the child to the first and paramount consideration; the Corrections Act 2004 relating to placement of children with prisoner mothers; and interim orders in respect of children under the Domestic Violence Act 1995. • Additional regulation is not required.
126	Section 23 should be amended to allow agencies to appoint a privacy officer from outside the agency.	**Agree**	• Would help to reduce the compliance costs of small businesses if they can share a privacy officer with other small businesses, or buy in specialist advice when needed to supplement day-to-day in-house privacy staff.
			•
MOJ rec	Duty on agencies and individuals to take reasonable steps to resolve their disputes.	**Agree**	• This approach would allow government to work efficiently to deliver good social outcomes. More complaints could be settled in a non-litigious, efficient and effective way.
7 Stage 2 report	Recommendation 7 from Stage 2 of the privacy review relating to Public Registers. Provision should be made in the Act for applications for name and/or address suppression to the Privacy Commissioner, and that each public register statute should refer to the availability of such applications.	**Defer**	• Deferring this recommendation would enable public register recommendations to be considered as a whole package.

Conclusions and recommendations

45 These proposals are seen to be positive for business and the public sector by giving the public the confidence to provide information to them. In the public sector, ensuring privacy concerns are addressed upfront is critical to achieving the Government's expectations for a more efficient, effective and joined up service delivery through Better Public Services. For the private sector, they are seen as being in line with developing international expectations for doing business worldwide.

46 The package of privacy measures being proposed aims to ensure that the set of incentives for agencies to develop better privacy governance systems is strengthened and that people can feel confident that their personal information is protected. Some of the most far-reaching Law Commission recommendations have been modified in order to develop responses that are proportionate to the extent of potential harm to individuals. Where possible, incentives and guidance are proposed rather than sanctions, to avoid overregulation, although the potential for sanctions can also act as an incentive to change behaviours.

47 Any change in policy and legislation significant enough to change behaviours and outcomes will also be accompanied by costs. The privacy reforms are no exception.

48 Even though the majority of Law Commission recommendations about privacy reform are either exempt from this RIS or are of a less substantial nature, there are a handful of proposals that will result in compliance costs to agencies (public and private). Where additional costs to agencies are most likely to be experienced relates to being required to notify all individuals when a serious breach has occurred, as well as ensuring that privacy rules and systems are adhered to if a compliance notice is issued. The costs potentially associated with these changes are hard to quantify as every situation is unique.

49 On the whole, the risk of overregulation with an accompanying increase in the compliance burden on agencies has been avoided in the proposed privacy reforms.

50 It has not been possible to estimate the possible compliance costs to agencies of the privacy proposals, because OPC does not currently have access to information about system-wide privacy limitations, particularly of private sector agencies.

51 However, it is possible to say that the law already effectively requires agencies to operate privacy systems so as to minimise the chance of harm being done to individuals. The key proposals in this paper – namely mandatory breach notification, enhanced own motion investigations and compliance notices – only involve marginal costs in relation to these existing obligations:

- 51.1 mandatory breach notification – marginal costs of reporting breaches to OPC and affected individuals;
- 51.2 own motion inquiries – costs will be particularly low across agencies as only a few agencies in any given year are likely to be subject to an own motion inquiry, given the funding restraints on OPC.
- 51.3 compliance notices – marginal costs to agencies as compliance notices will be a 'last stop' regulatory tool.

52 In addition, to limit costs to agencies as far as possible the proposals rely less on monitoring and penalties, and more on early intervention by OPC, powers that will enable OPC to identify system-wide problems, and the infrastructure to provide guidance and education. A significant new role for OPC will be involvement in the development of:

- 52.1 information-sharing agreements

52.2 mechanisms for achieving Better Public Service targets that are consistent with privacy imperatives

52.3 systems that are set up to continuously review and refresh security management within a wider risk framework, as recommended by Cabinet in May 2013 in response to the Government Chief Information Officer's "Review of Publicly Accessible Systems".

53 While examples of support are more obvious for public sector agencies, the same principles will apply to private companies seeking guidance and assistance. Facilitation, support, and 'before-the-fact' assistance is far less burdensome on agencies than compliance with a set of rigid rules that are subsequently monitored and penalties imposed where compliance is not found.

Meeting objectives

54 The package of proposed reforms (including mandatory reporting of privacy breaches in a two-tier arrangement, enhanced own motion investigations, the ability to issue compliance notices, and cross-border protections of personal information) will significantly improve the capacity of the regulator to detect emerging and systemic issues at an early point and to either prevent or resolve these as soon as possible.

55 Early detection and the avoidance of future more serious breaches will both contribute to the minimisation of harm and build consumer trust in how their personal details are used by Government agencies, businesses, and across jurisdictions.

56 While the proposed package will provide the Commissioner with the tools needed to address privacy risks, there will be safeguards around their use to minimise the compliance costs to agencies. The primary role of the Commissioner will remain the facilitation of compliance and to work with agencies to improve privacy.

57 The proposed package is in line with developing international expectations for doing business worldwide with one exception; other jurisdictions rely on the imposition of heavy fines to ensure compliance. For example, in Australia agencies face a fine of up to A$1.7 million for repeat and serious privacy breaches. The New Zealand package of reforms is more moderate. Because we are proposing a package of reforms that balances increased prescription with increased support, New Zealand should not consider imposing fines for privacy breaches at this time. Unlike Australia and some other jurisdictions, New Zealand tends to a legal framework that is less-regulated, imposing fewer costs on businesses if at all possible. The need for and usefulness of fines could be considered, if need be, once the impacts of the privacy reforms have been determined. If it becomes clear that guidance and early intervention is not effective, the use of sanctions may be appropriate. The final section in this RIS covers monitoring, evaluation and review.

Financial impacts for the Office of the Privacy Commissioner

58 The additional demand that OPC is currently facing as well as the additional functions we are asking it to do now and in the future call for a much better resourced Office than is currently the case. OPC is a modest organisation that has managed to absorb a lot of additional demand without any additional resources over the past seven years.

59 Institutions of government such as OPC are tasked with roles in strengthening the state sector, improving system performance and contributing to economic performance. The Commissioner's ability to fulfil her current role in these critical areas is limited due to increased demand for privacy services. A sustainable base level of funding for the OPC is required.

60 OPC currently receives $3.2 million in Crown funding every year – this has not changed since 2007. Over the last four years, demand for OPC services has

significantly increased. Examples include complaints increasing by 36%; public enquiries by 54%, media enquiries by 29%, and privacy breach notifications rose from 3 to 107.

61 To provide for the OPC to contribute and operate effectively it is recommended that OPC receives increased baseline funding of

62 There are three broad options for meeting these costs. Funding from justice sector baselines, funding from a levy system or cost recovery, or additional funding from the centre. The preferred option is additional funding from the centre.

64 Although OPC is funded through Vote Justice, only part of its functions are connected with broader justice outcomes – in this respect it is not dissimilar to other Crown Entities that are also funded through Vote Justice, such as the Electoral Commission and the Real Estate Agents Authority.

65 The work of the Commissioner benefits the entire economy, and a strong and independent Commissioner assists in the Government's broader goal of improving and modernising the state sector through safe and efficient exchange of data. These are public goods that should be rightly funded by all of Government.

67 The possibility of public and/or state sector contributions via either a levy system or cost recovery has been considered. Both mechanisms have significant disadvantages.

68 A levy would be impracticable because:

68.1 the cost of administering a levy would be disproportionate to the amount of revenue to be collected and impose compliance costs on business, whether administered independently or in combination with other levies

68.2 combining a privacy levy with an existing levy system risks compromising the effectiveness of existing levies by confusing businesses about what they are paying for, increasing non-payment and/or reducing the information provided by businesses to agencies to avoid payment. The levy would also not target all of those who benefit from robust privacy settings.

69 In terms of cost recovery, OPC services are too variable to enable fixed charges, and recovery of costs incurred would limit incentives for cost efficiencies.

Benefits of additional funding

70 Overseas studies[2] indicate that each privacy breach can cost an agency (in both tangible and intangible costs) at least US $200 (NZ $243) per individual affected, on

---

2 Romanosky, Hoffman, and Acquisti. (2012). *Empirical Analysis of Data Breach Litigation.* Eleventh Annual Workshop on the Economics of Information Security WEIS 2012

Ponemon Institute. (March 2011). *2010 Annual Study: US Cost of a Data Breach: Compliance Pressures, Cyber Attacks Targeting Sensitive Data Drive Leading IT Organizations to Respond Quickly and Pay More*

Acquisti, Freidman and Telang. (2006). *Is There a Cost to Privacy Breaches? An Event Study.* Twenty-seventh International Conference on Information Systems, Milwaukee 2006 and Workshop on the Economics of Information Security 2006

average. If this assumed average cost can be applied in the New Zealand context, investment of $3.000 million per annum would only need to prevent three public sector breaches affecting 4,000 or so people each, each year, for the investment to have been cost neutral to Government. In the context of the number and scale of public sector breaches over the past year or so and the nature of the privacy reforms, this achievement is expected to be exceeded. Over the last four years, for example, New Zealand has experienced:

70.1 a 36% increase in complaints to OPC

70.2 a rise in breach notifications to OPC from three to 107

70.3 many of these breaches have potentially involved thousands of clients – the Ministry of Social Development's insecure kiosks alone meant that 529,000 clients were vulnerable (2012 Statistical report)

70.4 in February 2013, a Parliamentary Select Committee was advised that ACC (with a database of 80 million client records) had experienced an average of 75 privacy breaches per month in the last quarter. The "Pullar" breach in March 2012 involved 6,700 client records.

71 The proposals for reform are considered to be good for business as well as the public sector by giving the public the confidence to provide information to them.

72 The table below demonstrates the intervention logic for the proposed investment:

Objective	• Reduced harm to individuals • Fewer remedial costs to agencies; more trust in agencies on the part of individuals • International trade supported through compliance with international privacy standards, with resulting economic growth benefits • More efficient public service at less cost
Longer-tem outcomes	• Reduced risk of costly and embarrassing public (and private) sector breaches • Contribution towards the BPS target of *an average of 70 per cent of New Zealanders' most common transactions with government being completed in a digital environment by 2017* – as more people trust in and have confidence that the public sector will protect their personal information • Improved capacity of OPC to support: the achievement of all BPS targets; next steps from the GCIO review; the development of transnational agreements
Immediate outcomes	• Creation of an enduring set of incentives to take privacy seriously • Reinforcement of other disciplines such as public sector risk management and governance tools • Improved agency ability to protect personal information appropriately
Outputs	• OPC's functions and powers bolstered
Financial inputs	• 100% increase in OPC's baseline, plus transitional costs

Consultation

11 The following consultation has been undertaken:

Agency conducting consultation	Who was consulted	Key points arising from consultation
Law Commission	• Public • private sector organisations, • non-government organisations • Government agencies. • The Commissioner's review of the Act ('Necessary and Desirable') inputs to the Law Commission's review. The review received 76 submissions from public agencies, private sector agencies, and individuals	• individuals were supportive of more regulation and better protection • businesses supported appropriate thresholds before intervention occurs, to ensure proportionality and to discourage vexatious complaints • mandatory breach notifications were not supported by private sector agencies such as banks and credit card companies - they considered that the firms should make a decision about the level of harm to individuals and whether or not to address a breach, and were concerned about 'inappropriate' responses from individuals if they were alerted to a breach • public sector organisations suggested that further OPC guidance about privacy arrangements in the environment of technology would be helpful • other public sector agencies with large client bases: - were frustrated by receiving a large number of information requests; - and disagreed with mandatory breach notifications - most breaches were of a minor nature and there was no need to inform individuals.
Response The key messages from the Law Commission's consultation have been taken into account in the proposals that either agree or modify the Law Commission's recommendations. The use of thresholds in the case of mandatory breach notifications, own-motion investigations and compliance notices, for example, aim for proportionality of responses appropriate to the level of harm, while ensuring that individuals can be better protected.		
MOJ	• Government agencies	• interested in ensuring alignment as far as possible between New Zealand's privacy settings and those of key international jurisdictions • supportive of mandatory data breach notification, but were: - concerned that notifications to individuals in cases of serious breaches could further weaken vulnerable people (particularly those with mental health disabilities) - supportive of an amendment to introduce an element of reasonableness for agencies notifying of breaches - interested in the drafting of the thresholds for notification. • Supportive of enhanced own motion investigations, but were concerned about proposed power of entry.

		• were concerned that the introduction of a new privacy principle regarding the disclosure of personal information overseas will cut across existing information sharing arrangements.
	• Targeted representative private sector agencies	• identified the usefulness of OPC continuing its educative and conciliation role as a first option prior to escalation • some concerns that privacy law should focus more on the public sector than the private sector and about compliance costs for business • were concerned that an OPC audit function may result in hunts for breaches. Thresholds for initiating an audit or inquiry and who would pay were of interest. • sought advice on the definitions of 'material' and 'serious' data breaches for the purposes of notification, and information about the thresholds for the issue of compliance notices • some concerns about proposals regarding the disclosure of personal information overseas.
Response • These proposals are consistent with international trends. • The mandatory breach notification proposal has been amended so that agencies must take reasonable steps to notify of data breaches and to include an additional exception relating to the vulnerability of people affected. • An additional exception was added to the cross border disclosure principle, so that individuals can consent to their information being sent overseas. • The Commissioner will have the ability to publish a list of overseas frameworks that constitute acceptable privacy standards. The Act will provide guidance on the types of steps that could be taken and on what constitutes acceptable privacy standards. • The proposed power of entry for OPC was removed • OPC's educative and conciliation role is supported through new functions and additional funding. Guidance will include definitions of 'material' and 'serious' data breaches, and of the thresholds for initiating an own-motion investigation. • Do not agree that enhanced privacy settings should focus more on the public sector. In the modern technological environment, the private sector is susceptible to data breaches and it is necessary for privacy law to focus on the private sector if business is to be able to trade internationally in markets where privacy standards are expected.		
MOJ	Privacy Commissioner	• Strongly supports the proposals to implement the majority of the Law Commission's package of reforms • A few points of difference with MOJ proposals: - Agree with the Law Commission that OPC should have an audit power; - Agree with the Law Commission that the role of the Director should be removed in privacy proceedings; - Agencies that fail to comply with mandatory data breach rules should face a civil fine rather than a criminal offence.

Implementation

73 OPC will lead the implementation of the operational proposals contained in the package of privacy reforms; working closely with the Ministry of Justice and other relevant parties to ensure that the policy intent is appropriately implemented.

74 It is intended that the development of guidance and educational material will be led by OPC, in consultation with the Ministry of Justice, while the new Privacy Act moves through the House. It will be ready for publication once the new Act commences. Funding for the new functions and powers of the OPC including the development and publication of guidance and educational material is being sought.

75 Implementation risks will be mitigated by:

- 75.1 policy involvement in the development of guidance material and OPC's new functions and powers, once approved
- 75.2 adequate funding of the new powers and functions
- 75.3 safeguards around the use of new tools to minimise their compliance costs to agencies and to recognise natural justice.

76 Compliance costs are being minimised through the policy design of the proposals. Some of the more significant Law Commission recommendations, for example, have been modified to incorporate proportionality and thresholds of harm.

77 The proposals contained in the package of privacy reforms will be incorporated into the drafting of a new Act. Outdated provisions will be retired, and definitions, principles and purpose statements will be enhanced.

78 OPC will enforce the new laws from the date they are introduced. The passage of the new laws through the House will provide agencies with the time needed to prepare for new procedures.

Monitoring, evaluation and review

79 Section 26 of the Act requires the Commissioner to review the operation of the Act every five years. The Law Commission has recommended (recommendation 49) that this provision remain, but the Government proposes rejecting that recommendation and repealing that section of the Act.

80 Government has introduced a regulatory scanning programme, overseen by Treasury. This involves the systematic evaluation of an agency's legislation and regulations. There is an annual reporting cycle for regulatory scanning.

81 The Ministry of Justice scans groups of legislation for which it is responsible as part of a "rolling programme", with the aim that all regulation is scanned at regular intervals. The Act will be part of this programme. The Ministry will consult relevant stakeholders including the Commissioner.

82 The Act operates in a highly changeable environment with technology and international developments suggesting that the Act may need to be reviewed more frequently than every five years.

83 Section 24 of the Act requires the Commissioner to report on the operation of the Act. Once the proposed initiatives are in force, OPC will be able to gather and report on data with respect to:

- 83.1 the number and size of breaches, by type of breach (serious, material)
- 83.2 the number of compliance notices, by type of notice, and outcomes
- 83.3 the number of own motion investigations, by type of issue detected, and outcomes.

Appendix Two

Law Commission and Privacy Commissioner Recommendations – Status in the RIS

Status Key:

1 = the Government agreed in the interim response
2 = the Government responded to 12 Law Commission recommendations when it introduced Privacy (Info Sharing) Bill
3 = implemented through the Criminal Procedure Act 2011
4 = guidance, referred to either OPC or LAC or the Ombudsmen, as appropriate
5 = included in supplementary response
6 = responded to in another workstream
7 = deferred in interim response
8 = rejected in interim response - either no further work or not a recommendation for Government
9 = Privacy Commissioner's recommendations overtaken by Law Commission recommendations
10 = Privacy Commissioner's recommendations withdrawn by the Privacy Commissioner
11 = implemented through another Act

Recommendations from the Privacy review

Rec no.	Recommendations (from Privacy Act Review)	Status	Included in RIS?
1	A new Privacy Act should be enacted, which will also incorporate changes recommended by the Privacy Commissioner in *Necessary and Desirable*	1	N/A
2	The Privacy Act should continue to take an open-textured, principles-based approach to regulating information privacy	1	N/A
3	The Privacy Act should have a purpose section	5	Yes
4	OPC should develop guidance on the definition of "personal information"	4 But costings in Cab paper	N/A
5	The Privacy Act should provide that codes of practice may apply to any of the privacy principles to information about deceased persons	5	Exempt
6	Causes of action under the Privacy Act should survive the complainant's death	5	Yes
7	The definition of "collect" should be amended to exclude the situation where an agency has taken no active steps to acquire the information	5	Exempt
8	The definition of "publicly available publication" should be clarified to, inter alia, make it clear that it includes websites	5	Exempt

		costings in Cab paper	
10	The scope of "publicly available publication" exemptions to principles 10 and 11 should be narrowed	6	N/A
11	The word "directly" should be deleted from principles 2(1) and 3(1). *[Principles 2 & 3 refer to the collection of information directly from the individual concerned]*	5	Exempt
12	Principle 2(2) should be amended by adding a new exception covering situations in which an agency believes, on reasonable grounds, that non-compliance is necessary to prevent or lessen a serious threat to the health or safety of any individual. *Principle 2 refers to the collection of information directly from the individual concerned*	5	Yes
13.1	Principle 3(4)(a) should be deleted. *Principle 3 relates to collecting information from the individual concerned. Principle 3 (4)(a) is an exception where non-compliance is authorised by the individual*	5	Exempt
13.2	Principle 3(4)(f)(ii) should be deleted. *Principle 3 relates to collecting information from the individual concerned. Principle 3(4)(f)(ii) is an exception where the information will be used for statistical or research purposes*	5	Exempt
14	Principle 4 should be amended to make it clear that it applies to attempts to collect information. *Principle 4 relates to the collection of information by unlawful, unfair or unreasonable means*	5	Exempt
15	OPC to develop guidance relating to employees browsing information	4 But costings in Cab paper	N/A
16	Principle 8 should be amended to make it clear that it applies to attempts to collect information *Principle 8 provides that the accuracy of information is to be checked before use*	5	Exempt
17	Section 45 should be amended to provide that an agency shall not give access to information requested under principle 6(1)(b) if the agency has reasonable grounds for believing that the individual concerned is making the request under duress	5	Yes

18	Section 66(2) should be amended to provide clearly that failure by an agency to comply with the requirements of section 45 is an interference with privacy.	5	Yes
19	"Authorise" should be defined in section 2 as excluding situations in which an individual's agreement is obtained under duress	5	Yes
20	Where an agency is not willing to correct personal information, the agency should be required to inform the requester of his or her right to request that a statement be attached to the information of the correction sought but not made.	5	Exempt
21	Sections 27 – 29 should be amended to incorporate the agency "belief on reasonable grounds' threshold, for consistency with principles 10 and 11.	5	Exempt
22	Section 27(1)(d) should be amended so that an agency may refuse access if disclosure of the information would be likely to present a serious threat to public health or public safety, or to the life or health of any individual.	5	Yes
23	A new provision should be added to section 29, allowing agencies to refuse access where disclosure of the information would create a significant likelihood of serious harassment of an individual.	5	Yes
24	OPC, in consultation with the Ombudsmen, should develop guidance on access requests involving mixed information	4 But costings in Cab paper	N/A
25	A new provision should be added to section 29 allowing agencies to refuse access where disclosure of the information requested would disclose information about another individual who is a victim	5	Yes
26	Section 29 should be amended to enable relevant health practitioners to assess an individual's mental state.	5	Exempt
27	A new provision should be added to section 29, allowing agencies to refuse access if the same information, or substantially the same information, has previously been provided to the requestor	5	Yes
28	Section 35(3)(b)(i), which provides that a private sector agency may charge for correction of personal information, should be deleted.	5	Yes
29	Complexity of the issues raised by a personal information request should be added to the grounds in section 41(1) on which an agency may extend the time limit for responding to a request.	5	Yes
30	The words "and imminent" should be deleted from principles 10(d) and 11(f)	2	N/A
31	Act should set out criteria for assessing seriousness for the purposes of the existing health and safety exceptions	2	N/A
32	Principle 12(2) should be redrafted so that the meaning of "assign" is clearer. *Principle 12 relates to the use of unique identifiers*	5	Exempt
33	An exception for the use of unique identifiers for statistical and research purposes should be added to principle 12(2). *Principle 12 relates to the use of unique identifiers*	5	Yes
34	OPC should develop guidance on compliance with principle 12(4)	4	N/A

35	Principle 1 should be amended by adding a new sub-clause providing that individuals should be able to interact with agencies anonymously or under a pseudonym, where it is lawful and practicable to do so in the circumstances. *Principle 1 provides that agencies should only collect information where it is necessary for a lawful purpose connected with the function of the agency*	5	Yes
36	The Privacy Act should apply to the Parliamentary Service, but only in respect of its departmental holdings. Information held by the Parliamentary Service on behalf of Members of Parliament should not be covered by the Privacy Act.	5	Yes
37	The Ombudsmen should be deleted from the list of entities excluded from the definition of "agency".	5	Yes
38	The definition of "news medium" should be amended	6	N/A
39	Reference to Radio New Zealand and Television New Zealand should be removed	6	N/A
40.1	Section 54 should be amended to allow the Privacy Commissioner to grant exemptions from principle 9. *Principle 9 requires agencies not to keep information for longer than necessary, principle 12 relates to unique identifiers*	5	Yes
40.2	Section 54 should be amended to allow the Privacy Commissioner to grant exemptions from principle 12. *Principle 9 requires agencies not to keep information for longer than necessary, principle 12 relates to unique identifiers*	5	Yes
41	Section 54 should be amended to require the Privacy Commissioner to report annually on exemptions applied for and granted under section 54, and to maintain on the Commissioner's website a list of all current exemptions.	5	Yes
42	Section 55 should be amended to provide that principles 6 and 7 do not apply in respect of personal information held by or on behalf of the Auditor-General, and in connection with the Auditor-General's statutory functions.	5	Yes
43	Section 56 should be amended to state expressly that the exemption applies to all of principles 1 to 11. *Section 56 exempts personal information relating to domestic affairs from the privacy principles*	5	Yes
44	Section 56 should be amended to provide that it applies to information collected or held "solely" (rather than "solely or principally") in connection with household affairs.	5	Yes
45.1 and 45.2	Section 56 should be amended to provide that it does not apply to misleading or unlawful conduct. *Section 56 exempts personal information relating to domestic affairs from the privacy principles*	5	Yes
45.3	Section 56 should be amended to provide that it does not apply where the collection, use or disclosure of personal information would be highly offensive to an objective person	6	N/A
46	Section 57 should be amended to provide that principles 1,5,8 and 9 apply to the intelligence organisations	6	N/A
47	Section 13 should be amended to make it clear that it is not a complete list of the Privacy Commissioner's functions.	5	Exempt
48	Section 13(1)(d) and section 21 should be repealed. *These sections give the Privacy Commissioner discretion to publish directories of personal information*	5	Exempt

49	The Privacy Act should contain a provision that it is to be reviewed every five years.	5	Exempt
50	The Government should be required to table in Parliament within six months a response to each review of the Act.	5	Exempt
51	The list of the Privacy Commissioner's functions in the present section 13 should be abridged and consolidated	5	Exempt
52	Codes of practice should continue to be developed by the Privacy Commissioner, but should require approval by the Governor-General in Council.	5	Yes
53	The Governor-General in Council should be able to reject a proposed code, but not to amend it.	5	Yes
54	The harm threshold in section 66 should remain in relation to complaints *Section 66 sets the criteria for an interference with privacy, which forms the basis for a complaint.*	5	Exempt
55	The role of the Director of Human Rights Proceedings should be absorbed into the OPC	5	Yes
56	The Privacy Commissioner should determine access complaints	5	Yes
57	Compliance with a notice to release information should be enforced by order of the Tribunal	5	Yes
58	A determination under principle 6 should be appealable to the Tribunal	5	Yes
59	A claim for damages should be filed separately with the Tribunal	5	Yes
60	The Privacy Act should specifically provide that representative complaints are permitted.	5	Yes
61	The chairperson of the Human Rights Review Tribunal should be a judge at the level of a District Court Judge.	5	Yes
62	The Human Rights Review Tribunal should not be empowered to order exemplary damages	5	Yes
63	Privacy Commissioner should have the power to issue compliance notices	5	Yes
64	Privacy Commissioner should have the power to require audits	5	Yes
65	Privacy Commissioner should issue a protocol for process to be followed for conducting an audit	5	Yes
66.1	There should be a new offence of knowingly destroying documents	5	Yes
66.2	There should be a new offence of intentionally misleading an agency	5	Yes
67	Data breach notification should be mandatory	5	Yes
68	Sets out the criteria for notification	5	Yes
69	Sets out what should be taken into account when determining whether a breach is serious	5	Yes
70	Responsibility to notify should lie on the agency which held the information	5	Yes
71	Individuals whose information has been compromised and the OPC should be notified	5	Yes
72	Act should provide that OPC will not publish the identities of the agencies that notify breaches	5	Yes

73	Notification should be made as soon as practicable	5	Yes
74	The notice should fully and fairly inform the individual	5	Yes
75	Notification should be to the individual	5	Yes
76	There should be a public interest exception	5	Yes
77	Failure to notify should be a ground of complaint to the Privacy Commissioner	5	Yes
78	The obligation to notify should be enacted as part of principle 5	5	Yes
79	If a data breach notification becomes compulsory, OPC should issue guidance	5	Yes
80	Section 7 should be repealed and replaced by a new provision to clarify the relationship between the Act and other enactments.	5	Exempt
81	Section 7(5) should be moved to Part 6 of the Act *Section 7(5) provides that principle 7 (correction of personal information) does not apply to the Department of Statistics where the information was obtained under Statistics Act 1975. Part 6 is titled "Codes of practice and exemptions from information privacy principles"*	5	Exempt
82	Section 7(6) should be moved to Part 7 of the Act, should such a provision remain necessary *Section 7(6) provides that nothing in the privacy principles should apply to public registers, subject to Part 7. Part 7 sets out provisions specifically for public registers, including separate public register privacy principles*	5	Exempt
83	LAC guidelines should contain a guideline that new legislation should specify the relationship with the Act	4	N/A
84	LAC should re-examine its guidelines on relationships between Acts	4	N/A
85	OPC and the Ministry of Justice should consider issuing a list of frequently-arising statutory overrides of the Act	4 But costings in Cab paper	N/A
86	An exception should be added to principle 11 making it clear that when requests for personal information are made to agencies subject to the Official Information Act 1982 or the Local Government Information and Meetings Act 1987, the latter Acts govern such requests	5	Exempt
87	The Public Records Act 2005 should require the Chief Archivist to consult the Privacy Commissioner when preparing standards about access to archived records.	5	Yes
88	A subsection should be added to section 18 of the Public Records Act expressly providing that that section prevails over principle 9 of the Privacy Act.	5	Yes
89	Section 16 of the Criminal Disclosure Act 2008 should contain a provision that, in deciding whether information is relevant for the purpose of section 13(2) of that Act, consideration must be given to the extent to which it relates to the private affairs of another individual.	5	Exempt

90	The Evidence Regulations 2007 should expressly provide that they apply to the exclusion of privacy principles 6 and 7. *These regulations apply to a video record when it is intended that the record may later be offered as evidence in criminal proceedings. Principles 6 and 7 relate to the access and correction of personal information*	5	Exempt
91	Section 42(2) of the Criminal Disclosure Act should be amended to refer to the Evidence Regulations 2007	3	N/A
92.1	Statutory secrecy provisions should be addressed in the response to recommendations 83, 84 and 85	4 But costings in Cab paper	N/A
92.2	Statutory secrecy provisions - the enhanced discussion of relationships between Acts (recommendations 83 and 84 refer) should be addressed in the LAC Guidelines	4	N/A
93	Section 27(1)(c) should be amended to clarify that the access refusal ground is concerned with protecting the maintenance of the law by public sector agencies	5	Exempt
94	Ministry of Justice, OPC and the Ombudsmen should produce guidance on the maintenance of the law exemption	4 But costings in Cab paper	N/A
95	The OPC should develop independent guidance on the maintenance of the law exemption if coordinated guidance is not possible in the short term	4 As above	N/A
96	OPC should produce guidance on the maintenance of the law exemption in principle 11	4 As above	N/A
97	A new exception to principle 11 should be created that would expressly permit an agency to report any reasonably held suspicion or belief that an offence has been or may be committed *[Principle 11 relates to the disclosure of personal information]*	5	Yes
98	OPC and the Police should consider working collaboratively on an information campaign about the reporting of crime	4 But costings in Cab paper	N/A
99	Part 11 of the Act should be repealed	2	N/A
100	Access to public registers should be dealt with under the relevant statute authorising the particular register	7	N/A

101	Section 13(1)(n) should be amended to delete the word "computer". *Section 13 lists the Privacy Commissioner's functions*	5	Exempt
102.1	The technology-neutral privacy principles should be retained	5	Exempt
102.2	The principles should be reviewed every 5 years	5	Exempt
103	Privacy Commissioner should consider convening an expert Privacy by Design Panel	5	Exempt
104	The Government should issue a Cabinet Office circular setting out when public sector agencies are expected to produce a privacy impact assessment.	6	Exempt
105	SSC should provide guidance on its website as to expectations for use of privacy impact assessments in the public sector, such guidance being prepared in consultation with the Department of Internal Affairs and the Privacy Commissioner.	6	Exempt
106	Privacy Commission should consider whether to issue a code of practice on biometrics	5	Exempt
107	Act should include an express statement of full accountability for cross-border outsourcing arrangements	5	Yes
108	OPC should provide guidance for agencies conducting a risk assessment prior to outsourcing personal information overseas	4 But costings in Cab paper	N/A
109	Act should include an express statement of full accountability for domestic outsourcing arrangements	5	Yes
110	A new accountability measure should be introduced for disclosures of personal information overseas	5	Yes
111	Provides exemptions to the new measures referred to in recommendation 110	5	Yes
112	Privacy Commissioner should have power to approve specified overseas privacy frameworks as providing acceptable privacy standards	5	Yes
113	Privacy Commission should provide guidance for New Zealand agencies on conducting risk assessments prior to disclosing personal information overseas	4 But costings in Cab paper	N/A
114	Act should be amended to allow the Privacy Commissioner to share relevant information with overseas privacy enforcement authorities	5	Yes
115	Act should include a provision allowing for the future adoption of a cross-border privacy rules system in New Zealand	5	Yes
116	The Marketing Association's Do Not Call register should be put on a statutory footing	6	N/A

117	Principle 12 should be amended to encourage measures to control the public display of unique identifiers, as a response to the problem of identity crime. *Principle 12 relates to unique identifiers*	5	Yes
118	Privacy Commissioner should produce guidance for agencies on the range of options available to reduce the misuse of unique identifiers	4 But costings in Cab paper	N/A
119	Section 14 should be amended to provide that, in exercising his or her functions, the Privacy Commissioner must take account of Maori needs and cultural perspectives, and of the cultural diversity of New Zealand society.	5	Yes
120.1	Principle 4 should be amended to provide that, in considering whether the collection of personal information is unfair or unreasonably intrusive for the purposes of principle 4(b), the age of the individual concerned must be taken into account. *Principle 4 relates to the manner of collection of personal information*	5	Yes
120.2	Privacy Commissioner should develop guidance material on taking the age of the individual into account	4 But costings in Cab paper	N/A
121	The Advertising Standards Authority, the Marketing Association and other relevant agencies should review codes on advertising to children	8	N/A
122	Section 14(b) should be amended to refer to New Zealand's international obligations concerning the rights and best interests of the child.	5	Yes
123	OPC should convene a working group to consider issues of capacity under the Act	4 But costings in Cab paper	N/A
124	Further work should be undertaken to explore issues of privacy and disability, to be facilitated by OPC	4 As above	N/A
125	Government should review the handling of health information	8	N/A
126	Section 23 should be amended to allow agencies to appoint a privacy officer from outside the agency.	5	Yes
127	There should be a single definition of "information matching programme"	7	N/A
128	The period of notice of adverse action provided in section 103 should be 10 days	7	N/A
129	To the examples of "adverse action" should be added decisions to impose a penalty and to recover a penalty or fine	7	N/A

130	Continuing programmes of information matching should have to be authorised under Part 10 of the Act	2	N/A
131	Agencies seeking legislation to authorise an information matching programme should provide the Privacy Commissioner with a protocol	7	N/A
132	There should no longer be a requirement of five-yearly review by the Privacy Commissioner of every information-matching provision, but the Commissioner should be able to conduct reviews as and when desirable.	5	Exempt
133	The government should be required to respond to a report within 6 months of it being presented	7	N/A
134	The Privacy Commissioner should be able to report separately on information matching programmes rather than including this in the annual report	5	Exempt
135	The information matching rules currently contained in Schedule 4 of the Privacy Act should be placed in the body of the Privacy Act, and the current rules 3 and 8 should be deleted.	7	N/A
136	The current blanket exemptions for Inland Revenue contained in section 101(5) and rule 6(3) of Schedule 4 should be repealed, but exemptions should be provided for in particular matching authorities where that is appropriate.	7	N/A
7 Stage 2 report	Recommendation 7 from Stage 2 relating to Public Registers. Provision should be made in the Act for applications for name and/or address suppression to the Privacy Commissioner, and that each public register statute should refer to the availability of such applications.	5	Yes
18 Stage 3 report	Commissioner to report on developments in surveillance	8	N/A
19 Stage 3 report	Recommendation from Stage 3 of the Law Commission's Review of the Law of Privacy: Both Closed-Circuit Television (CCTV) and Radio-Frequency Identification (RFID) should be regulated within the Privacy Act framework. The Privacy Commissioner should continue to monitor the adequacy of existing law to deal with these technologies.	5	Exempt
MoJ rec	Duty on agencies and individuals to take reasonable steps to resolve their disputes.	5	Yes

Recommendations from Privacy Commissioner reviews and referred to in the Law Commission's PAR recommendation number 1

Note: N/A refers to recommendations that have either been overtaken by Law Commission recommendations, implemented through another Act or workstream, or withdrawn by the Privacy Commissioner

Rec no.	Recommendations (from Privacy Commissioner reviews)	Status	In RIS?
1	The relevant changes in legislative drafting styles recently adopted by the Parliamentary Counsel Office should be applied throughout the Privacy Act.	5	Exempt
2	The marginal notes and headings in the following principle, sections, Part and rule should be amended to make them more helpful, accurate and precise: principle 9; sections 7, 27, 28, 42, 45, 73, 95, 100, 101 and 105; Part X; information matching rule 8.	5	Exempt
3	The present section notes concerning the official information legislation should be presented in a comparative table at the end of the Act.	5	Exempt
4	The Parliamentary Counsel Office should be requested to arrange for a consolidated reprint of the Privacy Act following the implementation of reforms adopted as a result of this report.	5	Exempt
5	An appropriate committee of Parliament should consider whether it is desirable to grant individuals access rights to information held about them by the House of Representatives or to adopt rules similar to any of the 12 information privacy principles.	9 Overtaken by LC rec 36	N/A
6	An appropriate committee of Parliament should consider whether it is desirable to: (a) adopt any measures to encourage members of Parliament to apply, or follow, any of the 12 information privacy principle; or (b) provide that MPs in their official capacities are agencies for some purposes of the information privacy principles	9 As above	N/A
7	Consideration should be given to whether it is appropriate to replace the total exemption for the Parliamentary Service Commission in subparagraph (b)(v) of the definition of "agency" with a partial exemption	9 As above	N/A
7A	As an alternative to recommendation 7. Recommend that subparagraph (b)(v) of the definition of 'agency' in section of the Privacy Act be amended so that the Parliamentary Service Commission be made subject to information privacy principles 1-5, and 7-12.	9 As above	N/A
8	The partial exemption for the Parliamentary Service in subparagraph (b)(vi) of the definition of "agency" should be repealed, or further restricted, if this can be achieved in a manner that does not impact upon the exemption in subparagraph (b)(iv).	9 As above	N/A

8A	As an alternative to recommendation 8. Recommend that, as with recommendation 7A, subparagraph (b)(v) of the definition of 'agency' in section of the Privacy Act be amended so that: (a) the Parliamentary Service Commission be made subject to information privacy principles 1-5, and 7-12; (b) the present partial exemption that applies to the Parliamentary Service generally be continued in relation to rights of access normally enjoyed under information privacy principle 6, with access rights also extended to prospective employees and contractors.	9 As above	N/A
9	Consideration should be given to including a definition of "tribunal" limited to statutory tribunals forming part of the New Zealand administrative or judicial structure.	10	N/A
10	Subparagraph (b)(ix) of the definition of "agency" should be repealed so that the Ombudsmen are considered to be an "agency" for the purposes of the Act.	9 Overtaken by LC rec 37	N/A
11	Consideration should be given to adopting a new definition of "document" in section 2 in conjunction with any redefinition of the term in the proposed Evidence Code.	5	Exempt
12	Consideration should be given to amending the definition of "personal information" to clarify the position of information sourced from, but not contained in, the register of deaths.	9 Overtaken by LC rec 4	N/A
13	Consideration should be given to redefining or recasting "public sector agency", "Minister", "department", "organisation" and "local authority".	5	Exempt
14	Consideration should be given to enacting a definition of "private sector agency".	5	Exempt
15	The definition of "statutory officer" should be moved from section 2(1) into section 3.	5	Exempt
16	Consideration should be given to the desirability of enacting a definition of "use" which will encompass the retrieval, consultation or use of information.	5	Exempt
17	Section 2(2), (avoidance of doubt clause in interpretation section) should be replaced with a more concise provision.	5	Exempt
17A	Consideration should be given to adding, as a second part of information privacy principle 1, a new principle that "wherever it is lawful and practicable, individuals should have the option of not identifying themselves when entering transactions."	9 Overtaken by LC rec 35	N/A
18	Section 46(4) should be amended to provide that a code of practice may require an agency to take all practicable steps to ensure that an individual may ascertain the agency's policies and practices in relation to particular personal information.	5	Exempt
19	Information privacy principles 1, 3(1) and 8 should be amended to substitute the phrase "purpose or purposes" for the word "purpose". Note: Not necessary as *section 33 of the Interpretation Act 1999 provides for words in the singular to be read as words in plural and vice versa*	11	Exempt
19A	The word "directly" should be omitted from information privacy principle 3(1).	9 Overtaken by LC rec 11	N/A

20	Information privacy principle 3(4)(a), (non compliance is authorised by the individual concerned), should be repealed.	9 Overtaken by LC rec 13	N/A
21	Information privacy principle 3(4)(f)(ii), (information will be used for statistical or research purposes and individual not identifiable), should be repealed.	9 As above	N/A
22	Consideration should be given to establishing a judicial warrant process in relation to the use of covert video surveillance in the investigation of offences. Incorporated into *the Search and Surveillance Act 2012*	11	N/A
23	Information privacy principle 5(a)(ii), (storage and security of personal information), should be amended by inserting the word "browsing" or "inspection".	9 Overtaken by LC rec 15	N/A
23A	The Privacy Act should include an obligation requiring agencies to notify affected individuals where a security breach by the agency puts the individual at risk.	9 Overtaken by LC recs 67-61	N/A
24	Information privacy principle 7 (correction of personal information), should be suitably amended so that agencies are obliged to inform requestors, in cases where the agency is not willing to correct information, that they may request that a statement be attached to the information.	9 Overtaken by LC rec 20	N/A
25	Information privacy principle 7 (correction of personal information) should be supplemented with a right to prevent the use or disclosure of personal information for the purposes of direct marketing through the deletion or blocking of personal information held by the agency for direct marketing purposes.	9 Overtaken by LC rec 116; which is status 6	N/A
25A	There should be a reference in information privacy principle 7 to the application of Part 5 of the Act.	5	Exempt
25B	Consideration should be given to the merits of a national system, established under statute, to control the use of automated dialling machines and enable individuals to opt-out of telemarketing.	9 Overtaken by LC rec 116; which is status 6	N/A
26	Consideration should be given to amending information privacy principle 8 to substitute the phrase "use or disclose" for "use" in the first line.	9 Overtaken by LC rec 16	N/A
27	Section 46(4) should be amended to provide that a code of practice may require an agency to retain specified information or documents for a specified period, not exceeding six years.	5	Exempt
28	In relation to the controls on reassignment of unique identifiers: (a) information privacy principle 12(2) should be limited so that the prohibition is solely in relation to the reassignment of unique identifiers originally generated, created or assigned by a public sector agency; and (b) section 46(4) should be amended to make it clear that a code of practice may apply the controls in principle 12(2) to the	9 Overtaken by LC rec 33	N/A

	assignment of unique identifiers generated, created or assigned by any agency (not simply a public sector agency).		
28A	The Law Commission or officials, in further reviewing principle 12, should usefully have regard to: (a) the Australian experience and proposals with its identifier principle (b) the usefulness of including exceptions to principle 12(2) (c) the merit of including controls in principle 12 to encourage number truncation or other ways of controlling the public display of unique identifiers.	9 Overtaken by LC rec 117	N/A
29	Section 66(1) should be amended so that an interference with privacy may be established notwithstanding the absence of any harm or detriment of the type set out at section 66(1)(b) in cases of wilful breach of information privacy principle 12(2).	9 Overtaken by LC rec 54	N/A
30	Section 7(1) should be amended by transferring its content, in so far as it relates to information privacy principle 11, into principle 11 as a new exception.	9 Overtaken by LC recs 80-82	N/A
31	Consideration should be given to transferring the content of: (a) section 7(4) into information privacy principles 1 to 5, 7 to 10, and 12 as exceptions; and (b) section 7(5) into Part VI.	9 Overtaken by LC recs 80-82	N/A
32	The content of section 7(2) and (3), in so far as they relate to information privacy principle 6, should be relocated into Part IV.	9 Overtaken by LC recs 80-82	N/A
33	Section 7(2) and (3), in so far as they relate to information privacy principle 11, should be repealed and replaced with a single provision, which may be relocated into principle 11 itself, to the effect that where another enactment imposes a more restrictive obligation of secrecy or non-disclosure than principle 11, the principle does not operate to provide additional grounds for disclosure.	9 Overtaken by LC recs 80-82	N/A
34	A sunset clause should provide for the expiry of section 7(3) after a period of 3 years.	9 Overtaken by LC recs 80-82	N/A
34A	With respect to statutory secrecy provisions saved by section 7(2): (a) the departments which administer statutes containing such provisions should consider whether they ought to be amended so that individual access requests under information privacy principle 6 are not unnecessarily precluded; and (b) in particular, section 81 of the Tax Administration Act 1994 should be amended to allow for individual access by individual concerned pursuant to information privacy principle 6 (in drafting such a provision care should be taken to address the risk of coerced access requests).	9 Overtaken by LC recs 80-82	N/A
35	The Act should be amended to include express provision for controlling trans-border data flows, consistent with clause 17 of the OECD Guidelines and the emerging international approach to data export. In particular consideration should be given to providing: (a) a mechanism which would enable mutual assistance to be extended to prohibit data exports in circumstances where New	9 Overtaken by LC recs	N/A

	Zealand is being used as a conduit for transfers designed to circumvent controls in EU and other privacy laws; (b) mechanisms for imposing restrictions concerning categories of personal data for which there are particular sensitivities and in respect of which the recipient countries would provide no adequate protection.	107-115	
36	Section 11 (enforceability of principles) should be amended so that the entitlement under information privacy principle 6(1) to have access to information held by an agency is a legal right in circumstances where the agency is prosecuting the individual for an offence. *Note: already implemented through the Criminal Disclosure Act 2008*	11	N/A
37	There should be provision for the Commissioner to put a case for funding directly to Treasury and relevant Ministers.	10	N/A
37A	A provision should be inserted into Part 3 of the Act stating that the Commissioner must act independently in the exercise or performance of his or her functions	11	N/A
37B	The Privacy Commissioner should have mandatory audit powers in relation to at least the public sector but preferably both public and private sectors.	9 Overtaken by rec 64	N/A
38	Section 15(3) should be amended to make clear that a deputy may be designated as an alternate Human Rights Commissioner with the concurrence with the Chief Human Rights Commissioner.	10	N/A
39	Section 20(2) should be amended by substituting "Human Rights Act 1993" for the reference to the "Human Rights Commission Act 1977".	5	Exempt
39A	References to "Proceedings Commissioner" in sections 20, 77, and 116 should be replaced by "Director of Human Rights Proceedings".	5	Exempt
40	Consideration should be given to repealing section 21 (directories of personal information). Consequently section 13(1)(d) should be repealed and the content of section 21(1)(a) to (f) transferred to a rewritten section 22 (Commissioner may require agency to supply information).	9 Overtaken by LC Rec 48	N/A
41	Consideration should be given to the costs and benefits of having the Ministry of Justice include some of the information listed in section 21(1) in any future Directory of Official Information.	9 Overtaken by LC rec 48	N/A
42	Section 21(3) should be amended so that the Commissioner is obliged to have regard, in determining whether or not a directory of personal information should be prepared, to the compliance costs to agencies consequent upon such a determination.	9 Overtaken by LC rec 48	N/A
43	An appropriate amendment should be made to section 21(1) or 22 so that it is plain the Privacy Commissioner has the power to obtain from an agency the identity of the agency's privacy officer to enable the Commissioner to respond to enquiries from the public.	5	Exempt
44	Section 23 (privacy officers) should be amended to delete the words "within that agency".	9 Overtaken by LC rec 126	N/A
45	Clause 2(3) of the First Schedule should be repealed so that the Minister does not have the function of determining how many staff the Commissioner engages whether generally or in respect of any specified duties. Note: already repealed by the Crown Entities Act 2004.	11	N/A
46	Clause 6(2) of the First Schedule should be repealed as being unnecessary.	11	N/A

46A	Section 26 should be amended so that a government response to the Privacy Commissioner's recommendations is required to be presented to Parliament within six months of receipt and that subsequent reviews should be at five year intervals after a government response is available.	9 Overtaken by LC recs 49 and 50.	N/A
47	The existing reasons for refusal of requests set out in sections 27, 28 and 29 should be reorganised into an ungrouped list of reasons to make it easier for users of the Act to locate relevant provisions.	5	Exempt
48	Consideration should be given to the merits of redrafting the "maintenance of the law" withholding grounds to make it plainer that the constituent law enforcement interests protected.	9 Overtaken by LC recs 93 to 96	N/A
49	Consideration should be given to the desirability of enabling the withholding of information where there is a significant likelihood of harassment of an individual as a result of the disclosure of information.	9 Overtaken by LC rec 23	N/A
50	A straightforward definition of 'trade secret' should be inserted into section 28.	5	Exempt
51	Consideration should be given to amending section 28(1)(b) to provide for withholding of information where the disclosure would unreasonably prejudice the commercial position of the agency itself, particularly where the information requested would reveal the agency's bargaining position in respect of negotiations involving the individual concerned. *Referred to MBIE for consideration*	9 overtaken by LC rec 17 of OIA report (which has been referred)	N/A
52	Consideration should be given to providing statutory guidance on the withholding of information in the common cases of "mixed" information concerning the requestor and other individuals.	9 Overtaken by LC rec 24	N/A
53	It should be made clear that section 29(1)(b) is not available in relation to material that is provided by a person within the agency as part of his or her job.	5	Exempt
54	Sections 43 and 44 should be amended so that the grounds in support of the reasons for withholding evaluative material be given, without the requestor needing to expressly ask, unless the giving of those grounds would itself prejudice the interests protected by section 29(1)(b).	5	Exempt
55	Section 29(1)(b) should be amended to clarify that the author of evaluative material may refuse an information privacy request in circumstances where the material may be withheld by the recipient agency.	5	Exempt
56	Consideration should be given to amending section 29(1)(c) to provide for consultation with the individual's medical practitioner or, in the circumstances of the case, the individual's psychologist.	9 Overtaken by LC rec 26	N/A
56A	Consideration should be given to simplifying or omitting the definition of "medical practitioner" in section 29(4).	9 Overtaken by LC rec 26	N/A

57	Section 29(1)(f) should be redrafted so that it provides a self-contained explanation of the meaning of legal professional privilege.	5	Exempt
58	Section 29(2)(c) should be redrafted to make plain the link with the obligations to transfer a request.	5	Exempt
58A	As alternative to recommendation 66, (see Compliance & Administration Costs) consideration should be given to adding new reasons for refusal to section 29 to cover positions where: • a person making a request has already been refused access to the information requested, provided that no reasonable ground exist for that person to request the information again; and • a person making a request has already been given access to the information requested on a recent occasion, provided that no reasonable grounds exist for the person to request the information again.	9 Overtaken by LC rec 27	N/A
59	Section 31, (restriction where person sentenced to imprisonment), should be repealed. *Note: already implemented via the Criminal Disclosure Act 2008*	11	N/A
60	Consideration should be given to extending the application of section 32 to information to which section 29(1)(e) applies.	5	Exempt
60A	The following statutory provisions, and any similar provisions should be amended so that relevant requests are treated as information privacy requests in appropriate cases: Coroners Act 1988 (section 44); Transport Services Licensing Act 1989 (section 24); Civil Aviation Act 1990 (sections 10, 19, and 74); Building Act 1991 (2nd Schedule, clause 7); Maritime Transport Act 1994 (sections 49, 50, 189, and 276); Hazardous Substances and New Organisms Act 1996 (section 53). *Note: there has been recent legislative amendments to a number of these Acts*	5	Exempt
61	The standing requirements in section 34 should be abolished. *Note: already implemented through the Privacy (Cross-border Information) Amendment Act 2010.*	11	N/A
62	Public sector agencies should be entitled to make a reasonable charge, of the type permitted by section 35, for making information available to an individual overseas who is neither a New Zealand citizen nor permanent resident.	5	Exempt
63	If the general standing requirement in section 34 is removed then section 13(3) of the Adoption (Intercountry) Act 1997 should be repealed. *Note: already implemented through the Privacy (Cross-border Information) Amendment Act 2010.*	11	N/A
64	Section 35 (when charges apply for requests) should be redrafted in a simpler fashion.	5	Exempt
65	Section 35(3)(b)(i) (charging for corrections) should be repealed.	9 Overtaken by LC rec 28	N/A
66	The Commissioner or the Tribunal should be empowered to exempt an agency from having to deal with a particular individual's access request for a fixed period where it can be shown that the individual has lodged requests of a repetitious or systematic nature which would unreasonably interfere with the operations of the agency and amount to an abuse of the right of access.	9 Overtaken by LC rec 27	N/A
67	Section 37 should be amended to make it clear that in cases where a request for urgency has been substantiated, an agency is obliged to make reasonable endeavours to process the request with priority.	5	Exempt
67A	Section 38 (agency to provide assistance to individual) should be replaced with a provision modelled upon the replacement to section 13 of the Official Information Act 1982 recommended by the Law Commission.	5	Exempt
68	Section 39 should be amended so that: (a) an agency is relieved of the obligation to transfer a request in circumstances where it has good reason to believe that the individual does not wish the request to be transferred; and (b) the agency duly informs the requestor, together with information about the appropriate agency to which any future request should be directed.	5	Exempt
69	Consideration should be given to clarifying the meaning of the phrase "time limit fixed" in section 66(3) so as to emphasise the	5	Exempt

	primary obligation to give access "as soon as reasonably practicable".		
69A	The 20 working day outer time limit in section 40(1), (decisions on requests) should be replaced with a 15 working day limit. There should be a year's delay before the new limit becomes operative.	5	Exempt
69B	Consideration should be given to removing section 40(2) into a separate section dealing with an agency's entitlements and duties *following* the taking of a decision to grant an individual access to information, including the duty to make information available without undue delay.	5	Exempt
70	Section 40(3) and (4) (procedure for transferring requests) should be repealed.	5	Exempt
71	Complexity of the issues raised by a request should be added to the grounds for an extension of time under section 41(1)	9 Overtaken by LC rec 29	N/A
72	Section 41(3) should be amended by replacing the phrase "within 20 working days" with "as soon as reasonably practicable, and in any case not later than 20 working days".	5	Exempt
73	Section 46(2)(aa) should be amended by deleting all of those words in parentheses, that is "but not all of those principles".	5	Exempt
74	Section 46(4) should be amended by adding a paragraph acknowledging that a code may provide for such other matters as specified in any other Act.	5	Exempt
75	Section 46(6) should be replaced with a provision which empowers the Privacy Commissioner to include in a code of practice a provision applying principle 11 to an agency, or a class of agencies, to health information about any deceased person for a period specified in the code beyond any such person's death.	9 Overtaken by LC rec 5	N/A
75A	Section 46(6) should be amended so that it applies to information privacy principle 5 as well as principle 11.	9 Overtaken by LC rec 5	N/A
76	Consideration should be given to amending section 47(3) to make it clear that a body can apply for a code whether it represents the whole of a class of agencies, industry, profession etc or just a substantial section.	5	Exempt
77	There should be provision for the Commissioner to require a representative body applicant to undertake notification under section 47(4), (proposal for issuing of code of practice), in terms directed by the Commissioner.	5	Exempt
78	Section 47(5), (publication of notice requirement for proposals for issuing of code of practice) should be repealed.	5	Exempt
79	Section 54(1) should be amended to enable the Commissioner to grant an exemption to enable information to be kept notwithstanding that this would otherwise be in breach of principle 9.	9 Overtaken by LC rec 40	N/A
80	Section 54 should provide that the Commissioner may require the applicant to publicly notify an application in appropriate terms.	5	Exempt
81	Consideration should be given to the desirability of narrowing section 55(b) so as to enable access requests by the individual concerned to evidence given, or submissions made, to a Royal Commission prior to the report to the Governor-General where that evidence was given, or the submissions made, in open public hearing. *Overtaken by DIA work on the Inquiries Bill*	6	Exempt
81A	Paragraph (j) of the definition of "official information" in the Official Information Act 1982 should be amended to replace "department or Minister of the Crown or organisation" with "agency (as that term is defined in the Privacy Act 1993)".	5	Exempt
82	Section 56 should be amended so that an individual cannot rely upon the domestic affairs exemption where that individual has collected personal information from an agency by falsely representing that he or she has the authorisation of the individual concerned or is the individual concerned.	9 Overtaken by LC rec	N/A

		44	
82A	The domestic affairs exemption in section 56 should be limited so that it does not apply to cases of secret filming of people in intimate situations or to unlawful collection of personal information.	9 Overtaken by LC rec 45	N/A
83	The exemption for intelligence organisations in section 57 should be narrowed so that principles 1, 5, 8 and 9 apply to information collected, obtained, held, or used, by an intelligence organisation.	9 Overtaken by LC rec 46	N/A
83A	Officials responsible for disaster management in New Zealand should give consideration to whether any amendment to the Privacy Act is desirable to provide for best practice disaster information management in the event of a declared emergency and, in particular, whether any amendments such as those adopted in Australia are useful. *Note: Privacy Commissioner has subsequently issued a Code of Practice covering information-sharing in civil defence emergencies. This recommendation is now redundant.*	6	N/A
84	Public register privacy principle 1 should be amended so that search references are required to be consistent with the purpose of a particular register.	5	Exempt
85	As new public register provisions are enacted, or existing ones reviewed or consolidated or amended, consideration should be given to including statutory statements of purpose.	5	Exempt
86	Consideration should be given to establishing in the Act a regulation-making power to specify, in respect of any particular public register, the purposes for which the register is established and is open to search by the public.	5	Exempt
87	Public register privacy principle 2 should be re-enacted with a structure which more clearly leads users to identify its elements.	5	Exempt
88	Public register privacy principle 3 should be amended by adding "in New Zealand" after the words "a member of the public".	5	Exempt
89	If recommendation 88 is adopted, there should be a power in the Act to make regulations, after consultation with the Privacy Commissioner, in respect of any public register to authorise and control the electronic transmission of personal data which is not limited to members of the public within New Zealand.	5	Exempt
90	Public register privacy principle 4 should be amended so that the constraints upon charging for access to personal information from a public register apply only in relation to the making available of information to the individual concerned.	5	Exempt
91	A further public register privacy principle should be enacted that provides that personal information containing an individual's name, together with the individual's address or telephone number, is not to be disclosed from a public register on a volume or bulk basis unless this is consistent with the purpose for which the register is maintained.	5	Exempt
92	Section 7(6) should be replaced with a subsection in section 8 providing that the information privacy principles apply in respect of a public register only to the extent specified in section 60 and 63(2)(b)	5	Exempt
93	Section 60 should be amended as follows: (a) in subsection (1) omit the phrases "subject to subsection (3) of this section" and "so far as is reasonably practicable"; (b) the content of subsection (3) should be moved adjacent to subsection (1) and redrafted in plainer fashion; (c) in subsection (2) "person" should be replaced by "agency".	5	Exempt
94	Section 60(2) should be amended: (a) by omitting the words "as far as is reasonably practicable"; and (b) by substituting an exception based upon the authorisation of the individual concerned.	5	Exempt

95	The public register privacy principles should be enforceable in a similar manner to the information privacy principles by amending, as necessary, sections 61(3)-(5) and 66.	5	Exempt
96	The Order in Council process in section 65 should be utilised to add existing register provisions in enactments to the list in the Second Schedule. The Ministry of Justice should commence work to identify the relevant enactments, and to consult with the relevant agencies, so that the first Order in Council is ready to be issued during the 1998/99 year with the completion of the project by the end of the following year.	5	Exempt
97	The Ministry of Justice should, in carrying out the exercise to bring register provisions into the Second Schedule pursuant to section 65, also consider in respect of each register the desirability of issuing regulations under section 121 of the Domestic Violence Act 1995.	5	Exempt
98	A new public register privacy principle should be created which obliges agencies maintaining public registers to adopt a process to hold details of an individual's whereabouts separately from information generally accessible to the public where it is shown that the individual's safety or that of the individual's family would be put at risk through the disclosure of the information. An exception is to be provided where alternative safeguards exist to ensure that such information is not disclosed to the public for purposes unrelated to the purposes for which the information was collected or obtained.	5	Exempt
99	A mechanism should be established in Part VII of the Act, with the details set out in a new schedule, enabling individuals to obtain suppression directions in relation to public registers which would replace Part VI of the Domestic Violence Act but be applicable to a wider range of circumstances concerning personal safety and harassment.	5	Exempt
100	The official information statutes should be excluded from questions of release of personal information from public registers.	5	Exempt
101	Section 66(1) should be amended by deleting the words "and only if".	5	Exempt
101A	Section 66(2)(a) should be amended by inserting appropriate reference to a decision to transfer a request under section 39.	5	Exempt
101B	Section 66(4) should be amended to encompass undue delay on the part of an agency in transferring a request under section 39 (transfer of requests).	5	Exempt
101C	Section 66(2)(a)(vi) should also refer to a refusal of a request under information privacy principle 7(1)(b).	5	Exempt
101D	Section 66(3) should be amended so that, in relation to a correction request, a failure to meet the time limit fixed by section 40(1) is deemed to be a refusal to correct personal information.	5	Exempt
101E	Section 66(4) should be amended so that undue delay in correcting information in response to a correction request is deemed, for the purposes of section 66(2)(a)(vi), to be a refusal to correct the information to which the request relates.	5	Exempt
101F	Consideration should be given to clarifying the relationship between sections 44 and 66.	5	Exempt
102	Section 67(2) and (3) which provide for the lodging of complaints under the Privacy Act with the Ombudsmen, and for the transfer of such complaints, should be repealed.	5	Exempt
102A	Consideration should be given to providing for the registration and handling of representative complaints.	9 Overtaken by LC rec 60	N/A
103	Section 70(2) should be amended so that the Commissioner is obliged to advise of the procedure to be followed only where he has decided to investigate a complaint so as to avoid overlap with the obligations in section 71(3)	5	Exempt
104	Section 70 should be amended to recognise that a decision to investigate a complaint, or to take no action on a complaint, may be postponed until preliminary inquiries are made of the complainant for the purpose of determining whether: (a) the Commissioner has power to investigate the matter;	5	Exempt

	(b) the Commissioner may, in his or her discretion, decide not to investigate the matter; or (c) the complainant wishes to proceed with the complaint.		
104A	Section 71 should be amended so that the Commissioner has discretion to decide to take no action on a complaint where the complaint was made more than 12 months after the complainant became aware of the action complained about.	5	Exempt
105	Consideration should be given to establishing a process whereby a decision by the Commissioner that a complaint is beyond jurisdiction can, on this question alone, be referred by the complainant to the Complaints Review Tribunal for its decision on the matter.	5	Exempt
106	Provision should be made in Part VIII of the Act for the Commissioner to defer action, or further action, on a complaint where: (a) the complainant has not complained to the agency concerned and the Commissioner considers that the complainant should do so in an attempt to directly resolve the matter; or (b) the complaint concerns an agency in respect of which there is an independent, expeditious and appropriate procedure for addressing such complaints available through an industry body which the complainant has not used.	Overtaken by MoJ Rec (which has status 5 in this RIS)	Exempt
107	Sections 72, 72A and 72B should be combined into a single section providing for the referral of complaints to the Ombudsmen, Health and Disability Commissioner and Inspector-General of Intelligence and Security, and consideration should be given to listing other statutory complaints bodies.	5	Exempt
107A	Provision should be made for the transfer of complaints to, or the cooperative handling of complaints with, privacy commissioners and similar authorities in other states.	9 Overtaken by LC rec 114	N/A
108	Adequate funding should be made available so that the volume of complaints received at the Office of the Privacy Commissioner can be processed, as required by section 75, "with due expedition".	Overtaken by bid for baseline increase	N/A
109	Section 77(1)(a) should be amended so that the Commissioner is required to continue endeavouring to secure a settlement only where it appears to the Commissioner that settlement is possible.	5	Exempt
110	Section 78 should be broadened to encompass all charging complaints.	5	Exempt
111	Consideration should be given to including in, or following, section 81(5) a provision that the Prime Minister may refer a report given under section 81(4) to the Intelligence and Security Committee.	5	Exempt
112	Provision should be made by amending section 82(2), or otherwise, to allow Tribunal proceedings to be brought by the Proceedings Commissioner where there is a breach of an assurance given to the Privacy Commissioner under section 74 (settlement of complaints) or 77 (procedure after investigation).	9 Overtaken by LC rec 63	Exempt
112A	Consideration should be given to clarifying the position in respect of proceedings taken under section 83 where there is a mixture of issues before the Tribunal, some which have, and others which have not, been the subject of an investigation by the Privacy Commissioner.	5	Exempt
112B	Section 83 should provide that an aggrieved individual may only bring proceedings within six months of receiving notice that: (a) the Commissioner or Director of Human Rights Proceedings are of the opinion that the complaint does not have substance or should not be proceeded with; or (b) the DHRP agrees to the aggrieved individual bringing proceedings or declines to take proceedings.	5	Exempt
113	Section 88(2) and (3), (damages awarded in proceedings), should be more closely aligned with section 88 of the Human Rights Act 1993.	5	Exempt

113A	Section 88(2) should be amended to enable the Proceedings Commissioner to pay damages recovered directly to the aggrieved individual on whose behalf the proceedings were brought. *Note: implemented by the Privacy Amendment Act 2003*	11	N/A
113B	Consideration should be given to: (a) establishing a panel for additional members of the High Court regarding appeals, separate from that used by the Complaints Review Tribunal; and/or (b) ceasing to apply section 126 of the Human Rights Act to appeals to the High Court taken in respect of Privacy Act cases; or (c) allowing for additional members to be appointed to the High Court on a case by case basis where sought by the parties or ordered by the Court itself.	10	N/A
113C	Section 123(4), (revocation of delegations), should be amended to empower the High Court to allow further time to lodge an appeal in appropriate cases. *Note: section 123 was repealed by the Crown Entities Act 2004.*	11	N/A
114	Section 92 should be amended so that the Commissioner may require an agency to comply with a requirement made pursuant to section 91 within a shorter period than 20 working days where the urgency of the case so requires.	10	N/A
115	Section 92(3), (failure of agency to comply with requests of Commissioner can be reported to Prime Minister), should be repealed.	5	Exempt
116	Section 95(3) should be amended to specify that: (a) the Prime Minister, in respect of paragraph (a); and (b) the Attorney-General, in respect of paragraph (b); personally may exercise the power to prevent disclosure of information to the Privacy Commissioner.	10	N/A
116A	Consideration should be given to including an explicit privilege against the admissibility of apologies in Tribunal proceedings, modelled upon the Civil Liability Act 2002 (NSW), with a view to promoting apologies in the securing of settlements.	5	Exempt
117	The definition of "adverse action" in section 97 should be supplemented by a paragraph relating to decisions to impose a penalty and to recover a penalty earlier imposed.	9 Overtaken by LC recs 127-136	N/A
118	Consideration should be given to amending the definitions of "authorised information matching programme" and "information matching programme" in section 97 so as to exclude manual comparison from their scope.	10	N/A
119	Consideration should be given to replacing references in Part X and elsewhere to "information matching" by "data matching".	10	N/A
120	The definition of "specified agency" in section 97 should be amended so that the agencies are listed in the Third Schedule alongside the information matching provisions to which they relate.	9 Overtaken by LC recs 127-136	N/A
121	Consideration should be given to: (a) including in section 97, in addition to the definition of "specified agency" (which could be renamed "participating agency"), definitions of "source agency", "matching agency" and "user agency"; and (b) utilising these newly defined terms in Part X and the Fourth Schedule as appropriate.	9 Overtaken by LC recs 127-136	N/A
122	Section 98(c) should be amended so that alternative means of achieving the objective of a proposed matching programme are examined with a view to considering whether they would be more, or less, privacy intrusive.	9 Overtaken by LC recs 127-136	N/A
123	Section 98(e) should be amended so that in considering whether a programme involves information matching on a scale that is excessive, regard is also had to:	9 Overtaken	N/A

	(i) the amount of detail about an individual that will be disclosed as a result of the programme; and (ii) the frequency of matching.	by LC recs 127-136	
124	Section 98(f) should be amended so that the information matching guideline refers not only to the information matching rules but also to Part X of the Act.	9 Overtaken by LC recs 127-136	N/A
125	Section 99 should be amended to require the parties to review any information matching agreement at least once every three years and to report the results of that review to the Privacy Commissioner.	9 Overtaken by LC recs 127-136	N/A
126	Consideration should be given to limiting the Inland Revenue Department's exemptions in section 101(5) and information matching rule 6(3) so that IRD is exempted from obligations to destroy information only where this is an intended objective of the programme.	9 Overtaken by LC recs 127-136	N/A
127	Section 102 should be amended to make clear that it refers to both the 60 working day time limit in section 101(1) and the 12 month time limit in section 101(2)	9 Overtaken by LC recs 127-136	N/A
128	Section 103(1) should be amended by substituting a 10 working day period for the present 5 working day period.	9 Overtaken by LC recs 127-136	N/A
129	Section 103(1A), (notice of adverse action proposed), should be repealed.	9 Overtaken by LC recs 127-136	N/A
130	Consideration should be given to amending section 104(2)(e) to adopt aspects of the clause 12(v) of the Australian Data-matching Program (Assistance and Tax) Guidelines.	10	N/A
131	Section 105 should be amended so that the annual information matching report may be submitted separately from the annual report required under section 24.	9 Overtaken by LC rec 134	Exempt
132	Consideration should be given to funding the Privacy Commissioner's information matching monitoring activities by charges on specified agencies involved in carrying out information matching programmes.	9 Overtaken by LC recs 127-136	N/A
133	Information matching rule 1 should be retitled "Openness and public awareness concerning operation of programme" and consideration should be given to enhancing the rule by detailing mandatory requirements, and a variety of discretionary methods, by which agencies may ensure that individuals who will be affected by a programme are made aware of its existence and effect.	9 Overtaken by LC recs 127-136	N/A

134	Information matching rule 2 should be amended by deleting the phrase "unless their use is essential to the success of the programme" and replace it with provision for agencies to apply to the Commissioner for approval to use unique identifiers where the Commissioner is satisfied that their use is essential to the success of the programme.	9 Overtaken by LC recs 127-136	N/A
135	A more informative heading should be given to information matching rule 5 and consideration should be given to redrafting the rule in a clearer fashion possibly drawing upon the Australian approach and using defined terms.	9 Overtaken by LC recs 127-136	N/A
135A	The Commissioner should be empowered to grant exemptions from information matching rule 6(1).	9 Overtaken by LC recs 127-136	N/A
136	Information matching rule 8(2) should be repealed or, if retained, its purpose and effect made plain.	9 Overtaken by LC recs 127-136	N/A
137	Provision should be made for terms used in Part X, and the information matching rules, to be able to be defined in the information matching rules themselves.	9 Overtaken by LC recs 127-136	N/A
138	Section 108 should be amended to replace the reference to "subclause (2)(d)(i) of principle 2 or paragraph (e)(i) of principle 11" with a reference to all of the exceptions to principles 2 and 11.	9 Overtaken by LC recs 127-136	N/A
139	Section 112 providing for local authorities to be authorised to have access to law enforcement information should be repealed together with the definition of "local authority" in section 110 and the references to local authorities in the Fifth Schedule.	5	Exempt
140	If section 112 is not repealed in its entirety then the reference to local authorities in the Fifth Schedule relating to the national register of drivers' licences should be repealed.	5	Exempt
141	All existing approvals given under section 4E of the Wanganui Computer Centre Act 1976 should be reviewed and: (a) any that are unnecessary should be revoked; (b) any which need to be continued should be replaced, within a reasonable time, with a new notice carrying appropriate conditions issued under section 112.	5	Exempt
142	Provision should be made to allow the Fifth Schedule to be amended by Order in Council subject to a five year sunset clause.	5	Exempt
143	Consideration should be given to the merits of making consistent amendments to: (a) section 115 of the Act; (b) section 48 of the Official Information Act 1982; and (c) (section 41 of the Local Government Official Information and Meetings Act 1987; to meet the perceived difficulties of interpretation raised by the distinction in the first and second subsections of each of these provisions between "the making available of information" and the "making available of, or the giving of access to, information".	5	Exempt
144	Section 96, or the First Schedule, should be amended so that the obligation of secrecy clearly extends to former Commissioners and persons formerly engaged or employed in connection with the work of the Commissioner.	5	Exempt

	Fourth Supplement: 2.21 - Accordingly, recommendation 144 should now read as follows: *Section 96... should be amended so that the obligation of secrecy clearly extends to former Commissioners and persons formerly engaged or employed in connection with the work of the Commissioner. Provision should also be made for the Director of Human Rights Proceedings.*		
145	Sections 117, 117A and 117B should be combined into a single consultation section with consideration given to placing the details of the officer with whom consultation is to be undertaken and the purposes of such consultation in a new schedule.	5	Exempt
146	Consideration should be given to making provision, along the lines of sections 117 to 117B, for consultation with other statutory bodies such as the Police Complaints Authority.	5	Exempt
147	Sections 124 and 125 should be repealed and replaced by a single brief provision providing that the relevant delegation provisions in the Local Government Act 1974 and Local Government Official Information and Meetings Act 1987 apply.	5	Exempt
148	There should be an offence provision created concerning any person who intentionally misleads an agency by: (a) impersonating the individual concerned; or (b) misrepresenting the existence or nature of authorisation from the individual concerned; (c) in order to make the information available to that person or another person or to have the personal information used, altered or destroyed.	9 Over-taken by LC recs 66.1 and 66.2	N/A
149	There should be an offence created of knowingly destroying documents containing personal information to which the individual concerned has sought access in order to evade an access request.	9 Over-taken by LC recs 66.1 and 66.2	N/A
149A	Note recommendation 149. Consideration should be given to creating an explicit duty to retain requested personal information for as long as is reasonably necessary to allow the individual to exhaust any recourse under the Act, to accompany the proposed offence of knowingly destroying documents to evade an access request	5	Exempt
150	Section 107 should provide that all information for an offence must be laid within 12 months from the time when the matter of the information arose.	10	N/A
151	A provision should be included to prohibit employers, prospective employers, and providers of services, requiring individuals to exercise their access rights to obtain criminal history information as a condition of obtaining employment, continuing employment, or obtaining services.	5	Exempt
152	Provision should be made to constrain contractual requirements that oblige individuals to supply copies of health records.	5	Exempt
153	Section 132 (savings provision) should be repealed.	5	Exempt
154	The Ministry of Justice, together with the Privacy Commissioner and the specified agencies, should study the Fourth Schedule to consider whether: (a) the information matching rules might be expressed more clearly; (b) the clarity or effectiveness of the rules would be enhanced by the use of new concepts, which might be defined, or by defining existing concepts that are used; (c) the use of flow-charts would improve presentation.	9 Overtaken by LC recs 127-136	N/A

Appendix 3

Government response to Law Commission's recommendations from its review of the Privacy Act 1993 (including both interim and supplementary responses)

Recommendations	How addressed
1, 2, 91	**Agreed** in the interim Government response
5, 7, 8, 11, 12, 13.1, 14, 16-18, 20, 22, 23, 25, 26, 28, 29, 32, 33, 35, 40.1, 41-44, 45.1, 45.2, 47, 48, 51, 54, 56-59, 60, 62, 63, 66.1, 66.2, 80-82, 90, 93, 97, 101, 102.1, 107, 109, 110-112, 117, 119, 120.1, 126, 132, 134 MoJ recommendation regarding duty on agencies and individuals to take reasonable steps to resolve their disputes, 19 from Stage 3 of the Law Commission's review	**Agreed** in the supplementary Government response
3, 37, 64, 65, 67-79, 114-115	**Agreed in a modified form, or partially agreed**, in the supplementary Government response
100,127, 128, 129, 131, 133, 135 and 136	**Deferred** by interim Government response
36, 52, 53, 7 from Stage 2 of the Law Commission's review	**Deferred** in supplementary Government response
104, 105	**Included** in the response to GCIO's report on publicly accessible systems
125, 18 from Stage 3 of the Law Commission's review	**Rejected** in interim Government response
27	**Rejected** but, instead, the supplementary Government response **invites the Privacy Commissioner and the Ombudsmen** to provide additional education and guidance
103, 106	The supplementary Government response **invites the Privacy Commissioner** to consider these recommendations
6, 13.2, 19, 21, 40.2, 49, 50, 55, 61, 86, 87, 88, 89, 102.2, 122	**Rejected** in supplementary Government response
30, 31, 99, 130 and the eight recommendations in Appendix 1	The Government **responded** to these recommendations on Government information sharing when it introduced the Privacy (Information Sharing) Bill
91	**Implemented** through the Criminal Procedure Act 2011
10, 45.3	**Implemented** in Harmful Communications [CAB Min (13) 10/5]
116	**Considered** by Cabinet in context of the Consumer Law Reform Bill [EGI Min (12) 16/5]
46	To be **considered** by Cabinet as part of policy matters arising from the review of NZSIS

	[CAB Min (13) 14.1]
83, 84 and 92.2	**Referred** to the LAC for its Guidelines, as agreed in **interim response**
Law Commission Privacy Recommendations (cont)	**How addressed**
4, 9, 15, 24, 34, 85, 92.1, 94, 95, 96, 98, 108, 113, 118, 120.2, 123, 124	The interim Government response **invited the Privacy Commissioner** to consult the Ministry of Justice and relevant partner agencies and submit a plan for developing the guidance and education material recommended by the Law Commission
116	**Transferred** to the Ministry of Business, Innovation and Enterprise
121	**Not for Government**
38, 39	**To be considered** in the Government response to 'new media, as agreed in **interim response**

Government response to Privacy Commissioner's recommendations from its review of the Privacy Act 1993: *Necessary and Desirable* and four supplementary reports

Recommendations	How addressed
4, 5, 6, 7, 7A, 8, 8A, 10, 12, 17A, 19A, 20, 21, 23, 23A, 24, 25, 25B, 26, 28, 28A, 29, 30, 31, 32, 33, 34, 34A, 35, 37B, 40, 41, 42, 44, 46A, 48, 49, 52, 56, 56A,58A, 65, 66, 71, 75, 75A, 79, 82, 82A, 83, 102A, 107A, 112, 117, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 131, 132, 133, 134, 135, 135A, 136, 137, 138, 148, 149, 154	**Overtaken** by Law Commission recommendations
1, 2, 3, 16, 17, 25A, 39, 39A, 43, 47, 53, 54, 55, 58, 60, 60A, 64, 68, 69, 69B, 70, 73, 74, 78, 80, 81A, 101, 101A, 101C, 101D, 101E, 101F, 102, 103, 104A, 107, 109, 110, 112A, 112B, 113, 115, 116A, 144, 145, 146, 147, 149A,153	**Agreed**
9, 37, 38, 113B, 114, 116, 118, 119, 130, 150	**Withdrawn** by Privacy Commissioner
19, 22, 36, 37A, 45, 46, 59, 61, 63, 113A, 113C	**Implemented** through the enactment of or amendment to other legislation
51, 81, 83A, 106, 108	**Referred** to (or addressed in) another work stream, **or** overtaken either by work in another work stream **or** overtaken by a MoJ recommendation **or** addressed through bid for baseline increase
11, 13, 14, 15, 50, 57, 62, 67, 69A, 72, 76, 77, 101B, 104, 105, 111, 151, 152	**Rejected**
18, 27, 67A, 84-100, 139-143	**Deferred**