In confidence

Office of the Minister of Justice

Cabinet Social Policy Committee

REFORMING THE PRIVACY ACT 1993

Proposal

1. This paper seeks Cabinet agreement to:

   1.1. policy decisions for a new Privacy Bill;

   1.2. increase funding for the Office of the Privacy Commissioner; and

   1.3. the attached supplementary Government Response to the Law Commission's review of the Privacy Act 1993.

Executive summary

2. 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 single individuals.

3. Since then information technology has developed significantly. Large amounts of data now can be stored, retrieved and transmitted digitally. This enables businesses and government to operate more efficiently and effectively in delivering services.

4. In this environment privacy breaches can impact many individuals, as has been seen by the significant data breaches which have occurred in the public, and to some extent, the private sectors. Consequently a regime more focused on early identification and prevention of privacy risks, rather than after the fact remedies, is required. This is the approach recommended by the Law Commission in its review titled Review of the Privacy Act (the Law Commission Report), and is consistent with international trends in privacy law.

5. Key proposals create stronger incentives for agencies to identify and prevent privacy risks, and give the Privacy Commissioner (the Commissioner) a stronger role through:

   5.1. mandatory reporting of data 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;

   5.2. enhanced own motion investigations – strengthening the Commissioner's existing own motion investigation 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

   5.3. compliance notices – the power to issue compliance notices for privacy breaches as a result of a complaint, own motion investigation, data breach notification or other avenue.

6. I am also proposing amendments that will:

   6.1. streamline the complaints resolution process to build trust in the system and increase efficiency and effectiveness;

   6.2. clarify the law and impose new obligations relating to cross-border flows of information to support New Zealand businesses to operate effectively internationally; and

   6.3. fix gaps in the privacy regime, clarify the law and make compliance easier for agencies.

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. The primary role of the Commissioner will remain to facilitate compliance and work with agencies.

8. 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, with one exception; other jurisdictions use large fines as an enforcement tool. Our penalty-related proposals are moderate by comparison.

9. In addition to these proposals, there have been other recent developments around improving privacy practice in the public sector in response to recent high profile breaches. Much of this work has been led by the Government Chief Information Officer (GCIO). At the end of 2013 Cabinet noted the GCIO's intention to establish a Government Chief Privacy Officer to provide privacy leadership across government.

10. 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. I recommend resourcing OPC:

    10.1. 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;

    10.2. to implement the Privacy Act reforms through further operational baseline increase of $1.190 million on-going from 2016/17, plus combined transitional costs from 2013/14 to 2015/16 of $0.738 in total.

Background

The current privacy framework

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

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

13. There are two main features of the Act. First, the Act generally requires agencies to handle personal information in accordance with 12 information privacy principles. The principles 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.

14. Second, 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.

15. However, the principal function of the Commissioner is to address privacy breaches through a complaints based system. Under this system, individuals who consider their privacy has been breached and have not been able to achieve a 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.

16. 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.

The Review of the Privacy Act 1993

17. The Ministry of Justice reviewed New Zealand's privacy framework. This work was informed by:

    17.1. the Law Commission's report;

    17.2. the Commissioner's report titled *Necessary and Desirable* (and subsequent supplementary reports). The recommendations have been included because the Law Commission recommended that both the Law Commission and the *Necessary and Desirable* recommendations are taken into account;

    17.3. recent actions to lift system level capability and performance in the management of personal information within the State sector; and

    17.4. international comparisons.

18. The Law Commission's report was the fourth and final stage of a privacy review that began in 2006. The report makes many recommendations to reform the Act. On 27 March 2012 the Government tabled its initial response which addressed 51 recommendations, and deferred the majority of the remaining recommendations for further analysis. The Government agreed to enact a new Privacy Act [SOC Min [12] 3/1].

19. The initial Government Response noted that a number of Law Commission recommendations were addressed by the Privacy Amendment Act 2013. This

Amendment Act introduced Part 9A to enable approved information sharing agreements to be entered into to facilitate public services.

20. The remaining Law Commission and *Necessary and Desirable* recommendations have now been analysed. Many recommendations are pragmatic solutions to address gaps in the law that have become apparent over the past 20 years, and to address the changing landscape for privacy.

21. In addition to the work by the Law Commission and the Commissioner, a range of actions have been taken to lift the State sector's performance in the management of personal information. This followed on from the GCIO Review of Publicly Accessible Information Systems and the subsequent GCIO-led work designed to improve privacy and security capability across the State sector [Cab Min (13) 6/2D refers]. These actions include the:

    21.1. establishment of an Information Privacy and Security Governance Group;

    21.2. work led by the Department of Internal Affairs on developing a system-wide view of information management, including privacy and security; and

    21.3. Privacy Leadership Forum that has developed practical resources to improve practice and build capability.

22. Cabinet has also recently agreed to establish a Government Chief Privacy Officer (GCPO). The GCPO will be responsible for privacy leadership across government including assurance and advice on privacy issues, support to agencies to meet their privacy responsibilities, and co-ordinated engagement with the Commissioner.

Problem definition

23. 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

24. 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.

25. 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.

26. 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 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).

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

    27.1. 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; and
        - ACC's "Pullar" breach in March 2012 involved 6,700 client records;

    27.2. 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;

    27.3. 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;

    27.4. a loss of public trust in agencies and how they secure and use personal information; and

    27.5. continuing breaches by agencies.

28. The costs of breaches are significant. There are costs to individuals such as financial losses, loss of dignity, emotional distress, time and cost associated with recovery efforts, and the opportunity for identity theft. There are also includes costs to agencies such as reputational damage, loss of client confidence, loss of clients, profit and stock market losses, and costs associated with consumer redress. Finally, there are the social and economic costs associated with people less willing to provide personal information.

29. 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.

Principles based approach

30. 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.

31. However, a consequence of retaining this flexibility is that the Act does not provide the certainty of "bright line" rules. The Law Commission's report 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."

32. 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.

Proposals to amend the privacy framework

33. Sound privacy law is good for people, business, and government. Individuals can have greater confidence that their information will be treated with respect, and the Government and businesses can have greater confidence in using and disclosing information efficiently and effectively to deliver services and grow the economy.

34. As the Commissioner has limited powers under the current compliance framework, breaches are common and there are few incentives for agencies to avoid future breaches. New Zealand needs a privacy regime that will enable the early identification and investigation of, and response to, systemic privacy risks.

35. I wish to preserve the best aspects of the current privacy framework, including a privacy regulator who can work constructively to conciliate disputes and help agencies improve their privacy systems. The Act's focus on complaints conciliation significantly reduces the volume of litigation that might otherwise reach the Human Rights Review Tribunal (the Tribunal).

36. I propose that the new Act should be sound, balanced privacy law so:

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

    36.2. 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.

37. These proposals will assist OPC to contribute to other Government initiatives, such as the Better Public Services programme, with associated significant investment in information technology. Agencies are expected to collaborate, share resources and eliminate silos. This transformation will include making better use of information. This introduces challenges for agencies to meet public and Government expectations for enhanced service delivery, while at the same time meeting public expectations for protection of personal information.

38. This package of reforms is consistent with international trends and revised OECD Privacy Guidelines (adopted in July 2013, replacing the 1980 Guidelines on which New Zealand's Privacy Act was based). Generally Canada, the United Kingdom and Australia either have broadly similar functions/powers in place, or will have in the near future. Implementing these proposals will add to New Zealand's reputation as a good place to do international business, and will contribute to economic growth and prosperity. The proposals will help ensure, for example, that New Zealand continues to enjoy its EU Adequacy status which is a major advantage to New Zealand business.

39. 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. This package of reforms is more moderate. I consider

that New Zealand should not consider imposing fines for privacy breaches until we have determined the impact of these reforms.

40. These proposals will enable the Commissioner to better identify and address emerging risks proportionately, clarify business obligations when private information is transferred across borders and streamline the complaints resolution process.

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

41. I propose mandatory breach notification, enhanced own motion investigations, compliance notices, and enhanced penalties for non-compliance, to ensure New Zealand has a privacy regime more focussed on early intervention and prevention of risks rather than after the fact remedies.

Mandatory data breach notification

42. I propose a two-tier regime for the notification of data breaches. Mandatory reporting of privacy breaches is critical for the Commissioner to become aware of, and begin to address, emerging issues prior to harm occurring.

43. Currently the Commissioner becomes aware of privacy breaches through voluntary notification, complaints and media reports. Voluntary breach notification results in inconsistent practices, and does not enable early identification of, and response to, the serious harm that can result from a privacy breach.

44. I am proposing the following two-tier notification regime:

    44.1. Tier one: agencies are required to take reasonable steps to notify the Commissioner of any material breaches as soon as reasonably practicable, taking into account: the sensitivity of the information; the number of people involved; and indications of a systemic problem.

    44.2. Tier two: this tier relates to more serious breaches. Agencies will be required to take reasonable steps to notify the Commissioner **and** affected individuals of breaches where there is a real risk of harm. This definition will hook into the current section 66 of the Act which defines 'interference with privacy' and is well understood. It includes actual or potential loss, injury, significant humiliation, or adverse effects on rights or benefits.

45. It will be up to the agency to determine whether a data breach meets the thresholds for mandatory reporting. There is no exception to the requirement to notify the Commissioner for either type of breach. Exceptions to the requirement to notify individuals include protecting trade secrets, security and vulnerable individuals.

46. For the Commissioner to become aware of privacy breaches and begin to address emerging issues prior to harm occurring, he or she needs to know that the breach has occurred. I propose that agencies that do not notify the Commissioner of breaches will be liable to a fine not exceeding $10,000 (a new offence). Agencies may also be liable for a breach of principle 5 (requirement to keep information secure) or principle 11 (limits on disclosure of information). I note that public sector agencies cannot currently be subjected to a fine under the Act and the proposed new fine will only apply to private sector agencies. I consider that the most effective deterrent for public sector agencies is 'naming and shaming.'

47. I have considered whether agencies that fail to notify the Commissioner of data breaches should be subject to a civil fine rather than creating a new criminal offence. I note that the Law Commission is doing some work on the use and design of civil pecuniary penalties and is reviewing the Crown Proceedings Act. I consider that the penalty for failing to notify the Commissioner of a breach should be a criminal offence as described above, in line with other offences in the Act, but this be reconsidered in light of the government response to the Law Commission's work.

48. In addition, I propose that the new Act should include a provision stating that the Commissioner will not publish the identities of agencies which notify breaches, unless the agencies consent or unless public notification is required in the public interest. This addresses an obvious disincentive to comply. I expect the Commissioner will also issue guidance on how notification should work.

49. I am aware that both the requirement to notify affected individuals and considering whether exceptions apply may impose some compliance costs on agencies, particularly where the breach is significant. I consider that costs are outweighed by the need for protection for individuals and long term benefits to agencies generally increased from public confidence in them.

International Comparisons – mandatory breach notifications

50. Mandatory notification of data breaches is now a common position in similar jurisdictions. The EU recently passed a regulation requiring telecommunication companies and ISPs to notify the 'supervisory authority' and the individuals affected. The EU draft data protection regulations, yet to be passed, would apply mandatory notification to other agencies. The UK is expected to soon follow. Australia and Canada have introduced federal Bills providing for mandatory notification. Some Canadian provinces have already amended their privacy laws to this effect. The revised OECD guidelines provide for breach notification to privacy enforcement authorities and adversely affected individuals.

Law Commission recommendation

51. The Law Commission recommended mandatory notification to affected individuals of serious breaches or where such notification will enable the individual to take steps to mitigate a real risk of significant harm (recommendations 67-79).

52. I prefer the two tier option outlined above because it would give the Commissioner a fuller picture of privacy risks across New Zealand and enable the identification of widespread problems before serious breaches occur.

Enhanced Own Motion Investigation Powers

53. I propose to enhance the Commissioner's existing own motion powers by increasing the penalty for non-compliance with requests for information from the Commissioner and allowing urgent requests to be made.

54. Currently the Commissioner can undertake an own motion inquiry into any matter if it appears to him or her 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 who does not comply with the Commissioner's requests commits an offence and is liable to a fine of $2,000.

55. I propose to enhance this existing power by:

    55.1. giving the Commissioner the discretion to decrease the 20 working days time frame for agency compliance; and

    55.2. increasing the penalty for offences for not complying with any requests for information from $2,000 to a maximum of $10,000.

56. The costs of conducting own motion inquiries will be met by the Commissioner (see financial implications section).

International Comparisons – audits and own motion investigations

57. This proposal is broadly comparable with international jurisdictions, but New Zealand will have a simpler and more consistent framework. By comparison, other jurisdictions operate a patchwork of own motion investigations and audits and (in some cases) 'advisory visits' that are applied differently depending on the type of agency (public/private, central/provincial).

Law Commission recommendation

58. The Law Commission recommended that the Commissioner should, for good reasons, be able to audit an agency (recommendations 64 and 65). I prefer enhancing the Commissioner's existing powers because:

    58.1. the proposal would reinforce the primary focus of the Commissioner to facilitate compliance through education, guidance and working with agencies, and for issues to be addressed at the lowest level;

    58.2. own motion inquiries are better able to focus on issues apparent across sectors, rather than focus on individual agencies; and

    58.3. if the Commissioner had the power to order audits at an agency's own expense, this could result in overuse of the power and under-reporting of privacy risks; if the cost is borne by the Commissioner then audits are not substantially different from own motion inquiries (the Law Commission was silent on funding).

The power to issue compliance notices for breaches of the Act

59. I propose that the Commissioner be able to issue compliance notices for breaches of the Act that come to his or her notice as the result of a complaint, an own motion investigation, a data breach notification, or from other avenues. Compliance notices will require an agency to do something, or to stop doing something, in accordance with the Act.

60. Currently the Commissioner can only make recommendations and has limited ability to act where wider concerns with systems or procedures are identified or where organisations are unwilling to comply.

61. There will be procedural safeguards, including natural justice, and the right to appeal to the Tribunal. There will also be statutory considerations to help ensure the compliance notice is proportionate, such as the number of people affected, any other possible means of securing compliance and the scale of investment required to comply with the notice. Compliance notices are enforceable in the Tribunal. Failure to comply with an order of the Tribunal will be dealt with in accordance with the provisions of the Human Rights Act.

International comparisons – compliance notices for a breach of the Act

62. All similar jurisdictions provide for compliance notices (by different names) which can be enforced through the Court; these apply to complaints and audits/investigations. Non-compliance can result in fines.

Law Commission recommendation

63. Consistent with my proposal, the Law Commission recommended that the Commissioner be able to issue compliance notices (recommendation 63).

Clarifying obligations when private information is transferred across borders

64. Technology advances since the Act was passed means that cross-border information flows, uncommon in 1993, now occur frequently. The Act does not comprehensively deal with cross-border information flows. As a result, New Zealanders have less consumer protection than citizens of other jurisdictions such as Europe, Canada and Australia. In situations where the Act does not apply, law, cost, or logistics may preclude an affected individual from seeking redress in the foreign country. My proposals aim to build trust in the system, support New Zealand businesses to operate effectively internationally, and take a balanced and proportionate approach to enforcement.

Cross-border outsourcing

65. I propose clarifying that an overseas service provider is an agent of the New Zealand agency when engaging in cross-border outsourcing. Cross-border outsourcing occurs when a New Zealand agency engages an overseas provider for storage or processing (examples include 'cloud computing' services and overseas call centres). This may involve sending personal information outside New Zealand or the overseas service provider accessing a New Zealand database.

66. Currently the Act generally treats an agency outsourcing information as still holding the information, and therefore accountable for it, but the New Zealand agency is not accountable where the overseas service provider uses the information for its own purposes (i.e. not the purpose for which the information was provided). This proposal clarifies that the New Zealand agency continues to be accountable for what happens to the information, and will be responsible for any privacy breaches by the overseas service provider. This clarification will help New Zealand agencies to assess the risks and benefits of outsourcing information for storage and processing, and give people more confidence that their information will be protected appropriately if it is outsourced overseas.

67. This proposal clarifies what is generally understood to be required by existing law, so there should be few, if any, costs for agencies already complying with these obligations. Any costs to agencies that are not already complying are outweighed by the proposal's benefits, which include promoting public confidence in the management of information outsourced overseas and enhancing remedies if information is mismanaged in offshore processing.

International Comparisons – cross-border outsourcing

68. This cross-border outsourcing proposal is consistent with the law in Canada, the UK and Australia. The EU directive and the revised OECD guidelines support this approach.

Law Commission recommendation

69. Consistent with my proposal, the Law Commission recommended that the Act be amended to clarify that an overseas service provider is an agent of the New Zealand agency (recommendation 107).

Cross-border disclosures

70. I propose a new privacy principle to require New Zealand agencies to take reasonable steps to ensure that information disclosed overseas will be subject to acceptable privacy standards in the foreign country.

71. Cross-border disclosures occur when a New Zealand agency discloses information to an agency from a different country, for that agency's own use. Currently any disclosure is authorised if:

    71.1. the disclosure is consistent with the purpose for which the information was obtained;

    71.2. the individual concerned authorises the disclosure; and

    71.3. other exceptions apply.

72. Once disclosed overseas, the information falls outside the Act's jurisdiction. The new privacy principle will give agencies considerable flexibility around what steps they take to ensure the acceptability of privacy standards in relevant foreign countries. Exceptions to the principle will include disclosures for the maintenance of the law, to avoid health and safety issues, and where expressly authorised by the individual concerned.

73. The Commissioner will be able to publish a list of overseas frameworks that constitute acceptable privacy standards. Guidance will be given on the types of steps that could be taken and on what constitutes acceptable privacy standards.

74. New Zealand agencies will be liable if they do not take reasonable steps to protect the information before it leaves their control (or do not establish that an exception to the principle applies). Agencies will not be liable for privacy breaches committed by the overseas agency in breach of any contractual measures or in reliance on foreign privacy laws.

75. Public confidence in cross-border information flows is essential for New Zealand's effective participation in global markets. This proposal will enhance access to justice for individuals, and encourage businesses to assess privacy risks before disclosing information overseas. While the new principle will create compliance costs for agencies, these are mitigated by the exceptions to the principle and the ability of the Commissioner to publish a list of acceptable overseas frameworks. I consider that the potential costs are justified in order to introduce greater protections for individuals.

International comparisons – information disclosures

76. Other jurisdictions already have similar provisions in place, with exceptions. The EU directive allows cross-border transfer of data only if there is an adequate level of protection, with some exceptions. Changes to strengthen Australia's cross-border disclosure principle come into force in March 2014. The revised OECD guidelines anticipate that States can require agencies disclosing data offshore to ensure the information is subject to adequate protection.

Law Commission recommendation

77. Consistent with my proposal, the Law Commission recommended that the Act be amended so that a New Zealand agency is required to take such steps as are reasonably necessary to ensure that the information will be subject to acceptable privacy standards in the foreign country (recommendations 110 to 112).

78. The Law Commission did not recommend an authorisation exception. The Law Commission considered it difficult to ensure such an exception would be understandable, efficient and cost-effective. I consider the proposed authorisation exception, based on new Australian provisions, is workable, and will help reduce compliance costs for businesses.

Streamlining the complaints resolution process to build trust in the system and increase efficiency and effectiveness

Access complaints

79. I propose streamlining 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.

80. I propose that the Commissioner be able to make enforceable decisions on access complaints about what information should be released and which withheld. Access decisions can be appealed to the Human Rights Review Tribunal (the Tribunal). This will streamline the complaints process to enable faster resolution.

81. Access complaints are complaints about an agency's decision not to give people access to their personal information. Currently, if the Commissioner cannot settle an access complaint an enforceable decision can only be obtained from the 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 concerns.

International comparisons – access complaints

82. The UK, Canada and Australia all provide for the privacy or information commissioners (at the relevant federal or state/provincial level) to investigate complaints about difficulty accessing personal information, and issue compliance notices, if necessary, or request a hearing through the courts.

Law Commission recommendation

83. Consistent with my proposal, the Law Commission recommended that the Commissioner be able to issue access determinations that are enforceable in the Tribunal (recommendations 56 to 59).

Referral to the Director of Human Rights Proceedings

84. If the Commissioner is unable to settle a complaint, the matter can be referred to the Director of Human Rights Proceedings (the Director) to determine whether proceedings should be filed in the Tribunal. The Law Commission considers that the current complaints resolution process results in duplication and delays, and recommended removing the Director's role from privacy complaints. Instead, the Commissioner would decide which cases should proceed to the Tribunal, act as the plaintiff in those cases, and perform the other privacy roles currently performed by the Director.

Preferred approach

85. I do not agree that the role of the Director should be removed in privacy cases, and consider that the Law Commission recommendation should be rejected. This is because:

    85.1. the primary conciliation role of the Commissioner would be maintained;

    85.2. the continued separation of compliance and litigation functions ensures that parties can freely engage in conciliation;

    85.3. prosecutorial resources and expertise will not need to be duplicated in OPC; and

    85.4. The majority of complaints are individuals complaining agencies have not provided access to their information. Under the proposed reforms, the Commissioner will be able to issue final decisions in such cases. This will have a far greater impact on streamlining the complaints process than implementing this recommendation.

The primary focus of the Commissioner on working with agencies is retained

86. As noted above, I wish to preserve the current focus of the Commissioner on working constructively with agencies to improve their privacy systems. This focus is a strength of the current framework, and will reduce the number and scale of privacy breaches, and any resulting harm that may occur from a breach.

87. The current focus on helping agencies to understand and fulfil their obligations is continued in a number of ways. The Law Commission made recommendations for increased guidance and education to improve understanding of the Act. The interim Government Response invited the Commissioner to consult the Ministry of Justice and other relevant agencies and submit a plan for developing the guidance and education material recommended by the Law Commission.

88. My proposals also contribute to this on-going focus. For example, reporting material breaches to the Commissioner will enable the Commissioner to work with agencies to ensure a more serious breach does not occur.

Additional proposals

New Offences

89. I am proposing to create the following two new offences. Both offences were recommended by the Law Commission because no there are no existing offences that cover the situations.

Misleading an agency

90. A new offence should be inserted into the new Act of misleading an agency by impersonating an individual or misrepresenting an authorisation from an individual in order to obtain that individual's personal information, or to have that information used, altered or destroyed.

91. This new offence will address the growing problem of 'pretexting', whereby individuals systematically mislead agencies to obtain personal information. While an affected individual may complain against the agency for disclosing the information, there is no sanction against the person who engaged in deception to obtain the information.

Destroying documents

92. A new offence should be inserted into the new Act of destroying documents containing personal information to which a person has sought access. In situations where the information has been destroyed, the complaints process is ineffective.

Intent element and level of penalty

93. Both new offences will contain an appropriate intent element, with the exact wording to be determined in consultation with Parliamentary Counsel Office during the drafting phase

94. I propose that these two new offences will incur a maximum fine upon conviction of $10,000. This is consistent with the proposal to increase the penalty for existing penalties to a maximum of $10,000.

Other proposals

95. I also propose to:

    95.1. include an express statement of full accountability for domestic outsourcing arrangements, as a parallel provision to cross-border outsourcing arrangements (implementing Law Commission recommendation 109);

    95.2. enable the Commissioner to share information with, provide assistance to, and co-operate with international counterparts (implementing Law Commission recommendation 114); and

    95.3. undertake further work to determine whether the APEC cross-border privacy system may provide a mechanism to increase benefits or reduce compliance costs (modifying Law Commission recommendation 115).

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

96. The main proposed changes will provide greater focus on early detection of privacy breaches, and give the Commissioner a greater enforcement role.

97. In addition to the main proposals, both the Law Commission Report and *Necessary and Desirable* recommended a range of changes to clarify the Act, give agencies more certainty and confidence in managing personal information and improve compliance.

98. Appendix One sets out the approach I propose to take to the less substantive recommendations from the Law Commission and *Necessary and Desirable*. I am also proposing one additional recommendation to place a duty on agencies and individuals to take reasonable steps to resolve their disputes.

Related Work

99. Cabinet has agreed to establish a Government Chief Privacy Officer (GCPO) in the Department of Internal Affairs to provide privacy leadership and lift privacy performance across State Services Agencies. Establishing the GCPO means there will be a stronger focus on privacy and security across government, and will enhance trust and confidence in the public sector. The roles of the GCPO and the Commissioner are complementary, and it is expected that the two agencies will work closely together to lift public sector performance in this area. Establishing the GCPO and the proposals to reform the Act both have financial implications. I have worked with the Ministers of State Services and Internal Affairs to ensure that both organisations are not funded to provide the same service.

Drafting instructions and further minor decisions

100. Inevitably during major law reform, issues will arise during the drafting stages which have not been considered by Cabinet. I propose that Cabinet authorise the Minister of Justice to make minor policy decisions within the overall framework approved by Cabinet. I expect my officials to consult if any minor policy decisions impact upon other agencies. If any major policy issues arise, I will seek Cabinet decisions in the normal way.

Consultation

101. The Law Commission consulted extensively during the development of its report with both public and private agencies. My proposals are broadly consistent with the Law Commission recommendations.

102. In addition, the Ministry discussed the key proposals in this paper with targeted representative private sector agencies: the Banker's Association, New Zealand Law Society, Marketing Association, Business New Zealand, Google, Trademe, Facebook, Netsafe, Telecom, Vodafone, Internet NZ, Consumer NZ, and New Zealand Medical Association.

103. The following agencies have been consulted on this paper: Accident Compensation Corporation, Ministries of Pacific Island Affairs, Primary Industries, Foreign Affairs and Trade, Education, Health, Culture and Heritage, Business, Innovation and Employment, Social Development, Environment, and Transport, Departments of Conservation, Corrections, and Internal Affairs, Inland Revenue, Crown Law Office, Civil Aviation Authority, Human Rights Commission, Office of Human Rights Proceedings, Housing New Zealand, Law Commission, New Zealand Security Intelligence Service, Government Communications Security Bureau, New Zealand Transport Agency, New Zealand Defence Force, Office of the Ombudsmen, Office of the Clerk of the House of Representatives, Parliamentary Service, New Zealand Police, State Services Commission, Serious Fraud Office, Statistics New Zealand, Treasury and Te Puni Kōkiri. The Department of the Prime Minister and Cabinet was informed of the contents of this paper.

104. Treasury supports updating the Privacy Act 1993 to reflect our more technologically driven, modern society. Treasury supports the policy proposals contained in this paper subject to funding acquired through the Budget 2014 process.

105. The Privacy Commissioner has also been consulted, and his comments have been incorporated. See below for additional comments.

106. I am also proposing to release an exposure draft as a means of addressing detailed implementation concerns prior to introduction of the Bill (see publicity section).

Comments from the Privacy Commissioner

107. I strongly support the Minister's proposals to implement the majority of the Law Commission's package of reforms for the Privacy Act. There is a need to move swiftly to make these recommendations law in New Zealand.

108. Targeted reform is necessary to meet international standards, to support responsible businesses, and to protect individuals in a complex global environment. The Law Commission's proposals are well consulted, moderate, and practical. Enacted as a package, they will provide regulatory tools to ensure the

law meets New Zealanders' expectations of protection and control of personal information in the digital age. They will also enable businesses to capture the benefits of modern IT with confidence.

109. There are a few matters on which my opinion differs from that of the Ministry of Justice. Brief details are set out here, and I am prepared to address these and other matters further if required.

An ability to audit is an important tool for a proactive and effective privacy regulator

110. As part of its package of reforms, the Law Commission recommended that OPC should have a moderate audit power. I agree with this recommendation, and believe it deserves inclusion in this legislation.

111. The power would enhance our effectiveness and credibility as a regulator, but could only be exercised for good reasons and with appropriate processes. It is increasingly common overseas (for example in the United Kingdom and Australia) for privacy commissioners to have a power to audit agencies.

The role of the Director of Human Rights Proceedings should be abolished for privacy proceedings

112. The Law Commission recommended that OPC should be able to bring cases directly to the Human Rights Review Tribunal, rather than cases having to go through a third party (the Director of Human Rights Proceedings). I agree.

113. This change would speed up and simplify the process both for individuals and for agencies, and would eliminate current duplication of effort and resources.

Agencies that fail to comply with mandatory data breach rules should face a civil fine rather than a criminal offence

114. The proposal in this paper would make it a criminal offence to fail to notify OPC of certain privacy breaches. While some penalty is required as part of a mandatory notification scheme, it is disproportionate to create a criminal offence. Instead, I recommend that the Human Rights Review Tribunal should have the ability to declare an agency in breach of the Act, and to fine it for its failure to notify. This would be a civil, not a criminal penalty.

115. In addition, under the current proposals a criminal offence would apply only to private sector agencies. Existing law states that public sector agencies cannot be criminally liable without an express legislative provision. There appears to be no good reason to create a distinction between the public sector and the private sector for failure to notify privacy breaches.

Financial implications

116. I propose that the funding for OPC is increased to allow it to effectively meet all of the functions we are asking it to undertake. This includes OPC's current role and the new functions as a result of these proposals, as discussed below.

OPC requires increased baseline funding to fulfil its current role

117. 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 his current role in these critical areas is limited due to increased demand for privacy services. OPC requires sustainable base level of funding.

118. OPC currently receives $3.2 million in Crown funding every year – this has not changed since 2007.

119. Over the last four years, demand for OPC services has significantly increased. Examples include complaints increasing by 36%; public enquiries by 54%, media enquiries have increased from 217 to 295 and privacy breach notifications rose from 3 to 107.

120. OPC can no longer rely on productivity improvements to balance its budget.

121. Dealing with the level of demand comes at the expense of OPC's ability to effectively carry out other functions which the Government needs. For example, OPC has no spare capacity to:

    121.1. respond to the GCIO review;

    121.2. assist agencies to reshape their privacy settings;

    121.3. assist with the development of transnational agreements; or

    121.4. review outdated codes of practice.

122. The Commissioner also does not have adequate resources to help the Government achieve its Better Public Service (BPS) priorities relating to:

    122.1. improving interactions with Government (result areas 9 and 10); or

    122.2. the IT platforms and sharing of information needed to support the achievement of other BPS targets to, for example, reduce child abuse, reduce offending, and increase educational achievement.

123. To provide for the OPC to contribute and operate effectively I recommend increased funding for existing functions as set out in section A of Table 1 below.

Additional OPC funding is required for the proposed new functions and information sharing agreement development

124. Once OPC is resourced to a sustainable base level, additional funding for new functions is required. Despite any increase in baseline funding OPC will not be able to absorb the additional transitional and ongoing costs associated with changes to the Act.

125. The proposals outlined in this paper for new OPC functions are necessary to deal with changes to the way information is managed as a result of technological change. This includes functions and changes to support New Zealand businesses to operate internationally.

126. The Privacy Amendment Act 2013 introduced a new mechanism to allow the sharing of personal information to facilitate public services (Approved Information Sharing Agreements). Providing guidance and assistance in the development of this new mechanism and the Commissioner's ongoing role in reviewing and monitoring agreements generates costs.

127. I recommend increased baseline and transitional funding for these costs as set out below.

	$ million				
	2013/14	**2014/15**	**2015/16**	**2016/17**	**2017/18 & outyears**
Ongoing operating costs – baseline increases					
A. Strengthening the Office					
Existing work	0.121	1.027	0.826	0.826	0.826
Better Public Services	0.121	0.644	0.644	0.644	0.644
Information-sharing agreements – Privacy Amendment Act 2013, including development and publication of guidance	0.095	0.252	0.252	0.252	0.252
Subtotal	0.336	1.923	1.722	1.722	1.722
B. New functions and transitional operating costs as a result of changes to the Privacy Act					
Proposed new functions			0.339	0.980	0.980
Development and publication of guidance etc	0.000	0.126	0.189	0.210	0.210
Cross-border compilation of approved jurisdictions list			0.084		
Subtotal	0.000	0.378	0.864	1.442	1.442
TOTAL COSTS (A+B)	**0.336**	**2.049**	**2.334**	**2.912**	**2.912**

128. There are three broad options for meeting these costs. Funding from justice sector baselines, funding from a levy system or cost recovery, or new funding. For the reasons set out below this paper recommends new funding.

129. The justice sector is currently facing cost pressures of almost a billion dollars out to 2020 and is working together to find ways of meeting those cost pressures.

130. Although the 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.

131. 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 activities that should be rightly funded by all of government.

132. If reprioritisation within the Justice Sector was required to meet these additional costs it is likely to require review and adjustments to front line services and programmes that address the drivers of crime. This would have to take place after the expenditure reviews for the sector agencies are complete, currently expected to be at the end of March 2014.

133. I have also explored the possibility of public and/or state sector contributions via either a levy system or cost recovery. Both mechanisms have significant disadvantages.

134. A levy would be impracticable because:

    134.1. the administration costs 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; and

    134.2. 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 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.

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

Costs on other agencies

136. Some agencies may face some costs implementing the requirements of the new Act. These are difficult to quantify, as discussed in the attached Regulatory Impact Statement, but are expected to result in longer-term savings.

Human rights

137. The policies contained in this paper appear to be consistent with the New Zealand Bill of Rights Act 1990 and the Human Rights Act 1993. A final determination of the consistency of the Bill with the New Zealand Bill of Rights Act will be possible once the Bill is drafted.

Legislative implications

138. These proposals will form the basis of a new Privacy Reform Bill, which will repeal and replace the Privacy Act 1993. The Privacy Bill has a priority of 5 (to be referred to a select committee in the year) on the 2014 Legislation Programme.

Regulatory impact analysis

139. The Regulatory Impact Analysis (RIA) requirements apply to the proposals in this paper and a Regulatory Impact Statement (RIS) is attached. The Regulatory Impact Analysis Team (RIAT) reviewed the RIS prepared by the Ministry of Justice and considers that the information and analysis summarised in the RIS meet the quality assurance criteria.

140. The RIS outlines the analysis conducted by the Law Commission in its review of the Privacy Act and also analyses alternative recommendations from officials. While the RIS does not provide detailed information on what the increased regulatory oversight arrangements mean for agencies' compliance costs, the process and consultation followed by the Law Commission suggest that the impacts compliance costs should not be major if guidance about technological implications is provided. There appears to be consensus that these impacts and the increased powers and resources for the Office of the Privacy Commissioner are proportionate to the benefits from increased clarity and certainty about privacy obligations.

Gender implications

141. There are no gender implications arising out of these proposals.

Disability perspective

142. There are no disability implications arising out of these proposals.

Publicity

143. I propose to issue an exposure draft of the new Bill for consultation with targeted private and public agencies, after Cabinet's agreement to the proposals but before the Bill is approved for introduction. I am also proposing to release the Cabinet paper and associated RIS before the exposure draft is released to enable those considering the exposure draft to understand the Government's objectives. It will add approximately three months to the timing of the Bill's introduction, but will help to identify unintended consequences (particularly for the private sector) and promote smooth implementation of the Bill. The exposure draft will not be an opportunity to challenge the key policy settings of the new Bill, which is the role of the select committee process.

Recommendations

144. The Minister of Justice recommends that the Committee:

Previous consideration

1. **note** that the Law Commission has reviewed the Privacy Act 1993 and released its report entitled *Review of the Privacy Act;*
2. **note** that it was agreed in the Initial Government Response, tabled on 21 March 2012 [SOC Min [12] 3/1 refers] that, inter alia:
   2.1 a new Privacy Act be enacted; and
   2.2 the majority of recommendations be deferred for further consideration;

Proposals to amend the privacy framework

3. **note** that information technology has developed significantly since the Privacy Act 1993 was introduced, which means that privacy breaches can now impact on large numbers of individuals;
4. **note** that sound privacy law means that people can have greater confidence that their information will be treated with respect, and government and business can have greater confidence in using and disclosing information to deliver services and grow the economy;
5. **note** that the package of reforms outlined below is designed to create sound, balanced privacy law so that:
   5.1 individuals have confidence that information shared with private and public sector agencies will be adequately protected; and
   5.2 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.
6. **note** that the package of reforms is consistent with international trends and revised OECD Privacy Guidelines;

7. **note** that the package of reforms is consistent with State sector actions to lift system level capability and performance in the management of personal information, including the proposal to establish a Chief Government Privacy Officer;

8. **note** that the availability of additional funding in Budget 2014 for the Office of the Privacy Commissioner will impact on whether it is practicable to proceed with the policy proposals for which agreement is sought in recommendations 10, 12, 15, 17, 19, 20, 23, 23, 27-29 and 31;

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

Mandatory data breach notification

9. **note** that currently the Commissioner becomes aware of data breaches through voluntary notification and media reports, which does not enable early identification of, and response to, any resulting harm;

10. **agree in principle,** subject to the availability of funding in Budget 2014, to the following two-tier notification regime for privacy breaches:

    10.1 tier one – agencies are required to take reasonable steps to notify the Commissioner of any material breaches, taking into account the following matters: the sensitivity of the information; the number of people involved; and indications of a systemic problem. There are no exceptions to this requirement;

    10.2 tier two - agencies will be required to take reasonable steps to notify the Commissioner **and** affected individuals of breaches where there is a real risk of harm;

    10.3 there are exceptions to notifying individuals of tier two breaches, including protecting trade secrets, security and vulnerable individuals;

    10.4 agencies that do not notify the Commissioner of tier one or tier two breaches will be liable to a fine not exceeding $10,000;

    10.5 agencies may also be liable for a breach of principle 5 (requirement to keep information secure) or principle 11 (limits on disclosure of information);

    10.6 the Commissioner will not publish the identities of agencies that notify breaches, unless the agencies consent or public notification is required in the public interest;

Enhanced own motion investigation powers

11. **note** that currently the Commissioner has powers to undertake an own motion inquiry if it appears that an individual's privacy is being, or may be, infringed;

12. **agree in principle,** subject to the availability of funding in Budget 2014, to enhance the existing powers by:

    12.1 giving the Commissioner discretion to decrease the 20 day time frame for agency compliance with the Commissioner's evidence powers for both own motion inquiries and complaint investigations; and

    12.2 increasing the penalty for offences for not complying with any requests for information to a maximum of $10,000;

13. **note** that the costs of conducting own motion inquiries will be met by the Commissioner;

Compliance notices

14. **note** that currently the Commissioner can only make recommendations and has limited ability to act where wider concerns with systems or procedures are identified, or where organisations are unwilling to comply;

15. **agree in principle,** subject to the availability of funding in Budget 2014, and subject to procedural safeguards and statutory considerations, that the Commissioner be able to issue compliance notices for breaches of the Act;

Clarifying business obligations when private information is transferred across borders

Cross-border outsourcing

16. **note** that cross-border outsourcing occurs when a New Zealand agency sends personal information to an overseas provider for storage and processing (examples include 'cloud computing' services and overseas call centres);

17. **agree in principle,** subject to the availability of funding in Budget 2014, that the new Act will clarify that an overseas service provider is an agent of the New Zealand agency when engaging in cross-border outsourcing;

Cross-border disclosure

18. **note** that once a New Zealand agency has disclosed information overseas, the information falls outside the current Act's jurisdiction;

19. **agree in principle,** subject to the availability of funding in Budget 2014, that**:**

    19.1 the new Act contain a new privacy principle that will require New Zealand agencies to take reasonable steps to ensure that information disclosed overseas will be subject to acceptable privacy standards;

    19.2 exceptions to the principle will include disclosures for the maintenance of the law, to avoid health and safety issues, and where expressly authorised by the individual concerned;

20. **agree in principle,** subject to the availability of funding in Budget 2014, that the:

    20.1 Commissioner can publish a list of overseas frameworks that constitute acceptable privacy standards; and

    20.2 new Act will provide guidance on the types of steps that could be taken and on what constitutes acceptable privacy standards;

Streamlining the complaints resolution system so that it is efficient and effective

Access complaints

21. **note** that if the Commissioner cannot settle complaints about an agency's decision on access to a person's own information, an enforceable decision can only be obtained from the Human Rights Review Tribunal;

22. **note** that Tribunal proceedings are adversarial and court-like, and it is not an appropriate forum for resolving access complaints;

23. **agree in principle,** subject to the availability of funding in Budget 2014, that the Commissioner be able to make enforceable decisions on access complaints to streamline the process and enable faster complaint resolution;

Role of the Director of Human Rights Proceedings

24. **note** that if the Commissioner cannot settle a complaint, the matter can be referred to the Director to determine whether proceedings should be filed in the Tribunal;

25. **note** that the Law Commission recommended removing the Director's role from privacy complaints and giving it to the Commissioner in order to remove duplication and delays;

26. **note** that the role of the Director should not be removed in privacy cases because:

    26.1 the primary conciliation role of the Commissioner would be maintained;

    26.2 the continued separation of compliance and litigation functions ensures that parties can freely engage in conciliation;

    26.3 prosecutorial resources and expertise will not need to be duplicated in OPC; and

    26.4 the proposal relating to access complaints will have a far greater impact on streamlining the complaints process that removing the role of the Director;

Other proposals

27. **agree in principle,** subject to the availability of funding in Budget 2014, that the new Act will contain two new offences of misleading an agency and destroying documents containing information to which a person has sought access, which will incur a maximum fine upon conviction of $10,000;

28. **agree in principle,** subject to the availability of funding in Budget 2014, that the new Act will include an express statement of full accountability for domestic outsourcing arrangements;

29. **agree in principle,** subject to the availability of funding in Budget 2014, that the new Act will enable the Commission to share information with, provide assistance to, and co-operate with international counterparts;

30. **note** that Appendix One sets out a range of less substantial and minor and technical recommendations that seek to modernise and clarify privacy law;

31. **agree in principle,** subject to the availability of funding in Budget 2014, to the approach set out in Appendix One for addressing the less substantive recommendations to amend the current Act;

32. **agree** that the Minister of Justice be authorised to make additional minor policy decisions within the overall framework approved by Cabinet, but any major policy issues will be subject to further Cabinet consideration;

33. **note** that my officials will consult on any additional proposals that may impact upon other agencies;

34. **note** that the Minister of Justice will issue an exposure draft of the new Bill for consultation with targeted private and public agencies, after Cabinet's agreement to the proposals but before the Bill is tabled in Parliament;

Financial implications

A) Strengthening the Office of the Privacy Commissioner

35. **note** that the Office of the Privacy Commissioner is under financial pressure despite significant recent productivity improvements, and the Office must be resourced to a sustainable base level to enable it to respond to increases in demand, while fulfilling all current expectations of the Office and taking a more active role in the Better Public Services programme;

36. **note** that decisions with respect to information-sharing agreements were previously agreed in SOC Min (12) 3/1 on 21 March 2012 and implemented through the Privacy Amendment Act 2013;

37. **note** the Minister of Justice has requested the following funding for strengthening the Office of the Privacy Commissioner as part of Budget 2014:

	$ million				
	2013/14	**2014/15**	**2015/16**	**2016/17**	**2017/18 & outyears**
Ongoing operating costs – baseline increases					
Strengthening the Office					
Existing work	0.121	1.027	0.826	0.826	0.826
Better Public Services	0.121	0.644	0.644	0.644	0.644
Information-sharing agreements – Privacy Amendment Act 2013	0.095	0.252	0.252	0.252	0.252
Total	0.336	1.923	1.722	1.722	1.722

B) Implications of updates to the Privacy Act 1993

38. **note** the Minister of Justice has requested the following funding to update the Privacy Act 1993 and deliver the expanded functions of the Office of the Privacy Commissioner as part of Budget 2014:

	$ million			
	2014/15	**2015/16**	**2016/17**	**2017/18 & outyears**
Ongoing operating costs – baseline increases				
New functions and transitional operating costs as a result of changes to the Privacy Act				
Proposed new functions		0.339	0.980	0.980
Development and publication of guidance etc	0.126	0.189	0.210	0.210
Cross-border compilation of approved jurisdictions list		0.084		
Total	0.126	0.612	1.190	1.190

39. **invite** the Minister of Justice to:

    39.1 issue drafting instructions to give effect to the above recommendations, subject to the availability of funding in Budget 2014; and

    39.2 present to the House of Representatives the Supplementary Government Response to the Law Commission report on *Review of the Privacy Act 1993* attached as Appendix Two.

Hon Judith Collins
Minister of Justice

Date signed: _____/_____/_____

Attachments: Appendix One – Less Substantive Recommendations
Supplementary Government Response