In Confidence
Office of the Minister of Justice

Chair
Cabinet Business Committee

PRIVACY BILL 2018 – APPROVAL FOR INTRODUCTION AND ADDITIONAL POLICY DECISIONS

Proposal

1. This paper seeks approval for the introduction of the Privacy Bill 2018 (the Bill). It also seeks Cabinet confirmation of additional policy decisions I have made that are reflected in the Bill.

Executive summary

2. The Privacy Act 1993 regulates the collection, use and disclosure of information about individuals. The Act's framework centres on 12 information privacy principles, which seek to protect people's privacy while also accommodating legitimate information use by government, businesses and other organisations.

3. The Privacy Act has now been in operation for 25 years. Over that time, technology has revolutionised the way personal information is collected, stored, shared and used. The Act's complaints regime, designed primarily to address individual interferences with privacy, has been rendered deficient in an age where privacy breaches can affect multitudes of people.

4. The Law Commission's 2011 *Review of the Privacy Act* (the Law Commission report) called for the Privacy Act to be repealed and replaced with a modernised law. The Privacy Bill, which implements most of the Law Commission's recommendations, is now ready for introduction. It incorporates key changes into New Zealand's privacy framework such as mandating reporting of data breaches, strengthening cross-border data flow protections, and empowering the Commissioner to issue compliance notices and access directions.

5. Some minor additional matters have been included in the Bill at my direction, and require Cabinet approval. These include:

    5.1. a purpose statement that focuses more strongly on promoting and protecting privacy, rather than balancing privacy against social and business objectives

    5.2. a single, clear threshold for notifying a privacy breach

    5.3. addressing two problems that have emerged with Approved Information Sharing Agreements (AISAs)

    5.4. two changes to the law enforcement information schedule

    5.5. retiring information matching agreements, which are outdated, and

    5.6. achieving consistency in the penalties across the Bill for like offences.

Background

The Privacy Act 1993

6. The collection, use and sharing of personal information in New Zealand is governed by the Privacy Act. It seeks to ensure that people's privacy is protected, while also accommodating legitimate information use. Twelve information privacy principles are at the core of the Act. The principles establish a framework for handling personal information at all points of its lifecycle, from collection to destruction.

7. The Act sets up a complaints system. If a person considers that a privacy breach has caused them harm, they can complain to the Privacy Commissioner. The Commissioner attempts to resolve the dispute. If it is not resolved, the individual may take the complaint to the Human Rights Review Tribunal.

Need for reform

8. Over the last twenty years, information technology has developed significantly. We are collecting, storing and disclosing more personal information than ever before using social media, e-commerce, internet-connected devices, cloud storage and other new technologies. Personal information can be easily distributed around the world and large quantities of data are readily stored, retrieved and disclosed.

9. This creates potential benefits for everyone, but also new challenges for protecting personal information. Today, privacy breaches can impact very many people. Consequently, a regime that is focused on early identification and prevention of privacy risks rather than after-the-fact remedies is required. This approach was recommended by the Law Commission report, and is consistent with international trends in privacy law.

10. The Law Commission report called for the Privacy Act to be repealed and replaced with a modernised law that would reflect changes in the handling of personal information since 1993. The previous Government accepted most of the recommendations [CAB Min (14) 10/5A]. It prioritised the Law Commission's recommendation for a new framework to allow personal information to be shared between government agencies, and AISAs were added to the Privacy Act in 2013. In 2016, Cabinet agreed that the Bill should also regulate the downstream use of de-identified personal information by agencies, and clarified some drafting issues [CAB Min (16) 0047].

The Privacy Bill

11. The Bill implements Law Commission recommendations, and previous recommendations from the Privacy Commissioner's 1998 *Necessary and Desirable* report (and subsequent supplementary reports). As recommended by the Law Commission, it retains a principles-based approach to privacy law but increases accountability mechanisms.

12. The Bill supports early identification of systemic privacy risks and gives the Privacy Commissioner a stronger role. The key changes are listed below.

    12.1. *Mandatory reporting of data breaches*: privacy breaches that pose a risk of harm to people must be notified to the Commissioner and to affected individuals.

12.2. *Compliance notices*: The Commissioner will be able to issue compliance notices to require an agency to do something, or stop doing something. The Human Rights Review Tribunal can enforce compliance notices and hear appeals.

12.3. *Strengthening cross-border data flow protections*: New Zealand agencies (the name used for any entity handling personal information) will be required to take reasonable steps to ensure that personal information disclosed overseas is subject to acceptable privacy standards. The Bill also clarifies the application of our law when a New Zealand agency engages an overseas service provider.

12.4. *New criminal offences*: It will be an offence to mislead an agency and to destroy documents containing personal information where a request has been made for it. The proposed penalty is a fine not exceeding $10,000.

12.5. *Commissioner making binding decisions on access requests*: The Commissioner will make decisions on complaints relating to access to information, rather than the Human Rights Review Tribunal. The Commissioner's decisions can be appealed to the Tribunal.

12.6. *Strengthening the Privacy Commissioner's information gathering powers*: The Commissioner's existing investigation power is strengthened by allowing him or her to shorten the timeframe in which an agency must comply, and increasing the penalty for non-compliance.

13. The changes will better align New Zealand's privacy law with international developments, such as the 2013 OECD Privacy Guidelines and the European Union's forthcoming General Data Protection Regulation.

Some aspects of the Bill require policy approval

14. I seek approval for some additional matters which have been included in the Bill at my direction, in accordance with authority granted by Cabinet [CAB Min (14) 10/5A]. These changes respond to departmental feedback, build on the public sector's experience of information sharing, and achieve consistency in the Bill's penalties.

A more privacy-focused purpose statement

15. The current Privacy Act contains a long title, which the Law Commission's 2011 report recommended replacing with a section stating that the purposes of the Act be to "promote and protect privacy of personal information, subject to exceptions and exemptions which recognise other rights and interests that will sometimes override privacy".

16. The previous government agreed that the Bill's purpose section should build on the Law Commission's suggestions, but also focus on balancing privacy with important social and business interests [CAB Min (14) 10/5A].

17. I do not favour this approach. The purpose section of any enactment is central to its interpretation, so it is important that it fairly and accurately describes the overriding object of the Bill. As such, I think it should contain a clearer focus on protecting and promoting individual privacy. At my direction, the Bill's purpose statement has been redrafted to more closely align with the current Act's long title and the Law

Commission's original recommendation to "promote and protect privacy of personal information".

Prescribing a clear threshold for notifying a data breach

18. I am proposing some changes to the Bill's mandatory breach notification requirements. In 2014, Cabinet agreed to introduce the following two-tier regime for breach notification.

    Tier One: agencies would be required to take reasonable steps to notify the Commissioner of any material breaches taking into account the sensitivity of the information, the number of people involved, and indications of a systemic problem.

    Tier Two: where there is a real risk of harm, agencies would be required to take reasonable steps to notify the Commissioner and affected individuals.

19. The agency would determine whether a breach meets one or the other of these thresholds for mandatory reporting. Failure to comply with the Bill's mandatory notification requirements would be an offence, punishable by a fine of up to $10,000.

20. The Law Commission did not recommend a two-tier approach in its 2011 report, although it did identify a range of factors that could lead to a breach being considered serious. Cabinet decided on a two-tier approach on the basis that this would give the Commissioner a fuller picture of privacy risks across New Zealand, and enable the identification of widespread problems before serious breaches occur.

21. Since this decision was made, Australia and Canada have introduced mandatory breach notification regimes. Both of these jurisdictions take a single tier approach, where the same threshold applies for notification of breaches to both the relevant regulatory body and affected individuals.

22. When government departments were consulted on the draft Bill, thirteen raised concerns about the thresholds for mandatory reporting. Their concerns included that:

    - it is not clear what "sensitive" means
    - the number of people affected might not be immediately known
    - whether a breach has resulted from a "systemic problem" is a matter for investigation and discussion with the Privacy Commissioner – it will not always be immediately known by the agency in question, and
    - uncertainty about whether breaches are material or serious will cause many agencies to request that the Privacy Commissioner decide. This will increase his workload, and consequently decrease his ability to focus resources on preventing serious breaches.

23. I share these concerns. To be effective, the mandatory breach reporting regime must be understandable for all agencies, inside and outside of government. It is also important that people are informed about any risk of harm. I therefore propose to simplify the threshold for notification to a single threshold. Mandatory breach reporting will apply when there is a risk that the breach will cause harm (as already defined in the Privacy Act and Bill). In this case, agencies will be required to notify the Commissioner and affected individuals of the breach.

Changes to address issues with Approved Information Sharing Agreements (AISAs)

24. AISAs allow agencies to share personal information to facilitate the provision of public services. They are approved by Order in Council. Five years have passed since AISAs were introduced, and some minor issues have emerged which I consider should be addressed through this Bill.

25. I am also aware that there is more general concern from some agencies about the time and resource it takes to develop AISAs. The Ministry of Justice will continue to monitor this area as more AISAs are put in place, and report to me if issues arise.

Removing the concept of representative parties from the AISA mechanism

26. The Privacy Act allows an agency to "represent the interests" of a class of agencies when entering into an AISA. This provision was intended to provide an easy way to add parties to an AISA if the agency to be added was of the same type as one already party to it. For example, this would enable small NGOs to be included without the need for a new Order in Council.

27. But the Act does not clearly state the responsibilities of representative parties, and as such, agencies have been reluctant to take on this role. For example, during the development of the Children's Action Plan AISA, an NGO umbrella body was reluctant to act as a representative party because it did not know what obligations that would involve.

28. I therefore propose to remove the concept of 'representative parties' and instead allow an AISA to list the classes of agency to which it can apply, regardless of whether one of that type is an original party to the AISA. Agencies that fall within a listed class could then be added by the lead agency. This change will achieve the original intent of the provision. The suite of safeguards for making an AISA (including consultation with the Privacy Commissioner, regular reporting and the list of matters of which a Minister must be satisfied before recommending an Order in Council) will remain unchanged.

Extending the ability to act as a lead agency for an AISA to certain crown agents

29. Every AISA must have a lead agency, whose responsibilities include reporting on the operation of the agreement. Currently, the lead agency must be a government department, NZ Police or the Transport Agency. This is problematic when another Crown Agent is the most logical lead agency. Other Crown Agents have significant roles within the state sector and it is inefficient to have to find another agency to sponsor an AISA. I therefore propose that the ability to act as a lead agency for the purposes of an AISA be extended to include the following Crown Agents:

- Accident Compensation Corporation
- Civil Aviation Authority of New Zealand
- All District Health Boards
- Earthquake Commission
- Education New Zealand
- Fire and Emergency New Zealand
- Housing New Zealand Corporation
- New Zealand Qualifications Authority
- Tertiary Education Commission
- WorkSafe New Zealand

Law enforcement information sharing

30. Schedule 5 of the Privacy Act (and the Bill) authorises the sharing of listed law enforcement information, including some court information. The focus of the schedule is sharing the information necessary to keep the justice system working. The schedule has its origins in the Wanganui Computer system, and was carried over to the Privacy Act 1993 with an Order in Council amendment mechanism (but with a sunset clause that expired in 1998). I consider two updates to the schedule, which remains an important mechanism for sharing law enforcement information, would be worthwhile.

Clarifying the relationship with the Senior Courts Act 2016 and the District Court Act 2016

31. The Senior Courts Act 2016 and the District Court Act 2016 establish a scheme for determining access to different types of court information, which now needs to be reflected in New Zealand's privacy regime. I propose an amendment to clarify the interface between the courts legislation and Schedule 5 of the Bill.

32. The two Courts Acts define 'court information' (information under the control of the judiciary, but held by the Ministry of Justice) and 'Ministry information' (information held by the Ministry of Justice as a member of the Executive branch of Government). The Courts Acts also set out the mechanisms to enable court information and Ministry information to be shared with other agencies.[1]

33. The proposed amendment to the Privacy Bill will make it clear that despite the provisions in the Senior Courts Act and the District Court Act, court information that is already in the schedule can continue to be shared. This will enable the existing arrangements to continue under clear authority. I consider it important not to disrupt these, because they cover important transactions such as employment-related criminal information checks.

Order in Council mechanism to amend the law enforcement schedule

34. I propose reinstating the ability to amend Schedule 5 by Order in Council, where the proposed change does not involve sharing court information. The Order in Council would need to be made on advice of the responsible Minister, after consultation with the Privacy Commissioner. The ability to amend the Schedule by Order in Council will enable it to be kept up to date without the need for further primary legislation.

35. This proposal would create a 'Henry VIII' clause, as it will allow regulation to amend legislation. In my view a Henry VIII clause is appropriate in this limited instance, as it will allow Schedule 5 to more readily respond to changes in technology, agency names and functions, and law enforcement priorities. Schedule 5 is narrowly focused on information sharing needed for the administration of justice. Mandatory consultation and the prescriptive nature of Schedule 5, which lists the specific information that can be shared, mean that the Order in Council mechanism will be used appropriately.

36. Sharing arrangements which involve court information will not be able to be amended or authorised by Order in Council. This recognises that court information should remain under the supervision of the court, except in the circumstances authorised under courts legislation.

---

[1] Court information may be shared via an Approved Information Sharing Agreement only if it is a specified type of court information, called 'permitted information'. Ministry information can be shared in accordance with relevant legislation, for example the Official Information Act and the Privacy Act.

Retiring Information Matching Programmes

37. Information matching involves comparing one set of information with another, to find data that relates to the same person. Under the Act, information matching programmes must be individually authorised by their own Act of Parliament. Matching must be carried out in accordance with an agreement that complies with rules in the Privacy Act and is approved by the Privacy Commissioner. The Act imposes relatively onerous reporting requirements.

38. Technology has moved on since the information matching provisions were introduced and they are now outmoded. Information matching is a type of information sharing, and information matching programmes can now be authorised using AISAs.

39. I therefore propose that no new information matching programmes should be authorised after the Privacy Bill is enacted. To avoid unnecessary disruption, existing programmes are preserved in the Bill and can continue to operate. Agencies will transition to AISAs over time as their priorities determine.

Consistency of penalties

40. Cabinet has agreed to increase the maximum fine available for two existing offences in the Privacy Act from $2,000 to $10,000, namely:

    40.1. obstructing, hindering or resisting (without reasonable excuse) the Privacy Commissioner or any other person in the exercise of their powers under the Act, and

    40.2. refusing or failing to comply with any lawful requirement of the Commissioner or any other person under the Act.

41. The change was part of strengthening the Privacy Commissioner's information-gathering powers and aligned with the maximum penalty proposed for the new offences that Cabinet agreed be included in the Bill, such as:

    41.1. failure to notify the Commissioner of a material breach

    41.2. impersonating an individual to get access to, or change, their personal information, and

    41.3. destroying any document containing personal information knowing that a request has been made in respect of that information.

42. Other offences have been carried over to the Bill, but the maximum fines which relate to those offences were not increased, and therefore remain at $2,000. These include:

    42.1. making any statement, or giving any information to the Commissioner or any other person exercising powers under this Act, knowing that the statement or information is false or misleading, and

    42.2. an individual representing directly or indirectly that he or she holds any authority under this Act when he or she does not hold that authority.

43. The potential harm from the worst instances of these offences is similar to that for the other offences in the Bill, and I propose setting the maximum fine at the same level of $10,000.

44. The Bill also sets out offences for failing to comply with a Human Rights Review Tribunal order that an agency comply with a compliance notice or an access direction issued by the

Commissioner. It is already an offence under the Human Rights Act 1993 for a person to fail to comply with a Tribunal order, punishable by a fine of up to $5,000.

45. Failing to comply with a Tribunal order is just as serious as failing to comply with the other requirements in the Act that are listed above. I therefore propose that the same maximum fine of $10,000 should apply. The penalty level for failing to comply with a Tribunal order in the Human Rights Act could be reconsidered if that Act is reviewed in the future.

Regulation of re-identification of personal information

46. In 2016, Cabinet agreed to introduce a new Information Privacy Principle that would regulate the inadvertent or deliberate use of re-identified data by agencies [CAB-16-MIN-0047]. This was to reduce the risk of individuals being re-identified at a later date.

47. However, following that Cabinet decision, the former responsible Minister tasked the Data Futures Partnership (DFP) with exploring a range of issues associated with the risk of re-identification. Work on a new Information Privacy Principle was put on hold, pending the outcome of that work. The DFP produced interim advice in July 2017 that recommended a systems approach to the risks and benefits of re-identification and other privacy threats.

48. The contracts for members of the DFP's working group expired before it produced a final report. As such, the Bill for introduction does not include a new Information Privacy Principle regulating the re-identification of personal information.

49. A very small number of less substantive Law Commission recommendations that were agreed by Cabinet have also not yet been included in the Bill due to drafting challenges and concern about potential unintended consequences. An example is the Law Commission's recommendation that Information Privacy Principle 1 be amended to provide that individuals should be able to interact with agencies anonymously or under a pseudonym, where it is lawful and practicable to do so. Justice officials will continue to work on those recommendations as the Bill progresses through the House.

The Privacy Commissioner's section 26 report

50. In December 2016, the Privacy Commissioner issued a report under section 26 of the Privacy Act, which requires the Commissioner to review the operation of the Act every five years. In this report, the Commissioner recommended that the following six measures be included into the Privacy Bill:

    50.1. new civil penalties for serious or repeated breaches of the Privacy Act

    50.2. empowering the Privacy Commissioner to require agencies to demonstrate their ongoing compliance with the Privacy Act by submitting a privacy management programme

    50.3. introducing controls on the risk of individuals being identified from data that has been de-identified (otherwise known as re-identification)

    50.4. introducing a new right to personal information portability to enable users to easily transfer data between different service providers

    50.5. reform of public register provisions in the Act, including enhancement of the ability to supress personal information from public registers, and

    50.6. making obstruction of the Privacy Commissioner a strict liability offence.

51. I do not wish to further delay the worthwhile reforms in the Privacy Bill to complete further policy work and consultation on these proposals. Change to implement the Law Commission's recommendations is overdue. The current Act is falling behind international developments and no longer affords New Zealanders the level of privacy protection enjoyed in comparable countries.

52. Privacy is an evolving area and I anticipate some of the Privacy Commissioner's recommendations may be suitable for a future privacy reform. The Privacy Commissioner may decide to submit to the Justice Committee on these issues, and the House will consider any recommendations for amendments to the Bill that the Committee makes.

Regulatory impact analysis

53. A Regulatory Impact Statement (RIS) for the Privacy Bill was prepared in accordance with Cabinet requirements and was submitted to Cabinet along with the paper seeking policy approvals in March 2014 [CAB Min (14) 10/5A].

54. Additional policy decisions were made in February 2016. A Regulatory Impact Statement (RIS) for these additional decisions was prepared in accordance with Cabinet requirements and was submitted to Cabinet in February 2016 [CAB Min (16) 0047].

55. The Regulatory Quality Team at Treasury has advised that regulatory impact analysis is not required for the proposals discussed above as they have no or only minor impacts on businesses, individuals or not-for-profit entities.

Compliance

56. The Bill complies with the following:

    56.1. the principles of the Treaty of Waitangi

    56.2. the rights and freedoms contained in the New Zealand Bill of Rights Act 1990 and the Human Rights Act 1993

    56.3. the disclosure statement requirements (a disclosure statement prepared by the Ministry of Justice is attached)

    56.4. relevant international standards and obligations, and

    56.5. the LAC *Guidelines on the Process and Content of Legislation* (2014 edition), which are maintained by the Legislation Design and Advisory Committee.

57. Crown Law is undertaking an assessment of whether the Bill is consistent with the Bill of Rights Act and will provide advice to the Attorney-General. Advice provided to the Attorney-General is generally expected to be available on the Ministry of Justice's website upon the Bill's introduction.

58. The Bill will repeal and replace the Privacy Act 1993. The changes will enhance the powers of the Privacy Commissioner (including identification of privacy risks) and individual privacy rights. The changes also support agency compliance with the Act.

Consultation

59. The following departments, agencies and crown entities have been consulted on this paper and the Privacy Bill:

Treasury, State Services Commission, Social Investment Agency, Stats NZ, Ministries for the Environment, Health, Defence, Education, Transport, Business, Innovation and Employment, Foreign Affairs and Trade, Pacific Peoples, Social Development, Environment, Culture and Heritage, Departments of Prime Minister and Cabinet, Internal Affairs, Corrections, Inland Revenue, Conservation, Land Information New Zealand, Inspector-General of Intelligence and Security, Police, Parliamentary Counsel, Primary Industries, Te Puni Kōkiri, Oranga Tamariki, Security Intelligence Service, Government Communications Security Bureau, Customs, Serious Fraud Office, Crown Law, Reserve Bank, New Zealand Transport Agency, Civil Aviation Authority, Human Rights Commission, Housing New Zealand, Maritime New Zealand, Accident Compensation Corporation, Government Chief Privacy Officer and the Office of the Privacy Commissioner.

60. The agencies consulted support the intent and overall direction of the Privacy Bill. Outstanding technical and drafting issues they have raised will be worked through as the Bill progresses through the Select Committee process.

61. The Privacy Commissioner has provided the following comment:

The Privacy Commissioner welcomes the introduction of the Privacy Bill to implement reforms recommended by the Law Commission and to maintain New Zealand's strong track record of protecting the privacy interests of individuals.

While the Commissioner is broadly supportive of the additional policy matters included in this paper, he considers that some policy issues still need to be worked through. For example, the Commissioner is concerned that the proposed criminal sanction for agencies to enforce the new privacy breach notification provisions may be counter-productive. Criminal offences are a blunt tool that will incentivise over-reporting by agencies, creating inefficient regulation and diluting the benefits of the policy. In contrast, he considers that further improvements to the regulatory toolbox to enforce compliance, such as seeking the imposition of civil penalties, have not been included.

The Commissioner will submit to the Justice Select Committee on certain aspects of the Bill that he considers need redrafting to effectively carry over key provisions of the current Privacy Act. It is important for industry to maintain the continuity of the Act's provisions that are not being reformed. Some of the current drafting changes for modernisation have the potential to create unnecessary compliance costs for users of the legislation and are inefficient for industry investing in adapting to the updated law. For example, central provisions in the Privacy Act relating to individuals' rights to seek access and correction of personal information are currently working well, but have been overhauled to an extent that creates overlap and complexity in the Bill.

The Commissioner will also submit that he continues to support the Law Commission recommendation to shift the privacy functions of the Director of Human Rights Proceedings into the Privacy Commissioner's office in order to streamline the handling of privacy complaints.

62. The New Zealand First and Green parties have been consulted.

Financial implications

63. The additional policy proposals in this paper are fiscally neutral. Contingency funding has already been set aside to support the Office of the Privacy Commissioner in its new

functions under the privacy reforms [CAB Min (14) 13/8 (18)]. The tagged contingency must be drawn down by 1 February 2020 [CAB Min (18) 0001]. I intend to seek Cabinet's approval to the draw down following the Bill's report back from Select Committee.

Gender implications and Disability Perspective

64. A gender implications and disability perspective analysis has not been undertaken, because the proposals are not intended to apply differently to people based on gender or disability.

Publicity

65. I propose to release this Cabinet paper proactively, upon the Bill's introduction to Parliament. Communications relating to this paper and the introduction of the Bill will be managed by my office, in consultation with other offices as appropriate.

Binding on the Crown

66. The Privacy Bill will bind the Crown.

Creating new agencies or amending law relating to existing agencies

67. The Bill does not create any new agencies. The Bill will create new powers for the Privacy Commissioner and extend the ability to be lead agency for AISAs to some crown agents.

Allocation of decision making powers

68. As discussed in paragraph 33 above, the Bill will reinstate the ability to amend Schedule 5 of the Privacy Act by Order in Council. It will also re-enact other mechanisms for changing the impact of the Information Privacy Principles by regulation, such as the AISA mechanism. For the first time, the Privacy Commissioner will be able to direct agencies to comply with the Act, or give an individual access to their personal information. The Human Rights Review Tribunal will hear appeals from those decisions.

69. The Bill does not otherwise involve the allocation of decision-making powers between the executive, the courts or tribunals.

Associated regulations

70. Regulations will be required for several purposes, such as the requirements for giving notices under the Act. In addition, the Bill will enable the making of Orders in Council for other purposes, such as amending Schedules 2, 3, 4, 5, 6, 7 and 9 of the Bill.

Other instruments

71. The Bill (like the current Privacy Act) empowers the making of Privacy Codes that are disallowable instruments, but not legislative instruments.

Definition of Minister/department

72. The Bill carries over definitions of 'Minister' and 'department' from the Privacy Act.

Commencement of legislation

73. The intention is for the Bill to come into force approximately six months after the date of Royal assent. For drafting purposes, a specific date has been inserted in the Bill which will be changed when the approximate date of enactment is known.

Parliamentary stages

74. The Bill should be introduced into the House on the first available date after Cabinet approval. I propose the Bill be referred to the Justice Committee.

Recommendations

75. I recommend that the Committee:

1. **Note** that the Law Commission's 2011 report *Review of the Privacy Act 1993* called for the Privacy Act 1993 to be repealed and replaced with a modernised law that would reflect changes in the handling of personal information since 1993;

2. **Note** that in March 2014, Cabinet agreed to the drafting of a Privacy Bill to implement most of the Law Commission's recommendations;

3. **Note** that the Privacy Bill holds a category [*withheld under section 9(2)(f)(i) of the Official Information Act 1982*] priority on the 2018 Legislation Programme;

4. **Note** that the Privacy Bill will replace the Privacy Act 1993 and contains key reforms which will mandate reporting of data breaches, strengthen cross-border data flow protections and empower the Commissioner to issue compliance notices and access directions;

Aspects of the Bill which still require policy approval

5. **Note** that Cabinet agreed 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 [CAB Min (14) 10/5A];

6. **Note** that in 2014, Cabinet agreed that the Bill's purpose statement would build upon the Law Commission's suggestions, but also focus on balancing privacy interests with important social and business interests [CAB Min (14) 10/5A];

7. **Agree** that the Bill's purpose statement focus on promoting and protecting individual privacy, rather than balancing privacy interests with important social and business interests;

8. **Note** that in 2014, Cabinet agreed to a two-tier threshold for mandatory privacy breaches, where for 'material' breaches the Privacy Commissioner must be notified, and for 'serious' breaches the Privacy Commissioner and affected individuals must be notified [CAB Min (14) 10/5A];

9. **Note** that government agencies think the two-tier mandatory breach notification regime is too complex, confusing, and will likely lead to agencies shifting responsibility for

determining the category of a data breach to the Privacy Commissioner rather than taking on that responsibility themselves;

10. **Agree** to a single threshold for mandatory privacy breach notification, whereby agencies are required to notify the Privacy Commissioner and affected individuals if there is a risk of harm;

11. **Agree** to remove the concept of 'representative parties' from the Approved Information Sharing Agreement mechanism, instead allowing an Information Sharing Agreement to list the classes of agency to which it can apply, regardless of whether one of that type of agency was an original party to the agreement;

12. **Agree** to extend the ability to act as a lead agency for an AISA to certain crown agents (listed in paragraph 29);

13. **Agree** that the Bill clarify the relationship between Schedule 5 of the Privacy Bill and the Senior Courts Act 2016 and the District Court Act 2016;

14. **Agree** that Schedule 5 of the Privacy Bill be able to be amended by Order in Council, unless the arrangements involve the sharing of court information;

15. **Note** that the information matching provisions in Part 10 of the Privacy Act are no longer required as an AISA can be used for approving information matching programmes;

16. **Agree** that existing information matching programmes continue to operate, but no new programmes be authorised under the new legislation;

17. **Agree** that all ten offences in the Privacy Bill have a maximum penalty of $10,000;

Regulation of the use of re-identified personal information

18. **Note** that, in 2016, Cabinet agreed to a new Information Privacy Principle which would regulate the inadvertent or deliberate use of re-identified data by agencies (CAB-16-MIN-0047 refers);

19. **Note** that an Information Privacy Principle regulating the use of re-identified data has not been included in the Privacy Bill, and that officials are not progressing work on re-identification at this time;

Issues that the Privacy Commissioner raised in his section 26 Report

20. **Note** that the Privacy Commissioner issued a Report in December 2016 under section 26 of the Privacy Act, listing six new proposals which he recommends be included in the Bill;

21. **Note** that the Privacy Commissioner's proposals should not delay the worthwhile reforms in the Bill but could be considered for a future amendment Bill;

Other recommendations

22. **Agree** that the Privacy Bill will bind the Crown;

23. **Approve** the Privacy Bill for introduction, subject to the final approval of the government caucus and sufficient support in the House of Representatives;

24. **Agree** that the Privacy Bill be introduced into the House on the first available date after Cabinet approval;

25. **Agree** that the that the Privacy Bill be:

    25.1 referred to the Justice Committee for consideration; and

    25.2 enacted by March 2019.

Authorised for lodgement

Hon Andrew Little
Minister of Justice