

Hon Andrew Little

Minister of Justice

Proactive release – Privacy Bill: Approval for Supplementary Order Paper and draw down of Budget 2014 tagged contingency

Date of issue: 28 May 2020

The following documents have been proactively released in accordance with Cabinet Office Circular CO (18) 4.

Some information has been withheld on the basis that it would not, if requested under the Official Information Act 1982 (OIA), be released. Where that is the case, the relevant section of the OIA has been noted and no public interest has been identified that would outweigh the reasons for withholding it.

No.	Document	Comments
1	Privacy Bill: Approval for Supplementary Order Paper and draw down of Budget 2014 tagged contingency <i>Cabinet paper</i> Office of the Minister of Justice 4 December 2019	Some information has been withheld in accordance with section 9(2)(h) of the OIA to maintain legal professional privilege. No public interest has been identified that would outweigh the reasons for withholding it.
2	Privacy Bill: Approval for Supplementary Order Paper and Draw-down of Tagged Contingency <i>Cabinet Minute: SWC-19-MIN-0190</i> Cabinet Office Meeting date: 4 December 2019	Released in full.

In Confidence

Office of the Minister of Justice

Chair, Cabinet Social Wellbeing Committee

Privacy Bill: Approval for Supplementary Order Paper and draw down of Budget 2014 tagged contingency

Proposal

- 1 I seek approval to:
 - 1.1 table the attached Supplementary Order Paper (SOP) which implements changes to the Privacy Bill (the Bill), and
 - 1.2 re-phase and draw down the Budget 2014 Vote Justice tagged contingency to implement the Bill, once enacted.

Executive summary

- 2 The Bill completed its second reading on 7 August 2019. I seek approval to table a Government SOP to refine some of the changes made to the Bill by the Justice and Electoral Committee (the Committee) and resolve outstanding issues. The substantive changes in the SOP are to:
 - 2.1 modify Information Privacy Principle (IPP) 4(2) to provide that particularly in circumstances where personal information is being collected from children and young persons, agencies must ensure their collection practices are lawful, fair and not unreasonably intrusive;
 - 2.2 apply the news media exemption in the Bill to overseas news media;
 - 2.3 specify that the Minister of Justice may request the Privacy Commissioner (the Commissioner) to advise whether a country or binding cross-border scheme has privacy law with comparable safeguards to New Zealand law;
 - 2.4 clarify agency liability and defences for a failure to notify a notifiable privacy breach;
 - 2.5 permit the Department of Internal Affairs to enter into new information matching agreements; and
 - 2.6 permit class actions in the Human Rights Review Tribunal (the Tribunal) by persons other than the Director of Human Rights Proceedings (the Director).
- 3 I also seek approval to draw down and re-phase the tagged contingency funding obtained through Budget 2014 to reflect the Bill's earlier commencement date. This will ensure that funding is available to the Office of the Privacy Commissioner (OPC), so it can properly support the Bill's implementation. The re-phasing of the contingency will result in a cost to the Crown.

Background

- 4 The Bill implements the Law Commission's recommendations from its 2011 *Review of the Privacy Act 1993*. The Bill updates New Zealand's privacy law to reflect the needs of the digital age. It maintains the principles-based framework of the Act but adds new accountability mechanisms and gives the Commissioner more powers to ensure compliance. The key changes include:
 - 4.1 mandatory reporting of privacy breaches
 - 4.2 enabling the Commissioner to issue compliance notices
 - 4.3 strengthening cross-border data flow protections
 - 4.4 allowing the Commissioner to make binding decisions on access requests
 - 4.5 new criminal offences, with a fine not exceeding \$10,000.
- 5 The Committee received 162 submissions on the Bill. Almost all submitters supported the Bill's direction, but some had concerns about certain clauses and questioned how the Bill's provisions will operate in practice. The Committee made several valuable changes to the Bill in response to submitter concerns.
- 6 The Bill completed its second reading on 7 August 2019.

Supplementary Order Paper

- 7 I propose to table the attached Government SOP to refine some of the Committee's changes to the Bill and resolve outstanding issues. The SOP follows consultation with privacy experts and with the Commissioner. The SOP also addresses outstanding issues (e.g. the Bill's approach to overseas disclosures of personal information).
- 8 The most substantive changes in the SOP are discussed below. The first two issues clarify the Committee's changes. The remainder concern outstanding issues in the Bill.

Collecting information from children and young people

- 9 There are 13 IPPs in the Bill which deal with how personal information is to be treated. The principles cover the collection, storage, use and disclosure of personal information, and give people the right to access and correct their information.
- 10 IPP 4 governs how personal information is collected. Agencies may only collect it by means that are lawful, fair and do not intrude to an unreasonable extent upon the personal affairs of the individual. The Committee included a new subclause in IPP 4 concerning collection of information from children and young persons. The Committee wanted to emphasise the vulnerability of children and young people who may be more willing than adults to disclose their information online, and who may not be aware why an agency wants their information.
- 11 The policy intent is to ensure that agencies take particular care when collecting information from children and young people. The policy intent could be better achieved if IPP 4(2) were redrafted to provide that when applying IPP 4, agencies must have particular regard to whether the individuals from whom the information is collected are children or young persons. The effect of this change will be a clearer signal to agencies that they need to consider who it is that is likely to access their websites and ensure their collection policies are lawful, fair and

not unreasonably intrusive. The change will balance the Committee's intention with what is practical for agencies and individuals.

Applying the news media exemption to overseas news media

- 12 The news media exemption in the Bill exempts the media from the usual privacy obligations under the Bill in relation to their news activities. This means the gathering, preparation and dissemination of news, information and opinion on current affairs by an agency whose primary business is journalism. The purpose of the exemption is to ensure the news media can perform the role required of it in a democracy, by supporting the free flow of information to the public. The Committee recommended exempting news media that are subject to the oversight of the Broadcasting Standards Authority (BSA) or the New Zealand Media Council (NZMC) or any other similar body prescribed in regulation.
- 13 The media exemption is not currently workable for news entities based overseas. It is possible that overseas media that have reporters based in New Zealand on a regular basis to report on events here could be subject to the Bill's privacy obligations. They could qualify as carrying on business here with respect to their news activities, but not get the benefit of the exemption as they are not regulated by the BSA or the NZMC. They could, however, be subject to appropriate standards of media conduct (including privacy standards) in their own jurisdiction. It would be unreasonable to expect those agencies to also be subject to local media standards bodies. This would likely raise comity issues and concerns about overlapping regulation.
- 14 The SOP will address this gap in the Bill by specifying that the news media exemption include news entities based overseas that:
 - 14.1 have publicly committed to observe recognised journalistic standards of conduct (including privacy standards), and
 - 14.2 are subject to an independent complaints procedure. The complaints process should be accessible to people from overseas (e.g. people residing in New Zealand). Complaints to the BSA, for example, do not require the complainant to be in New Zealand.

Approach to overseas disclosures of personal information

- 15 The Bill seeks to safeguard personal information disclosed overseas. As part of this process, the Bill provides for prescribed countries and binding cross-border schemes (binding schemes).¹ These are countries and binding schemes identified by regulations as providing comparable safeguards to those in New Zealand. The countries listed in the regulations will provide certainty for agencies about which countries they can send personal information to without taking additional measures to protect that information. However, the Bill does not specify who will assess countries and binding schemes as having comparable privacy safeguards. In 2014 Cabinet agreed (as per the Law Commission's recommendation) that the Commissioner have the power to approve specified overseas privacy frameworks as providing acceptable privacy standards and maintain a list of such frameworks on the OPC's website.
- 16 The international context has shifted since 2014, most significantly with the development of the EU General Data Protection Regulation (GDPR). The Comprehensive and Progressive Agreement for Trans Pacific Partnership (CPTPP) has also come into force. The CPTPP has created new obligations for New Zealand concerning the cross-border transfer of information.

¹ The Asia Pacific Economic Cooperation (APEC)'s Cross-Border Privacy Rules system is an example of a cross-border binding scheme.

Rules on cross-border data flows are likely to be included in trade agreements currently under negotiation (and agreed in the Singapore Upgrade, which is not yet in force).

17 By current international standards, the process contemplated by the Law Commission (maintaining a list of approved overseas privacy frameworks on the OPC's website) is not sufficiently robust or transparent. It is expected that New Zealand's key partners will carefully scrutinise our process for prescribing countries and binding schemes. The European Commission has already expressed a high level of interest in our process as part of New Zealand's EU adequacy review (which is ongoing and due to be completed by May 2020).²

18 s9(2)(h)
[Redacted text]

19 Due to these constraints, I anticipate that a much smaller number of countries will be prescribed in regulations, at least initially, than was contemplated in 2011. Prescribing more countries would provide greater certainty to businesses, and potentially reduce their compliance costs. But many of those same businesses also have an interest in New Zealand maintaining EU adequacy.

20 My view is that we need to tread carefully in this space as our process for prescribing countries and binding schemes will be subject to international scrutiny. There are competing privacy models internationally and with our global spread of trade and data connections, we need to ensure we can work with different regimes while still meeting our own requirements in respect of protection of personal information. I therefore intend to prioritise a robust and transparent regulation-making process over prescribing more countries faster.

The Privacy Commissioner will advise whether countries and binding schemes have comparable privacy safeguards

21 The SOP will specify that the Minister of Justice may direct the Commissioner to advise whether a country or binding scheme meets the Bill's comparable safeguards test (or to review any such advice).

22 I consider the OPC is best placed to undertake this role due to its independence from government, high level of privacy expertise and strong international connections. The criteria for assessing countries and binding schemes will be developed by the OPC in consultation with the Ministry of Justice and Ministry of Foreign Affairs and Trade (MFAT). The criteria and process of assessment will be published on the OPC's website.

23 As a Minister cannot direct the Commissioner on a specific matter under the Crown Entities Act 2004, the SOP will need to be explicit on this point. Expectations about progress in assessments will be managed through the standard accountability framework for Crown Entities.

24 Given that it will take some time to robustly assess jurisdictions, it will be important to prioritise those to be assessed. The Ministry of Justice, in consultation with MFAT and the OPC, will

² New Zealand is one of twelve countries that have EU 'adequacy' status. This means that businesses and organisations in the EU can send personal information here without having to apply extra safeguards. Our adequacy status was granted before the introduction of the GDPR and must be reviewed in light of the GDPR's new standards by 25 May 2020.

advise me on which jurisdictions should be prioritised for assessment. I will then direct the Commissioner as to the jurisdictions to be assessed. I will have a discretion to recommend (or not recommend) the making of regulations, following consultation with the Commissioner. I may only make a positive recommendation if I am satisfied that the relevant jurisdiction or binding scheme provides comparable privacy safeguards.

Liability for failure to notify a privacy breach

- 25 Part 6 of the Bill introduces mandatory notification of privacy breaches. The Bill creates an offence if an agency, without reasonable excuse, fails to notify the Commissioner of a notifiable privacy breach (clause 122). The penalty is a fine not exceeding \$10,000.
- 26 The Bill is clear that, for the purposes of civil liability for failure to notify a privacy breach, if a service provider or agent knows of the privacy breach, the outsourcer or principal is also treated as knowing of it. This would not apply for the purpose of the criminal offence of failing to notify the Commissioner where actual knowledge is required.
- 27 Other than principal and agent relationships, however, the Bill is not clear about the point at which an agency is deemed to know that a notifiable privacy breach has occurred. To address this gap, the SOP explicitly provides that anything relating to a notifiable privacy breach that is known by persons in their capacity as officers, employees or members of an agency is to be treated as being known by the agency. This is for the purposes of civil and criminal liability.
- 28 The Bill is also not clear on how liability for failure to notify a notifiable privacy breach will work in practice. This is because there is tension between the new liability provisions in Part 6 of the Bill and the existing general liability clause in the Bill (clause 211, carried over from section 126 of the Act).
- 29 I therefore recommend that the SOP clarify the relationship between these provisions by providing that:
- 29.1 the general defence in clause 211(2) will not apply to the liability of employers for failing to notify a privacy breach either to the Commissioner or to affected individuals; and
 - 29.2 the general defences in clause 211(1)(b) and (c) will not apply to an agency's failure to notify a privacy breach either to the Commissioner or to affected individuals.
- 30 To ensure consistency with how employees are treated under Part 6, clause 122(4) should further clarify that members or officers of an agency would not commit an offence if anything they do, or omit to do, results in their agency failing to notify the Commissioner under clause 118.

Future information matching agreements

- 31 The Bill does not allow any new information matching agreements (IMAs) to be entered into after it comes into force. Information matching programmes can now be authorised using Approved Information Sharing Agreements (AISAs). As no new IMAs are to be entered into after the Bill comes into force, the Bill repeals unused information matching provisions in other Acts.³
- 32 The Committee identified situations where agencies will need to provide for new IMAs under existing information matching provisions after the Bill commences. The Committee

³ The Commissioner consulted agencies for his review into unused statutory information matching provisions, *Review of Statutory Authorities for Information Matching* (September 2018). His report included a list of provisions recommended for repeal in the Bill.

recommended that new IMAs be permitted under section 226A of the Education Act and section 19D(3)(b) of the Social Welfare (Reciprocity Agreements and New Zealand Artificial Limb Service) Act.

- 33 Officials have identified a further situation where new IMAs should be permitted. The Department of Internal Affairs (DIA) shares identity information with a number of government agencies. It plans to authorise all of its information sharing via AISAs by 2023. During the transition period it is likely that DIA will need to provide for new IMAs to be entered into under existing legislated provisions (including provisions that are set to be repealed). This is largely due to process barriers that mean it is more efficient for agencies to access DIA's identity information through IMAs before transitioning to other arrangements.
- 34 To permit DIA to continue to share identity information via new IMAs, the SOP will:
- permit new IMAs under the Births, Deaths, Marriages and Relationships Registration Act 1995 (BDMRRA), the Citizenship Act 1977 and the Electronic Identity Verification Act 2012, and
 - retain the provisions for the Accident Compensation Corporation under Schedule 1A of the BDMRRA and the provisions for the Ministry of Social Development, the Ministry of Education and the Department of Inland Revenue under Schedule 4 of the Citizenship Act 1977.

Permitting class actions in the Tribunal by persons other than the Director

- 35 The Bill clarifies the ability for representative complaints to be made on behalf of a group of individuals as recommended by the Law Commission. A person or advocacy group will be able to bring a complaint about a breach that has affected a large group of people. After it has been investigated by the Commissioner, the complaint can form the basis of a proceeding in the Tribunal for damages.
- 36 The Bill specifies that the Director may bring a proceeding on behalf of a class of individuals and seek remedies. The right to bring such proceedings is confined to the Director. To widen the scope of who may bring such proceedings in the Tribunal, I recommend that the Bill clarify that class actions in the Tribunal may be brought by persons other than the Director.

Less substantial and minor and technical changes

- 37 The SOP includes a range of less substantial changes (including minor and technical changes). These changes include those set out in Appendix One. I propose that Cabinet authorise me to make decisions on any further amendments of this nature.

Financial implications - request to draw down and re-phase the tagged contingency

- 38 I seek approval to draw down and re-phase the tagged contingency funding obtained through Budget 2014 to reflect the Bill's earlier commencement date. The re-phasing of the contingency will result in a cost to the Crown.
- 39 The Vote Justice package in Budget 2014 included a tagged contingency for the OPC to implement the Bill (CAB Min (14) 13/8(18)). This funding would represent a substantial injection into the OPC's budget and is required to develop guidance, design protocols and hire additional staff to perform the Commissioner's new functions and powers introduced by the Bill. To be effective, the OPC's implementation work needs to happen well in advance of commencement so that agencies can update their contracts, privacy policies and internal procedures before the Bill commences.

- 40 I am advised that the Commissioner considers the tagged contingency in Budget 2014 is no longer sufficient to absorb the additional transitional and ongoing costs associated with implementing the Bill. Increased funding is also required for existing functions, due to increased demand for his Office's services. This includes funding for the Commissioner to take effective action to keep New Zealanders' personal information safe and ensure New Zealand businesses can operate globally with personal data. The Commissioner is therefore seeking an increase in the appropriation for his Office through Budget 2020.
- 41 In 2017, Cabinet noted the Minister of Justice would seek approval before 1 February 2020 to draw down the contingency for the implementation of a new Act, as required [CAB-17-MIN-0076]. The contingency is set to phase in over a two-year period, as shown in table 1, reaching an annual total of \$1.19 million by the start of the 2021 financial year. This phasing assumed a commencement date of 1 July 2021.

Table 1: Operating contingency

Privacy Act implementation costs	\$m – increase/(decrease)				
	2018/19	2019/20	2020/21	2021/22	2022/23 & outyears
Existing tagged contingency	0.612	1.190	1.190	1.190	1.190
Proposed contingency re-phasing	-	0.126	0.612	1.190	1.190
Savings in forecast expenditure	(0.612)	(1.064)	(0.578)	-	-

- 42 The Bill has since progressed more quickly than anticipated. The Bill was introduced in March 2018 and is due to commence in 2020. As such, I seek Cabinet approve to re-phase and draw down the contingency funding as shown in table 2.

Table 2: Proposed re-phasing

Privacy Act implementation costs	\$m – increase/(decrease)				
	2019/20	2020/21	2021/22	2021/22	2022/23 & outyears
Existing tagged contingency	0.126	0.612	1.190	1.190	1.190
Proposed contingency re-phasing	0.738	1.190	1.190	1.190	1.190
Additional forecast expenditure	0.612	0.578	-	-	-

- 43 The proposed re-phasing will result in a cost to the Crown. This is because some of the reductions in funding agreed in 2017 will need to be reversed. This simply reflects the earlier commencement of the Bill, rather than resulting from any new policy or any changes to the original funding agreed by Cabinet.
- 44 I seek approval to fund the cost of re-phasing from the between Budget contingency. It is not possible to fund this cost from the OPC's baselines because the OPC's appropriation is comparatively small (approximately \$4.950 million for 2019/20) and the funding was previously set aside by Cabinet for the specific purpose of implementing the Bill.

Consultation

- 45 The following departments, agencies and crown entities have been consulted on the proposals in this paper: the Treasury, the Ministries of Foreign Affairs and Trade, Business, Innovation and Employment, Defence, Education, Health, Social Development, Oranga Tamariki, Culture and Heritage, Environment, Primary Industries, the Department of Prime Minister and Cabinet, the Department of Internal Affairs; Customs, Inland Revenue, Land Information New Zealand, NZ Police, Parliamentary Counsel, Statistics NZ, New Zealand Transport Agency, Accident Compensation Corporation, Government Chief Privacy Officer, the Office of the Privacy Commissioner, the New Zealand Media Council and the Broadcasting Standards Authority.

Impact analysis

- 46 The Treasury Regulatory Quality Team consider that the decisions sought in this paper are exempt from the Regulatory Impact Analysis requirements on the basis that they have no or only minor impacts on businesses, individuals and not-for-profit entities.

Legislative implications

- 47 The proposed SOP will amend the Privacy Bill.

Gender implications

- 48 There are no gender implications arising out of these proposals.

Disability perspective

- 49 There are no disability implications arising out of these proposals.

Compliance

- 50 The SOP complies with:
- 50.1 the principles of the Treaty of Waitangi;
 - 50.2 the rights and freedoms contained in the New Zealand Bill of Rights Act 1990 and the Human Rights Act 1993;
 - 50.3 the disclosure statement requirements (a short form disclosure statement prepared by the Ministry of Justice is attached);
 - 50.4 relevant international standards and obligations, and
 - 50.5 the Legislation Guidelines (2018 edition), which are maintained by the Legislation Design and Advisory Committee.

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

Binding on the Crown

52 The Bill is binding on the Crown. The SOP will not change this.

Creating new agencies or amending law relating to existing agencies.

53 The SOP does not create new agencies or amend the law relating to existing agencies.

Allocation of decision making powers

54 The SOP does not affect the allocation of decision-making powers between the executive, the courts, and tribunals.

Associated regulations

55 Regulations are not needed to bring the SOP into operation. However, regulations will be needed to bring certain parts of the Bill into operation. I will seek policy approval for these regulations in due course.

Other instruments

56 The SOP does not include any provisions empowering the making of other instruments that are deemed to be legislative instruments or disallowable instruments (or both).

Definition of Minister/department

57 The SOP does not contain a definition of Minister, department (or equivalent government agency), or chief executive of a department (or equivalent position).

Commencement of legislation

58 The SOP when incorporated into the Bill will come into effect on the same date as the Bill. The Bill is intended to commence on 1 July 2020 or six months after the date of Royal assent whichever is later.

Parliamentary stages

59 The Bill has a category three priority (to be passed if possible in the year) on the 2019 Legislation Programme [CAB-19-MIN-0049]. It completed its second reading on 7 August 2019 and now awaits the Committee of the whole House stage.

Proactive Release

- 60 I propose to proactively release this paper in full within 30 business days after the SOP is tabled.

Recommendations

The Minister of Justice recommends that the Committee:

- 1 **Note** that the Privacy Bill was reported back from the Justice and Electoral Committee on 13 March 2019 and completed its Second Reading on 7 August 2019;
- 2 **note** that further changes are needed to the Bill via Supplementary Order Paper to clarify the policy intent, make the Bill more workable in practice and resolve outstanding issues;

Supplementary Order Paper

- 3 **approve** the attached Supplementary Order Paper for tabling which implements the following changes to the Bill:
 - 3.1 modify Information Privacy Principle 4(2) to provide that particularly in circumstances where personal information is being collected from children and young persons, agencies must ensure their collection practices are lawful, fair and not unreasonably intrusive;
 - 3.2 apply the news media exemption in the Bill to news media agencies based overseas if they have publicly committed to observe recognised journalistic standards of conduct (including privacy standards) and are subject to an independent complaints procedure that is available to people overseas (e.g. people residing in New Zealand);
 - 3.3 specify that the Minister of Justice may direct the Privacy Commissioner to advise whether a country or binding cross-border scheme provides comparable privacy safeguards to those in the Bill;
 - 3.4 specify that the Minister of Justice may direct the Privacy Commissioner to advise whether a country or binding cross-border scheme that has been prescribed as having comparable safeguards continues to provide such safeguards;
 - 3.5 clarify agency liability for failure to notify a notifiable privacy breach as follows:
 - 3.5.1 clarify that anything relating to a notifiable privacy breach that is known by persons in their capacity as employees, officers or members of an agency is to be treated as being known by the agency;
 - 3.5.2 clarify that the general defence in clause 211(2) will not apply to the liability of employers for failing to notify a privacy breach either to the Commissioner or to affected individuals;
 - 3.5.3 clarify that the general defence in clause 211(1)(b) and (c) will not apply to an agency's failure to notify a privacy breach either to the Commissioner or to affected individuals;
 - 3.5.4 clarify that members or officers of an agency would not commit an offence if anything they do or omit to do results in their agency failing to notify the Commissioner under clause 118.

- 3.6 permit future information matching agreements under the Births, Deaths, Marriages and Relationships Registration Act 1995, the Citizenship Act 1977 and the Electronic Identity Verification Act 2012, and
- 3.7 retain the information matching provisions for the Accident Compensation Corporation under Schedule 1A of the Births, Deaths, Marriages and Relationships Registration Act 1995 and the provisions for the Ministry of Social Development, the Ministry of Education and the Department of Inland Revenue under Schedule 4 of the Citizenship Act 1977;
- 3.8 permit class actions in the Human Rights Review Tribunal by persons other than the Director of Human Rights Proceedings;
- 3.9 a range of less substantial and minor and technical changes including those set out in Appendix One.
- 4 **note** that the attached Supplementary Order Paper amends the Privacy Bill which holds a category three priority (to be passed if possible in the year) on the 2019 Legislation Programme;
- 5 **agree** that the Minister of Justice be authorised to make any additional minor and technical drafting decisions that may be required before the Supplementary Order Paper is tabled in the House;

Re-phasing and drawing down tagged contingency funding

- 6 **note** that a tagged contingency was set up in Vote Justice through Budget 2014 for Privacy Act implementation costs;
- 7 **note** that on 20 December 2017 Cabinet [CAB-17-MIN-0076 refers]:
- 7.1 agreed to extend the draw down date from 1 February 2018 to 1 February 2020 for the tagged contingency set aside for Vote Justice in Budget 2014;
- 7.2 agreed to the following timing for the tagged contingency to reflect the timing changes for the likely commencement of the new Privacy Act:

Operating contingency

Initiative name	\$m – increase/(decrease)				
	2018/19	2019/20	2020/21	2021/22	2022/23 & outyears
Privacy Act implementation costs	-	0.126	0.612	1.190	1.190
Total operating	-	0.126	0.612	1.190	1.190

- 7.3 noted that the Minister of Justice would seek Cabinet's approval before 1 February 2020 to draw down the tagged contingency in recommendation 7.2 above for the implementation of the new Privacy Act, as required;
- 8 **note** that, as the Bill is expected to come into force on 1 July 2020 at the earliest, implementation needs to commence in the 2019/20 financial year;

- 9 **agree** to increase the tagged contingency established in Budget 2014 by the following amount to reflect the earlier implementation of the new Privacy Act, and that this additional expenditure be charged against the between-Budget contingency established as part of Budget 2019;

Initiative name	\$m – increase/(decrease)				
	2019/20	2020/21	2021/22	2022/23	2023/24 & outyears
Privacy Act implementation costs	0.612	0.578	-	-	-
Total operating	0.612	0.578	-	-	-

- 10 **approve** the following changes to appropriations to provide for the implementation of the new Privacy Act, with a corresponding impact on the operating balance and net core Crown debt:

	\$m – increase/(decrease)				
	2019/20	2020/21	2021/22	2022/23	2023/24 & Outyears
Vote Justice Minister of Justice Non-Departmental Output Expenses Services from the Privacy Commissioner	0.738	1.190	1.190	1.190	1.190
Total Operating	0.738	1.190	1.190	1.190	1.190

- 11 **agree** that the proposed changes to appropriations for 2019/20 above be included in the 2019/20 Supplementary Estimates and that, in the interim, the increases be met from Imprest Supply;
- 12 **agree** that the expenses incurred under recommendation 10 above be charged against the Privacy Act Implementation Costs – Tagged Operating Contingency described in recommendation 7 above and adjusted in recommendation 9 above;
- 13 **note** the Privacy Commissioner considers the tagged contingency in Budget 2014 is no longer sufficient to absorb the additional transitional and ongoing costs associated with implementing the Bill, and that increased funding is also required for existing services and is therefore seeking an increase in the appropriation for his Office through Budget 2020.

Authorised for lodgement

Hon Andrew Little

Minister of Justice

Appendix One: Table of less substantive and minor and technical changes in the Supplementary Order Paper

Clause	Issue	Change
Part 1 – Preliminary provisions		
Clause 2 – commencement date	A commencement date of 1 March 2020 is specified in the Bill as it simplifies the drafting of the consequential changes that refer to it. The policy intent is that agencies have a lead in time of six months to prepare for the Bill's changes. To allow for the Bill passing later this year, a change to the commencement date is recommended.	Commencement date changed to 1 July 2020. The policy intent is that the Bill will have a 6-month period between enactment and commencement.
Clause 2 – commencement of Codes of practice	Currently certain parts of the Bill will take effect from 1 March 2020 except for certain provisions which will come into effect on the day after the Royal Assent. For clarity, part 3 of the Bill, which deals with Codes of Practice, also needs to come into force on the day after the Royal Assent so that updated Codes of Practice can be notified and issued before the Bill commences.	Clause 2(1) of the Bill amended to add Part 3/clauses 35-43 of the Bill.
Clause 3 – purpose of this Act	Unlike the long title of the Act, the Bill's purpose clause does not include express reference to the right of an individual to access their personal information. To avoid the risk of the right of access being read down, the purpose clause should include specific reference to the right of an individual to access their personal information.	Clause 3 amended to: "(a) providing a framework for protecting an individual's right to privacy of personal information, including the right of an individual to access their personal information, while recognising that other rights and interests may at times also need to be taken into account."
Clause 3A – application to overseas government agencies	The Bill is not intended to apply to overseas governments performing public/governmental functions. It is intended to apply to commercial enterprises owned by an overseas government that carries on business in New Zealand. The definition of overseas agency in the Bill does not make this distinction clear.	Overseas agency defined in clause 6C of the Bill as not including an overseas government agency to the extent that the agency is performing any public function on behalf of the overseas government.

Clause	Issue	Change
Clause 3A – offences to apply regardless of where conduct takes place	The policy intent is that subject to sections 6 and 7 of the Crimes Act 1961, the offences in clause 212 of the Bill (e.g. misleading an agency to obtain someone else’s personal information) apply to any person regardless of where the conduct amounting to the offence takes place. However, clause 3A(2)(b) as drafted requires an element of the offence to be committed in New Zealand.	Amend clause 3A(2)(b) to provide that the offences in clause 212 of the Bill should apply regardless of the location of the offence if the person is within scope of the Bill (i.e. carrying on business in NZ).
Clause 6 – definition of country	The definition of “country in the Bill includes a State, territory, or province or any other part of a country. This definition is relevant to IPP 12 (1)(e) and needs to be more flexible to allow for the variety of types of jurisdiction that may be appropriate for designation by regulation under clause 212B e.g. the EU.	Definition of “country” amended, for the purposes of IPP 12 and clause 212A and 212B, to include a self-governing state, province, or territory.
Part 3 – Information privacy principles, public register privacy principles and codes of practice		
IPP 12 – disclosure of personal information outside New Zealand	IPP 12 sets out when an agency may disclose personal information to a foreign person or entity overseas in reliance on IPP 11. It does not cover disclosures to people from overseas who are present but not ordinarily resident in New Zealand. This group of people are now expressly covered by the Bill by virtue of new clause 3A. We recommend an amendment the Bill to exempt disclosures of personal information to people from overseas who are present but not ordinarily resident in New Zealand.	Definition of “foreign person or entity” amended to include a person who is not present in New Zealand.

Clause	Issue	Change
Part 4 – Access to and correction of personal information		
Clause 45 – Individuals may make IPP 6 request	Under the Act an access request can be made by an agent of the individual (including that individual's representative). This has not been clearly carried through into the Bill.	Clause 45 amended to clarify that an IPP 6 request may be made by the individual concerned or that individual's representative.
Part 5 – Complaints, investigations and proceedings		
Part 5 – who can make a complaint	The Bill provides a process for people to complain to the Commissioner, and if necessary, the Human Rights Review Tribunal (the Tribunal) if they believe an agency's action has interfered with someone's privacy. The current drafting does not clearly provide for how representative complaints are to be dealt with both in relation to investigations by the OPC and proceedings in the Tribunal.	Part 5 of the Bill amended to clarify how representative complaints are to be investigated by the OPC and how these types of proceedings will be dealt with in the Tribunal.
Clause 103 – aggrieved individual may commence proceedings in Tribunal	The Bill is clear that the Tribunal can award damages as part of an appeal against an access direction. It does not provide that an individual can bring a claim for damages when they have obtained an access direction and are not seeking to challenge the terms of that direction (or have obtained the information) but want a remedy for the impact on them for the delay in obtaining the information.	A further ground added to clause 103 to include a claim for damages when an access direction has been obtained and whether or not its terms are also challenged by the individual.
Clause 103 – aggrieved individual may commence proceedings in Tribunal	Under the Act a complainant can go to the Tribunal after an unsuccessful dispute resolution process where the Commissioner has determined that the matter should not be proceeded with and there has been no investigation. A complainant can also go to the Tribunal where the matter has been referred to the Director, but the Director declines to take the case. These pathways for access to the Tribunal are not clearly provided for in the Bill.	Clause 103 amended to preserve the ability for a complainant to access the Tribunal: <ul style="list-style-type: none"> • after an unsuccessful dispute resolution process where the Commissioner has determined that the matter should not be proceeded with and there has been no investigation; and • where the matter has been referred to the Director, but the Director declines to take the case.

Clause	Issue	Change
Part 6 – Notifiable privacy breaches and compliance notices		
Clause 121(2A) – requirements for notification	When an agency notifies an individual of a privacy breach, the Bill provides that the agency may disclose the identity of the recipient of the information if a serious threat exists to the life or health of the affected individual. This test is not consistent with the comparable IPP11 exception, which provides that there must be a necessary connection between the identity information, the serious threat and that disclosure can reduce the risk of the threat. We recommend for consistency that clause 121(2A) is amended to align with the comparable exception in IPP11(f)(ii).	Clause 121(2A) amended to provide that a notification to an affected individual, or their representative, may identify a person or body that has obtained, or may obtain, that affected individual’s personal information if the agency believes on reasonable grounds that the disclosure of the information is necessary to prevent or lessen a serious threat to the life or health of the affected individual or any other person.
Clause 124 – compliance notices	Clause 124 does not currently cover the full scope of the Commissioner’s power to issue a compliance notice. The policy intent is that the Commissioner can issue a compliance notice for breaches of codes of practice made under other legislation. Some codes made under other legislation use the Commissioner’s complaints procedure for enforcement (e.g. the Social Security Act 2018 and the Housing Restructuring and Tenancy Act 1992).	Clause 124(1)(b) amended to provide that the Commissioner may issue a compliance notice in relation to a breach of a code of practice or code of conduct made under the Privacy Act or under other legislation that utilises the Commissioner’s complaints jurisdiction. Consequential amendments to schedule 10 of the Bill so that where necessary schedule 10 also refers to Part 6.

Clause	Issue	Change
Part 7 – Sharing, accessing, and matching personal information		
Clause 141 – parties to an information sharing agreement	Section 96E of the Act (carried over as clause 140 in the Bill) specifically permits an approved information sharing agreement to provide for one part of an agency to share personal information with 1 or more other parts of the same agency. There is difficulty, however, in identifying who the parties to the agreement are. This could be resolved by clarifying that that a part of an agency entering into an information sharing agreement must be identified as a party to that agreement.	Clause 141(1) amended to clarify that part of an agency entering into an information sharing agreement must be identified as a party.
Clause 142 - agreement may apply to classes of agencies	The AISA framework permits an agreement with classes of agency. It is not clear what obligations the lead agency has to notify relevant parties of any changes to the schedule of parties.	New clause 142A (4A) inserted: “A lead agency must, after doing any of the things referred to in subsection (4), provide each of the parties to the information sharing agreement with a copy of the Schedule of Parties, or amended Schedule of Parties, as the case may be.”
Clause 138 and 143 – definition of lead agency	The Bill is not clear that part of a public sector agency may be the lead agency in an information sharing agreement (e.g. the Registrar- General of the BDMRRA is part of DIA and responsible for all information sharing under the BDMRAA but is not able to be the lead agency for an information sharing agreement).	Clause 138 and 143 amended to provide that a party that is a part of a public sector agency may be designated as the lead agency.

Clause	Issue	Change
Part 9 – Miscellaneous provisions		
Clause 213 – other regulations	The Bill does not currently provide for service of compliance notices by the Commissioner on an agency outside New Zealand, or service of proceedings in the HRRT outside New Zealand. As the Bill now expressly provides for when it would apply to agencies outside New Zealand, it is necessary, for the Bill to expressly authorise the service of compliance notices and proceedings outside New Zealand.	Clause 213 amended to include an express regulation-making power in respect of overseas service of compliance notices and proceedings in the Tribunal.
Schedule 4 – identity information	Schedule 4 provides for certain agencies to have access to an individual’s identity information held by holder agencies specified in the schedule. DIA is listed as an accessing agency and as a holder agency. The Registrar-General of the BDMRRA is not listed as either an accessing agency or holder agency although he acts independently of DIA in the exercise of the powers, functions and duties under the BDMRRA and is the statutory holder of the information.	The Registrar-General of the Births, Deaths, Marriages, and Relationships Registration Act 1995 added as an accessing agency and as a holding agency in Schedule 4 of the Bill.
Schedule 5 – law enforcement information	The Ministry of Justice has access to the ‘Police temporary file index’ listed in schedule 5 to obtain information about parties to offences for the purpose of processing cases before a court and to update Police records. However, Police advise that this should be removed from the Bill as reference to a Police temporary file index is obsolete and the information can be obtained from other sources.	Schedule updated to remove the reference to the subject ‘Police temporary file index’ as this subject is obsolete and the information can be obtained by other means.



Cabinet Social Wellbeing Committee

Minute of Decision

This document contains information for the New Zealand Cabinet. It must be treated in confidence and handled in accordance with any security classification, or other endorsement. The information can only be released, including under the Official Information Act 1982, by persons with the appropriate authority.

Privacy Bill: Approval for Supplementary Order Paper and Draw-down of Tagged Contingency

Portfolio Justice

On 4 December 2019, the Cabinet Social Wellbeing Committee:

Background

- 1 **noted** that the Privacy Bill (the Bill) holds a category three priority on the 2019 Legislation Programme (to be passed if possible in 2019);
- 2 **noted** that the Bill was reported back from the Justice and Electoral Committee on 13 March 2019 and completed its second reading on 7 August 2019;
- 3 **noted** that further changes are needed to the Bill via Supplementary Order Paper to clarify the policy intent, make the Bill more workable in practice and resolve outstanding issues;

Supplementary Order Paper

- 4 **approved** the Supplementary Order Paper [PCO 18441-1/4.0], attached to the submission under SWC-19-SUB-0190 for release, which implements the following changes to the Bill:
 - 4.1 modify Information Privacy Principle 4(2) to provide that, particularly in circumstances where personal information is being collected from children and young persons, agencies must ensure their collection practices are lawful, fair and not unreasonably intrusive;
 - 4.2 apply the news media exemption in the Bill to news media agencies based overseas if they have publicly committed to observe recognised journalistic standards of conduct (including privacy standards) and are subject to an independent complaints procedure that is available to people overseas (e.g. people residing in New Zealand);
 - 4.3 specify that the Minister of Justice may direct the Privacy Commissioner to advise whether a country or binding cross-border scheme provides comparable privacy safeguards to those in the Bill;

- 4.4 specify that the Minister of Justice may direct the Privacy Commissioner to advise whether a country or binding cross-border scheme that has been prescribed as having comparable safeguards continues to provide such safeguards;
- 4.5 clarify agency liability for failure to notify a notifiable privacy breach as follows:
- 4.5.1 clarify that anything relating to a notifiable privacy breach that is known by persons in their capacity as employees, officers, or members of an agency is to be treated as being known by the agency;
 - 4.5.2 clarify that the general defence in clause 211(2) will not apply to the liability of employers for failing to notify a privacy breach either to the Commissioner or to affected individuals;
 - 4.5.3 clarify that the general defence in clause 211(1)(b) and (c) will not apply to an agency's failure to notify a privacy breach either to the Privacy Commissioner or to affected individuals;
 - 4.5.4 clarify that members or officers of an agency would not commit an offence if anything they do or omit to do results in their agency failing to notify the Commissioner under clause 118;
- 4.6 permit future information matching agreements under the Births, Deaths, Marriages and Relationships Registration Act 1995, the Citizenship Act 1977, and the Electronic Identity Verification Act 2012;
- 4.7 retain the information-matching provisions for the Accident Compensation Corporation under Schedule 1A of the Births, Deaths, Marriages and Relationships Registration Act 1995 and the provisions for the Ministry of Social Development, the Ministry of Education and the Department of Inland Revenue under Schedule 4 of the Citizenship Act 1977;
- 4.8 permit class actions in the Human Rights Review Tribunal by persons other than the Director of Human Rights Proceedings;
- 4.9 a range of less substantial and minor and technical changes including those set out in Appendix One, attached to the submission under SWC-19-SUB-0190;
- 5 **noted** that the Supplementary Order Paper amends the Privacy Bill, which holds a category three priority (to be passed if possible in the year) on the 2019 Legislation Programme;
- 6 **authorised** the Minister of Justice to make any additional minor and technical drafting decisions that may be required before the Supplementary Order Paper is tabled in the House;

Re-phasing and drawing down tagged contingency funding

- 7 **noted** that a tagged contingency was set up in Vote Justice through Budget 2014 for Privacy Act implementation costs;

8 **noted** that on 20 December 2017, Cabinet:

8.1 agreed to extend the draw down date from 1 February 2018 to 1 February 2020 for the tagged contingency set aside for Vote Justice in Budget 2014;

8.2 agreed to the following timing for the tagged contingency to reflect the timing changes for the likely commencement of the new Privacy Act:

Operating contingency

Initiative name	\$m – increase/(decrease)				
	2018/19	2019/20	2020/21	2021/22	2022/23 & outyears
Privacy Act implementation costs	-	0.126	0.612	1.190	1.190
Total operating	-	0.126	0.612	1.190	1.190

8.3 noted that the Minister of Justice would seek Cabinet's approval before 1 February 2020 to draw down the tagged contingency referred to above for the implementation of the new Privacy Act, as required;

[CAB-17-MIN-0076]

9 **noted** that, as the Bill is expected to come into force on 1 July 2020 at the earliest, implementation needs to commence in the 2019/20 financial year;

10 **agreed** to increase the tagged contingency established in Budget 2014 by the following amount to reflect the earlier implementation of the new Privacy Act, and that this additional expenditure be charged against the between-Budget contingency established as part of Budget 2019;

Initiative name	\$m – increase/(decrease)				
	2019/20	2020/21	2021/22	2022/23	2023/24 & outyears
Privacy Act implementation costs	0.612	0.578	-	-	-
Total operating	0.612	0.578	-	-	-

11 **approved** the following changes to appropriations to provide for the implementation of the new Privacy Act, with a corresponding impact on the operating balance and net core Crown debt:

	\$m – increase/(decrease)				
	2019/20	2020/21	2021/22	2022/23	2023/24 & Outyears
Vote Justice					
Minister of Justice					
Non-Departmental Output Expenses					
Services from the Privacy Commissioner	0.738	1.190	1.190	1.190	1.190
Total Operating	0.738	1.190	1.190	1.190	1.190

- 12 **agreed** that the changes to appropriations for 2019/20 above be included in the 2019/20 Supplementary Estimates and that, in the interim, the increases be met from Imprest Supply;
- 13 **agreed** that the expenses incurred under paragraph 10 above be charged against the *Privacy Act Implementation Costs Tagged Operating Contingency* described in paragraph 8 above and adjusted in paragraph 10 above;
- 14 **noted** that the Privacy Commissioner considers the tagged contingency in Budget 2014 is no longer sufficient to absorb the additional transitional and ongoing costs associated with implementing the Bill, and that increased funding is also required for existing services, and is therefore seeking an increase in the appropriation for his Office through Budget 2020.

Vivien Meek
Committee Secretary

Present:

Rt Hon Jacinda Ardern
Rt Hon Winston Peters
Hon Kelvin Davis
Hon Grant Robertson
Hon Chris Hipkins
Hon Andrew Little
Hon Nanaia Mahuta
Hon Stuart Nash
Hon Jenny Salesa
Hon Kris Faafoi
Hon Tracey Martin (Chair)
Hon Poto Williams

Officials present from:

Officials Committee for SWC
Office of the Chair

Hard-copy distribution:

Minister of Justice