Coversheet: Additional policy approvals for the Privacy Bill

Advising agencies	The Ministry of Justice
Decision sought	Agreement to progress changes to the Privacy Bill to: 1. amend the threshold for mandatory notification of a privacy breach, so that agencies must notify breaches where the breach is likely to cause serious harm 2. clarify the Bill's application to agencies based overseas and information held overseas 3. expand the definition of "news activity" to include all forms of news media, so long as the news medium is subject to independent standards of conduct (including privacy standards) and a complaints procedure 4. align the treatment of Television New Zealand (TVNZ) and Radio New Zealand (RNZ) with other news media in respect of the news media exemption in the Bill.
Proposing Ministers	Minister of Justice

Summary: Problem and Proposed Approach

Problem Definition

What problem or opportunity does this proposal seek to address? Why is Government intervention required?

In 2014 Cabinet agreed to the drafting of a new Privacy Bill (the Bill) that responded to the Law Commission's 2011 Review of the Privacy Act 1993 (the Act) [CAB Min (14) 10/5A]. Three Regulatory Impact Statements (RIS) were prepared in 2012, 2014 and 2016 for earlier Cabinet policy decisions.

The Justice Committee has received 162 submissions on the Bill, many of which suggest changes. We propose to progress some of these through the Departmental Report on the Bill. Four of the changes we propose be included in the Bill meet the threshold for regulatory impact analysis (RIA), and are discussed below.

(1) The threshold for a notifiable privacy breach

The Bill introduces mandatory reporting of privacy breaches. A privacy breach in this context means unauthorised access to, or loss of, personal information. The Bill requires agencies to notify the Commissioner and affected individuals, if the breach has caused *harm*, or there is a risk it will do so.

Submitters are concerned that the threshold for mandatory notification is subjective, and will in effect require all breaches to be reported, even if harm is unlikely to occur. They consider that the Bill's threshold for mandatory notification risks significant over-reporting

and is out of step with comparable jurisdictions. The notification threshold attracted the largest number of submissions on the Bill.

(2) The Bill's application to agencies based overseas

The Bill details some specific situations in which it applies to information held overseas. However, the Bill does not address key issues, such as whether the Bill will apply to agencies that are based overseas, and if so, in what circumstances. Submitters are concerned that if the Bill's extra-territorial application is not expressly addressed, there will be a high level of uncertainty about when the Bill does, and does not, apply in a cross-border context. These situations arise much more frequently in a digital context, as people routinely submit their personal information directly to overseas-based agencies online.

(3) Definition of news medium and news activity

Carrying over provisions from the Act, the Bill excludes news media from its scope in respect of news activities. The exemption recognises that requiring the media to comply with the information privacy principles (IPPs) would impose an unreasonable limit on the free flow of information in the news media.

News medium is defined as any agency whose business, or part of whose business, consists of a news activity. A news activity is defined as preparing or compiling, and disseminating *articles or programmes* relating to news or current affairs. There is no requirement for news media carrying out news activities to be subject to independent standards of conduct. In practice, traditional news media (i.e. newspapers, magazines, radio and television) are already subject to regulation through the Broadcasting Standards Authority (BSA) and the New Zealand Media Council (NZMC).

Some submissions are concerned the scope of "news activity" is unclear, because the definition refers to 'articles and programmes' and so unfairly distinguishes between the form the news activity takes. There is uncertainty about which news media and news activities are, or are not, excluded from the Act (or Bill) and can therefore benefit from the media exemption.

(4) Applying the news media exemption in full to RNZ and TVNZ

Carrying over provisions from the Act, RNZ and TVNZ, unlike other news media, are not fully exempt from the Bill in respect of their news activities. They must comply with IPP6 (access to personal information) and IPP 7 (correction of personal information). The rationale for treating RNZ and TVNZ differently is that, as crown entities, they should be subject to greater transparency requirements than other news media.

RNZ and TVNZ have stated that the distinction for RNZ and TVNZ is no longer justified. They argue that they are not on a level playing field with their competitors, because the subject of an investigation is able to use the Act (or Bill) to request information about themselves while the investigation is ongoing, thereby frustrating its progress.

TVNZ and RNZ also face an additional compliance burden as they are subject to three regimes (the Broadcasting Standards Act 1989 (BSA), the Privacy Act and the Official Information Act 1982 (OIA)). They cited recent examples where this has led to the same complaint having to be dealt with three times, once under each regime.

Proposed Approach

How will Government intervention work to bring about the desired change? How is this the best option?

(1) The threshold for a notifiable privacy breach

We recommend raising the threshold for a notifiable privacy breach and clarifying how it will operate, to address concerns about:

- the lack of certainty for agencies applying the threshold in the Bill;
- the risk of over-notification; and
- to better align the Bill with comparable regimes overseas.

We recommend the threshold for notification of a privacy breach (to individuals and the Privacy Commissioner) should require notification of breaches only where a reasonable person would conclude that the breach is likely to cause serious harm. In assessing the risk of a privacy breach causing someone serious harm, agencies should also be able to take into account any actions they have taken that will reduce this risk.

This option most effectively supports the purposes of mandatory notification by ensuring people are made aware any breaches that pose a risk of serious harm; incentivising agencies to take security of personal information seriously (and to address breaches early before harm is caused); and assisting the Privacy Commissioner to address systemic issues. It will align New Zealand with comparable notification regimes overseas, which is useful for agencies operating across jurisdictions.

(2) The Bill's application to agencies based overseas

We recommend that in the case of overseas-based agencies, the Bill's application be determined by the extent of their connection to New Zealand. We recommend the Bill expressly apply to:

- agencies that are resident in New Zealand in respect of all of their conduct, inside *and outside* New Zealand, and
- agencies that carry on business in New Zealand in respect of conduct engaged in in the course of carrying on the agency's New Zealand business.

The intention would be to capture entities that regularly supply goods and services to a substantial number of people resident here. This level of connection makes it reasonable to regulate what is done by the entity here.

This option aligns with the approach taken in Australia and in other New Zealand legislation (such as the Fair Trading Act 1986).

(3) Definition of news medium and news activity

We recommend that the definition of news activity is broadened to capture means of disseminating news other than just "articles or programmes". The term news activity should capture books, online platforms and other methods of disseminating news that could develop in the future. The change will mean that media will be exempt from the Bill in respect of their news activities, regardless of the platform those news activities use.

To ensure that people can access a complaints process in respect of any privacy concerns, we also recommend that the Bill introduces a requirement that the exemption only apply to news media that are subject to independent standards of conduct (including privacy standards) and complaints procedures.

This approach recognises:

- the ongoing need for an exception from the privacy regime for the media, given the media's central role in a free and democratic society;
- the difficulty of predicting how news media platforms will continue to evolve;
- that media privileges come with responsibilities to provide fair, accurate, balanced and truthful reporting.

(4) Applying the news media exemption in full to RNZ and TVNZ

We recommend applying the news media exemption in full to RNZ and TVNZ. In our view, this is the best option because it will:

- allow RNZ and TVNZ to undertake their news activities freely
- provide an operational level playing field under the privacy regime for all news organisations, regardless of their ownership; and
- reduce the regulatory overlap that currently exists in this domain.

Section B: Summary Impacts: Benefits and costs

Who are the main expected beneficiaries and what is the nature of the expected benefit?

(1) The threshold for a notifiable privacy breach

The recommended changes to the threshold will reduce the compliance burden for agencies by making the mandatory notification regime more workable. The changes will also benefit the public, by reducing the risk of over notification and hence notification fatigue. There will be advantages for businesses operating on both sides of the Tasman, as the higher threshold aligns more closely with the Australian regime.

(2) The Bill's application to agencies based overseas

The recommended changes will provide greater certainty about which agencies must comply with the Bill, and in respect of what information, in a cross-border context. The Bill will apply to agencies that carry on business in New Zealand in respect of information collected in the course of carrying on that business. The clarification will benefit New Zealanders by ensuring privacy protection clearly applies when agencies carry on business here. It will also make it clear that the Bill applies to agencies resident in New Zealand in respect of their activities both here and overseas. This will reduce the risk of regulatory gaps, where a person is unable to obtain a remedy for a privacy breach.

(3) Definition of news medium and news activity

Broadening the scope of news activity to all media platforms will address uncertainty about whom the news media exemption in the Bill applies to. To the extent that non-traditional media are captured by the broadened definition of news activity, a barrier to the dissemination of news will be removed. Media will be able to undertake news activities without, for example, being required to request information from the person concerned directly (IPP 2), or disclose personal information held to anyone else (IPP11). They will be subject to privacy complaints from individuals concerned about privacy breaches, as news

media will only be able to benefit from the exemption if they are subject to independent standards of conduct (including privacy standards) and complaints procedures.

(4) Applying the news media exemption in full to RNZ and TVNZ

RNZ and TVNZ will benefit from a small reduction in compliance obligations as they will no longer be subject to the requirement to allow access to and correction of individuals' information under the privacy regime (IPP 6 and IPP 7). They will have greater freedom to undertake their news activities without the subject of an investigation being able to request information about themselves while an investigation is ongoing. The degree of regulatory overlap to which they are subject will also be reduced.

Where do the costs fall?

(1) The threshold for a notifiable privacy breach

Our 2014 RIS discussed the costs of introducing a mandatory notification regime for agencies and the Privacy Commissioner. That RIS noted that the actual costs of the notification regime could not be estimated. It also noted that mandatory breach notification will be potentially costly for agencies in the short term (if new systems need to be implemented), but has the potential for long term savings if client confidence is maintained and system issues are addressed. The proposals in this RIS will reduce those costs.

(2) The Bill's application to agencies based overseas

Agencies based overseas but carrying on business here that do not comply with New Zealand's privacy regime will need to make sure that their practices meet New Zealand standards and will also need to comply with the Act's other requirements (e.g. notify privacy breaches). The agencies could include small online retail businesses if they systematically, as opposed to occasionally, trade with a substantial number of New Zealanders. If these agencies already have best practice privacy standards (for example, to comply with the European Union's General Data Protection Regulation (GDPR)), any additional costs would be minimal.

(3) Definition of news medium and news activity

All news media will need to be subject to independent standards of conduct and complaints procedures in order to come within the news media exemption. Traditional news media organisations are subject to such standards already. New media and smaller media, such as bloggers, who want to get the benefit of the exemption may incur some small compliance costs through the payment of fees or levies to an industry regulatory body.

(4) Applying the news media exemption in full to RNZ and TVNZ

People will no longer have access and correction rights in respect of personal information collected by TVNZ and RNZ in the course of their news activities. People will still be able to complain about privacy matters to the BSA.

What are the likely risks and unintended impacts, how significant are they and how will they be minimised or mitigated?

(1) The threshold for a notifiable privacy breach

The primary concern with raising the notification threshold is that an agency could fail to notify an affected individual about the loss of their personal information, because it does not consider it meets the threshold. An individual could suffer harm which they could have prevented, had they been informed about the privacy breach.

We think, however, that the benefits from changing the notification regime are more likely to be undermined by the converse situation of a proliferation of low-level notifications, which could desensitise people to genuine risk of harm.

The Bill imposes a criminal offence for failure to notify the Privacy Commissioner of a notifiable breach. This may mean that agencies will continue to take a cautious approach to notification, which may undermine some of the benefits of increasing the threshold. This risk, however, needs to be balanced against the need to ensure agencies do not take too narrow a view of whether to notify.

(2) The Bill's application to agencies based overseas

Some agencies that carry on business here will have to comply with New Zealand law as well as the law of another country (i.e. there will be some regulatory overlap). This can be managed through the regulator's discretion in deciding which cases to pursue; for example the Privacy Commissioner may decide not to issue a compliance notice, if the data protection authority in another country is better placed to issue and enforce such a notice.

In considering this proposal we have sought to balance the need to avoid regulatory overlap with the need to avoid a situation where there are regulatory gaps, leaving people without any remedy. The proposal is based on an agency's level of connection with New Zealand. It is appropriate and desirable for New Zealand's privacy law to apply in situations where that agency is carrying on business here, and the issue in question has arisen in the course of that business.

(3) Definition of news medium and news activity

While the Privacy Commissioner supports broadening the definition of news activity to clarify its application to books, he expresses caution about the risk of unintended consequences from broadening the definition as proposed. He recommends that, for clarity and workability, the proposed qualifier must be expressed in specific terms so it is clear that only membership of the established media regulators (i.e. BSA and NZMC) qualify to exempt news media from the Bill. Alternatively, he suggests that the Bill should include a clear process for deciding whether standards of media regulation are adequate for this purpose (such as setting out criteria in regulations) to ensure a minimum standard of alternative redress.

We do not agree that the Bill should specify that only membership of the BSA and NZMC qualifies an agency for the exemption. This level of prescription would rule out the possibility of future changes (e.g. arising from work being undertaken by the Ministry for Culture and Heritage on the broader regulatory settings for the media). We agree that the Bill should include criteria on the media standards we expect would qualify for exemption.

We think that membership of an independent body with media standards (including privacy standards) and a complaints procedure would qualify for the exemption.

There is also a risk that changing the Bill alone will not be sufficient to make the exemption available to all news activities. It is not clear whether a book, even written by a member, would be considered 'news' by the NZMC. But this is something the NZMC could consider and adapt its requirements and processes for.

(4) Applying the news media exemption in full to RNZ and TVNZ

The Privacy Commissioner and the Ombudsman oppose the removal of the exception for RNZ and TVNZ.

The Privacy Commissioner is concerned about reducing the rights for individuals to access and correct their personal information. We acknowledge that access rights will be removed but this will only be in relation to RNZ and TVNZ's news activities. In our view, the media exemption should be extended to cover TVNZ and RNZ because the change will provide an operational level playing field for all news organisations, regardless of their ownership. Access and correction rights in respect of news activities can represent an unjustifiable limitation on freedom of information, whether the broadcaster is privately or publicly owned. The status quo, in our view, is outdated and inconsistent (e.g. Māori Television benefits from the exemption).

Both the Privacy Commissioner and the Ombudsman are also concerned that the change would put the Bill out of step with the OIA. Companies would retain a right to access and seek correction of information about themselves under the OIA, while individuals would not under the Privacy Act (or Bill). People may also be able to use the OIA as a workaround for accessing personal information, if a third party requests information about a person under the OIA and that person signs a privacy waiver.

We acknowledge that making this change to privacy law ahead of complementary changes to the OIA will create a discrepancy between the two regimes. But a concurrent review of the OIA and privacy law is impractical, as the Privacy Bill is already well advanced. The Government has signalled its intent to carry out targeted consultation, commencing later this year, to inform a decision on whether to progress a formal review of the OIA. Such a review could consider the position of RNZ and TVNZ under the OIA, and thus provide an opportunity to realign the two regimes.

Identify any significant incompatibility with the Government's 'Expectations for the design of regulatory systems'.

The proposed changes are consistent with the Government's expectations for the design of regulatory systems. The Bill includes reforms that will update and modernise New Zealand's privacy regime, and deliver significant benefits for New Zealanders. The additional reforms discussed in this RIA will further enhance the Bill and so support its overall objectives.

Section C: Evidence certainty and quality assurance

Agency rating of evidence certainty?
Our rating of evidence certainty is low-medium. We do not have quantitative data about the costs and benefits of the status quo versus the options identified in this RIA. The nature of the privacy regime is such that costs and benefits are hard to estimate, as each privacy breach, and agency to which the Act applies, is unique. The scale and cost of a mandatory notification process, for example, is influenced by the nature of the issue, the risk of harm that is posed, and the number of people affected. The analysis in this RIA is therefore qualitative. The key judgements (and assumptions) we have made about the impacts on agencies and individuals are included in relevant sections in the RIA. Evidence of the need for changes to the Bill has come from submissions. In developing options, the Ministry has consulted with the other government agencies, as well as the Office of the Privacy Commissioner. We have also drawn upon suggestions made by submitters in their submissions to the Justice Committee. We met directly with the New Zealand Law Society, the Privacy Foundation, Business New Zealand, PwC, Kensington Swan, Trade Me, Professor Paul Roth and Rick Shera. We met with TVNZ, RNZ, the Broadcasting Standards Authority, the NZ Media Council and the Ministry of Culture and Heritage to discuss the media exemption proposals. We also engaged David Goddard QC to provide expertise on the cross-border issues. We have drawn upon legislation in Australia, Canada and the EU for our proposal to change the threshold for mandatory breach notification. We have not been able to draw upon international *evidence* of how the regime is working because mandatory breach notification is a very recent development. Australia, Canada and the EU introduced the regime earlier this year. It has not been in place long enough overseas to allow for monitoring and evaluation of whether it is working as intended. We have drawn upon the Law Commission's analysis for our proposals to broaden the definition of news activity and align the treatment of TVNZ and RNZ with other news media in respect of their use of the media exemption in the Bill. The Law Commission made similar recommendations in its 2011 report, and elaborated on these recommendations in its 2013 report *News media meets the new media*. We have assumed that the current definition of news activity restricts the dissemination of news in certain platforms by news media subject to the privacy regime. This assumption is supported by at least two reported examples of information which contributed to books being requested from journalists under the Privacy Act, which could discourage people from publishing journalistic books.

Quality Assurance Reviewing Agency:
The Ministry of Justice
Quality Assurance Assessment:
The Ministry of Justice's RIA QA panel has reviewed the RIA: *Additional policy approvals for the Privacy Bill* prepared by the Ministry of Justice and considers that the information and analysis summarised in the RIA meets the QA criteria.
Reviewer Comments and Recommendations:
In reaching this conclusion, the QA panel notes the constraints posed by the limited availability of data to support the analysis. That constraint is always a factor with framework legislation such as the Privacy Act, which applies across all sectors, and to agencies ranging from the smallest sole trader to the largest corporation. The RIA's extensive use of submitters' evidence ensures a range of perspectives are available, which helps to make the qualitative analysis robust and reliable.

Impact Statement: Additional policy approvals for the Privacy Bill

General information

Purpose
The Ministry of Justice is solely responsible for the analysis and advice set out in this Regulatory Impact Statement (RIS), except as otherwise explicitly indicated. This analysis and advice has been produced for the purpose of informing decisions about whether or not to proceed with further changes to the following aspects of the Bill: (1) The threshold for a notifiable privacy breach (2) The territorial application of the Bill (3) Definition of news medium and news activity (4) Applying the news media exemption in full to RNZ and TVNZ.
Key Limitations or Constraints on Analysis
A key limitation is the qualitative nature of the analysis. This affects our evidence certainty, which is low-medium. Quantitative evidence and analysis would normally provide more certainty about whether the proposals will have net benefits. On the other hand, as noted above, we have taken into account submissions on the Privacy Bill, drawn upon Law Commission recommendations and consulted with key privacy law experts. *Key gaps and assumptions in the data:* *The threshold for a notifiable privacy breach:* We do not have quantitative evidence about the extent to which the changes proposed in this RIA will improve the workability of the mandatory breach notification regime and limit unnecessary compliance costs for agencies, because the notification regime does not yet exist. International data is also not available as comparable overseas notification regimes have only recently been introduced. Nevertheless, the preferred option is supported by nearly all submitters on this issue, and other government departments consulted on both this RIA and accompanying Cabinet paper. Both groups noted that the development of criteria should help make it easier for agencies to determine the likelihood of serious harm occurring and thereby improve the workability of the regime. *Clarifying the territorial application of the Bill*: A key unknown is the number of agencies based overseas who will be affected by the clarification of territoriality in the Bill i.e. carrying on business in New Zealand. To the extent that these agencies already operate best practice privacy standards, we have assumed any additional costs to be minimal. We may, however, have underestimated the additional compliance costs. At worst, some

businesses could choose to withdraw from the New Zealand market because the additional cost of compliance is too onerous for them. In our view this risk is small, however, particularly given that the New Zealand privacy regime does not expose firms to the large civil sanctions that are possible in other countries.

Definition of news medium and news activity: We have assumed that the current definition of news activity restricts the dissemination of news in certain platforms by news media subject to the Privacy regime.

Applying the news media exemption in full to RNZ and TVNZ : We have relied on self-reported evidence from TVNZ and RNZ on the implications of the exception to the exemption for their news activities.

Responsible Manager (signature and date):

Chris Hubscher

Policy Manager, Electoral and Constitutional Policy

Ministry of Justice

Date: 21 September 2018

Problem definition and objectives

What is the context within which action is proposed?

In 2014 Cabinet agreed to the drafting of a new Bill to repeal and replace the Privacy Act, implementing recommendations from a Law Commission report to modernise the Act [CAB Min (14) 10/5A]. As recommended by the Law Commission, the Privacy Bill retains a principles-based approach to privacy law but increases accountability mechanisms. It will create stronger incentives for agencies to identify and prevent privacy risks, and give the Privacy Commissioner a stronger regulatory role in responding to privacy breaches.
The Bill will better align New Zealand's law with international privacy frameworks, such as the OECD Guidelines and the GDPR. New Zealand businesses will be able to assure their overseas customers that our law offers a high standard of privacy protection.

The Privacy Bill had its first reading on 11 April 2018, and is currently being considered by the Justice Committee.

The proposed changes to the Bill discussed below respond to submitter concerns on:

- the Bill's workability in relation to mandatory breach notification
- insufficient clarity on the Bill's application to overseas agencies; and
- inconsistencies in its application to the media.

Addressing these issues will make the Bill more effective, clearer, and better aligned with comparable jurisdictions.

Submitters have put forward a range of other ideas for reform, many of which reflect emerging innovations in international privacy and consumer rights law, such as the GDPR. These issues are not part of the current Bill. They would require significant policy development and consultation, particularly as international best practice is not yet agreed. We anticipate that these issues will instead be considered as part of future policy work on privacy and digital rights.

What regulatory system, or systems, are already in place?

The Privacy Act 1993

The Privacy Act governs the collection, use and sharing of personal information in New Zealand. It seeks to ensure that people's privacy is protected. 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. The Act applies to every 'agency' that collects, holds or uses personal information, including government, the private sector and non-governmental organisations.

The Law Commission's 2011 Review of the Privacy Act 1993

The Law Commission reviewed privacy law from 2007 to 2011, and produced a series of reports. The fourth and final report, *Review of the Privacy Act 1993*, called for the Privacy Act to be repealed and replaced with a modernised law that would reflect changes in the handling of personal information. The Government accepted most of the Law Commission's recommendations. Others were rejected, accepted in modified form, or deferred (e.g. recommendations relating to the media).

Are there any constraints on the scope for decision making?
See the comments above under 'Key limitations or Constraints on Analysis'. No other constraints on the scope for decision making have been identified.

(1) The threshold for a notifiable privacy breach

What is the policy problem or opportunity?
The Bill introduces mandatory notification for a privacy breach, to the Commissioner and affected individuals. In this context, a privacy breach is the loss of, or unauthorised access to, personal information. Agencies must notify a privacy breach if it has caused harm to an affected individual or individuals, or there is a risk it will do so. Harm is defined as loss, detriment, damage, or injury to an individual, adversely affecting an individual's rights, benefits, privileges, obligations, or interests; or significant humiliation, loss of dignity, or injury to feelings. The Bill imposes a criminal offence for failure to notify the Commissioner of a notifiable breach; an agency may be liable to a fine of up to $10,000. The breach notification requirements are intended to help mitigate harm (or the risk of it), make agencies more accountable for breaches and allow the Commissioner to address systemic issues before they cause further harm. The majority of submitters thought that the threshold for notifiable privacy breaches in the Bill lacks clarity about how it would operate and is too low, creating uncertainty for agencies and a likely over reporting of breaches. They were concerned that the threshold would lead to over-notification, as nearly all breaches would need to be reported, even those unlikely to cause harm. This is because there is nearly always a 'risk' that could be identified. Over-notification can lead to notification fatigue, where individuals receive so many notifications that they do not take any action upon receipt of a notice, even though taking action could help to mitigate actual harm. Another concern with over notification is that the act of notification can cause anxiety and distress. This is particularly so if the affected individual is unable to do anything to address the breach, or assess the likelihood of harm (as they may not be told to whom their information has been disclosed). The resource implications of over-notification for the Commissioner and agencies was also raised. Business submitters noted that the threshold in the Bill is out of step with comparable jurisdictions, particularly the EU and Australia. They raised concerns about the potential damage to our international reputation if we appear to have a proportionally higher number of notifications. A further issue is the way that harm is assessed in the Bill. Most submitters, including the Legislation Design and Advisory Committee and the Law Society, think the current threshold for assessing harm is too subjective and uncertain. The Bill uses existing definitions of "harm" developed in the context of a complaints-based regime, where harm is generally assessed after the harm has occurred to the specific individual. This approach does not work as well for assessing risk before any harm has occurred, and where there may be a number of affected people with differing levels of tolerance for risk and harm.

What options are available to address the problem?

Two options were considered to address the problems identified in the status quo. They address different aspects of the issues raised by submitters, and are not mutually exclusive.

Option 1 - Increase the threshold for mandatory notification of a privacy breach

This would require agencies to notify individuals and the Commissioner of breaches that are likely to cause serious harm. Under this option, the number of notifications are likely to be reduced. As it focuses on 'serious harm', individuals will be more motivated to take the notification seriously and actively take steps to mitigate any harm arising. This option better aligns with one of the key aims of the notification regime - to help mitigate harm (or the risk of it).

The Bill will include criteria to help agencies determine whether a breach would be likely to cause serious harm, such as the nature of the information and the sensitivity of the information. Other jurisdictions use similar factors which help agencies and the regulatory body to apply the threshold consistently.

The notification threshold in other jurisdictions, such as Australia, considers both the risk of harm (likelihood) and the impact of the harm (materiality). We think these are both valid factors in setting the threshold. We also think that aligning the notification regime with Australia and similar jurisdictions will benefit New Zealand agencies who trade there.

Option 2 - Incorporate an objective approach to assessing the likelihood of harm occurring

Under this option, agencies would take an objective approach to assessing the likelihood of harm occurring; i.e. notification would be required if it a reasonable person would conclude that there is a risk of harm. This option addresses the issue that an agency may need to assess the risk of harm for a group of people where it is not practical to determine any one person's level of tolerance for risk and harm.

Australia and Canada both use an objective approach to assessing whether notification is required.

What do stakeholders think?

The notification threshold attracted the largest number of submissions (85 out of 162 submitters) from individuals to academics, community groups, local government, businesses, industry representatives, and privacy and legal experts. Collectively these submissions provided a cross-section of views from agencies which may have to notify under the new regime, and individuals who may receive such notifications.

Only three submitters (two individuals and the Marketing Association) favoured blanket notification, suggesting notification should be required wherever there is a breach. They argue the individual is best-placed to assess harm and decide what mitigating steps to take.

Two submitters suggest automatic notification should apply only in relation to breaches of 'sensitive' information, such as biometric or genetic information.

The majority of submitters, and the stakeholders with whom we consulted, were concerned about over-notification and the risk of notification fatigue undermining the intent of the mandatory notification regime. They strongly supported increasing the threshold.

Submitters were also unanimous in agreeing that the test needed to be more objective.

The Privacy Commissioner broadly supports changes to clarify the breach notification threshold and reduce uncertainty. However, the Commissioner notes that the criminal offence for failure to notify is still likely to incentivise a cautious approach by agencies, which could undermine the intent of this change.

What other options have been ruled out of scope, or not considered, and why?

A two-tier regime for mandatory notification is not analysed in this RIS, in light of a Cabinet decision to adopt a single tier regime in February 2018.

Cabinet originally approved a two-tier approach in 2014. This would have required:

- *for serious breaches* – notification both to the Commissioner and the affected individuals when there is a real risk of harm
- *for material breaches* – notification to the Commissioner only. A material breach was effectively a breach that did not meet the serious breach threshold determined by taking into account: the sensitivity of the information; the number of people involved; and indications of a systemic problem.

This approach was changed to a single tier threshold by Cabinet in February 2018, just prior to the introduction of the Bill. The change was made in response to concerns raised by government departments that having two tiers would create a high level of uncertainty and inconsistency, and the difficulty in prescribing two distinct, clear thresholds.

(2) The Bill's application to agencies based overseas

What is the policy problem or opportunity?

The Bill carries over provisions from the Act detailing specific situations in which the Bill will apply to agencies and information overseas. These provisions address some territorial scope issues. For example, clause 8 of the Bill confirms that if agency B holds information on behalf of agency A, then agency A is treated as holding that information regardless of whether agency B is outside New Zealand, or holds the information outside New Zealand.

The Bill does not address key issues such as whether the legislation will apply to agencies that are not "in" New Zealand, and if so, in what circumstances. Submitters are concerned that if the Bill doesn't expressly address territorial scope, there will be too much uncertainty about how it applies to overseas persons, agencies and information. These situations arise much more frequently in a digital context.

The Supreme Court has taken a cautious approach to the territorial scope of domestic law. Domestic law is treated as applying to persons and conduct outside New Zealand only if it provides for extra-territorial application expressly or by necessary implication. Not including a provision setting out when the Bill applies to overseas agencies could, therefore, result in a restrictive approach to territorial scope which provides insufficient privacy protection.

What options are available to address the problem?

We considered the following three options.

Option 1 - Make it clear who the Bill applies to, including agencies resident in NZ and those with an established place of business here

The Bill could make it clear that it applies to agencies that are resident in New Zealand. This could be defined to include agencies that have their central management and control here or an established place of business in New Zealand. Taking a strict interpretation, this option could represent a codification of what a court may decide to be the case under the Bill as it stands.

Under this option many agencies that regularly provide goods and services to New Zealanders, but are based overseas (e.g. online retailers, social media platforms), would not be covered and people may be left without an effective remedy for privacy breaches.

Option 2 - Clarify the territorial application of the Bill along the lines of the Australian Privacy Act 1988

The Australian Privacy Act 1988 makes express provision for its territorial scope – it applies to countries that have an "Australian link". The Bill could contain a similar provision. It would make it clear that the Bill applies to:

- agencies that are resident in New Zealand in respect of all of their conduct, inside *and outside* New Zealand, and
- agencies that carry on business in New Zealand in relation to conduct engaged in in the course of carrying on the agency's New Zealand business.

The key change would be to make it clear that the Bill applies to agencies that carry on business in New Zealand. The term "carrying on business" is used in other statutes. The intention would be to capture entities that supply goods and services to a substantial number of people resident in New Zealand on a regular basis, whether or not the entity has an established place of business in New Zealand, and whether or not any monetary payment is made for those goods or services.

We think the extension to entities carrying on business here makes good sense: this is a form of connection that involves presence through an agent and/or systematically and deliberately taking advantage of the opportunity to engage in trade here. This level of connection makes it reasonable to regulate what that entity does here.

Option 3 - Provide for the Bill to apply to any collection of personal information from, or in relation to, a person situated or resident in New Zealand, along the lines of the GDPR

This option focuses on the location of the subject of the information. The Bill would apply to any collection of personal information from, or in relation to, a person situated or resident in New Zealand. This is the approach adopted under the GDPR, although it is not yet clear how this provision will be interpreted.

An extension of the territorial scope by reference to the location of the persons about whom the information is collected and held raises comity issues, overlapping regulation concerns, and real difficulties in drawing an appropriate line between agencies that should and should not reasonably be required to comply with our privacy law. There would also be significant practical difficulties in enforcing a New Zealand law which purports to have broad extra-territorial application to entities that have no presence and do not carry on business here.

What do stakeholders think?
Eight submitters commented on this issue. All submitters that commented agreed that it would be useful to clarify when the Bill applies. Most submitters, including the Privacy Foundation and the Privacy Commissioner, support our preferred option. One submitter we spoke to expressed reservations about the Bill applying to agencies that were not resident but did carry on business here. They were concerned about overseas agencies needing to comply with multiple regulatory regimes, and speculated as to how they would feel about other countries taking the same approach. Based on media commentary, we expect businesses, particularly multi-nationals, would be similarly concerned about overlapping regulatory regimes and have considered this concern further below. One submitter favoured a broader approach that aligned with that taken in the GDPR. This would provide for the legislation to apply to any collection of personal information from, or in relation to, a person situated or resident in New Zealand.

What other options have been ruled out of scope, or not considered, and why?
This RIS does not consider the possibility of introducing pecuniary penalties for serious and repeated breaches of the Bill, as the Privacy Commissioner has proposed. That may give a more effective enforcement option for overseas agencies than criminal offences, at least for agencies based in Australia. This would be a significant reform to the enforcement framework - we think it should be considered as part of a full policy development process.

(3) Definition of news medium and news activity

What is the policy problem or opportunity?
Carrying over provisions from the Act, the Bill excludes certain people or organisations from its scope, by excluding them from the definition of agency. This exclusion is related to the nature of their role, and to allow them to operate freely, for example the courts are excluded in relation to their judicial functions. The news media are similarly excluded from compliance with the Bill and the information privacy principles, but only in relation to their news activities. The purpose of this exclusion is to ensure the news media can perform the role required of them in a democracy, by supporting the free flow of information to the public. The Bill carries over the existing definitions of “news medium” and “news activity” for the news media exemption. Some submissions are concerned the scope of “news activity” is unclear, because the definition refers to ‘articles and programmes’ and so unfairly distinguishes between the form the news activity takes. For example, a recent court case held that a book was not a ‘news activity,’ meaning that the journalist author did not have the benefit of the exemption, because a story was published in book form rather than serialised in a magazine.

What options are available to address the problem?

Option 1 - Maintain the status quo

Under the status quo, traditional news media (newspapers, magazines, radio and television) clearly fall within the definition of news activity in the Bill and are primarily regulated through the BSA and the NZMC. Traditional news media are therefore subject to independent standards of conduct (including privacy standards) and complaints procedures. People can also bring claims against the media in the courts (for instance, tortious claims in defamation and privacy). The status quo provides some privacy protection to people and traditional media are free to carry out their news activities consistent with their role in a democratic society.

The extent to which non-traditional media fall within the current exemption for news activity is unclear under the status quo. The courts and the Commissioner have interpreted the definitions of news medium and news activity differently in different cases. To the extent that some news activities do not get the benefit of the media exemption, this could discourage the dissemination of news and be regarded as an unjustifiable limitation on the free flow of information.

To the extent that non-traditional media are able to claim the exemption, people may be left with no complaints process available to them. This is because many non-traditional media are not subject to independent standards of conduct and a complaints process.

Option 2- Broaden the definition of news activity

This option broadens the definition of news activity by using more generic language (e.g. “publications and broadcasts”, “content”, or “material”).

Broadening the definition of news activity would mean that all forms of news activity get the benefit of the exemption. This option recognises the importance of media freedoms in a free and democratic society.

However, it also weakens privacy protections for individuals, as a broader range of news activities will be exempt from the Act, without any additional safeguards being put in place. For media that are not covered by an independent regulator, a complainant will need to rely on recourse to the courts in respect of any breaches of privacy.

Option 3 - Broaden the definition of news activity and change the definition of news media to exempt only those agencies that are subject to independent standards of conduct

Under this option, the definition of news activity will be broadened as discussed under Option 2. In addition, the Bill will specify that only news media that are subject to independent standards of conduct and complaints procedures administered by an independent body (e.g. the Press Council, the BSA, the NZMC or any other relevant standards body that might be established in future) could claim the exemption. The standards of conduct would need to include privacy standards.

This option has the benefits of option 2 but better accommodates both the importance of media freedom and people’s privacy interests. Only media organisations that are willing to be held to appropriate standards of media conduct (including privacy standards) are able to utilise media privileges for their news activities. This option provides effective oversight of media claiming the exemption, and access to a complaints process if privacy standards are not adhered to.

The change would mean that news media using 'traditional' media platforms will also need to be subject to a standards body to get the benefit of the exemption. This will be a shift from the status quo for traditional news media, as the exemption currently applies to them without a specific requirement in the Act (or Bill) that they be subject to an independent body. In practice, however, traditional media are usually subject to the BSA or NZMC already.

What do stakeholders think?

The Committee received six submissions on this issue from media organisations and individuals. The majority of submitters considered the definition should be broadened.

The Commissioner supports the proposal to clarify the definition of "news activity" in principle, however considers the Bill should explicitly state that membership of established media regulators (i.e. BSA and NZMC) qualifies for purposes of the Privacy Act exemption. If membership is not clearly stated, the Bill should include criteria about qualifying news media regulators in order to support decision-making about the scope of the exemption.

We do not agree that the Bill should specify that membership of the BSA and NZMC would immediately qualify for exemption. This level of prescription would rule out the possibility of future changes (e.g. arising from Ministry for Culture and Heritage work on broader media regulatory settings). We do agree that the Bill should include criteria on the media standards we expect would qualify for exemption. We think that membership of an independent body with media standards (including privacy standards) and a complaints procedure should qualify for the exemption.

What other options have been ruled out of scope, or not considered, and why?

We have not considered the Law Commissions' 2013 *News Media meets New Media* as those options were more wide-ranging than required for amendment to the Privacy Bill. The options included establishing a single, independent news media standards authority and a consistent definition of the term "news media" across a number of statutes.

(4) Applying the news media exemption in full to RNZ and TVNZ

What is the policy problem or opportunity?

The Bill continues to treat TVNZ and RNZ differently to other media in terms of their access to the media exemption. IPP 6 (access to personal information) and IPP 7 (correction of personal information) apply to RNZ and TVNZ in respect of their news activities. They can refuse an access request to protect confidential journalistic sources. The original rationale for this exception was that, as crown entities, TVNZ and RNZ should be subject to greater transparency requirements. This is a similar rationale for why the OIA also applies to these organisations.

The Law Commission recommended in its 2011 report that TVNZ and RNZ should get the full benefit of the media exemption as they operate on a similar basis as other news media in relation to their news activities. TVNZ and RNZ have submitted that they should be fully exempt from the Bill, because they want to operate on a level playing field with other media organisations. They think that they are at a disadvantage currently, because the subject of an investigation is able to use the Act to request information about themselves while the investigation is ongoing, thereby frustrating its progress. TVNZ and RNZ also cited examples of having to deal with the same complaint under three regimes: the Privacy Act, the OIA and the BSA.

We understand from RNZ and TVNZ that access and correction requests and complaints under IPPs 6 and 7 arise infrequently. Managing the complaints can be onerous, however, due to the three overlapping regimes.

What options are available to address the problem?

We have considered the following two options.

Option 1 - Maintain the status quo

Under this option, RNZ and TVNZ will continue to be subject to IPPs 6 and 7.

This would not address the issues TVNZ and RNZ are facing. It continues to place TVNZ and RNZ at a competitive disadvantage to private media companies. Further, it places an additional compliance burden of them, as they are potentially subject to three regulatory and complaints regimes.

The requirement to allow access to and correction of information could impair journalistic endeavours (to carry out news activities independently and without fear or favour). For instance, it may allow someone who TVNZ and RNZ is investigating to seek access to information gathered while the investigation in ongoing.

Option 2 - Bring RNZ and TVNZ fully within the media exemption

Under this option, RNZ and TVNZ will be fully brought within the media exemption. RNZ and TVNZ would be excluded from all privacy principles when undertaking news activities. This option puts all news media on an equal footing. It will also prevent duplication between Privacy Act access and correction requests and complaints to the Press Council/BSA.

Individuals will not have a right to access and correct their personal information held by RNZ and TVNZ in respect of their news activities. Instead, people could complain about any breach of privacy standards to the BSA. While this right is not as privacy protective as access and correction rights under the Privacy regime, the difference recognises the important role news media, including TVNZ and RNZ, play in a free and democratic society.

RNZ and TVNZ will still be required, however, to provide companies with their information under the OIA, or to provide a third party with personal information about another person (if that person waives privacy). The Law Commission noted these anomalous positions in its report but thought that it could be addressed by considering whether changes should be made to the OIA. We agree with this position.

What do stakeholders think?

TVNZ and RNZ support being fully exempted from the Bill. The Ministry for Culture and Heritage also supports this position.

The Privacy Commissioner and the Ombudsman oppose the removal of the exception for RNZ and TVNZ. The Privacy Commissioner is concerned about reducing the right for individuals to access and correct their personal information.

We acknowledge that access and correction rights will be removed, but this will only be in relation to RNZ and TVNZ's news activities. In our view, the media exemption should be extended to cover TVNZ and RNZ because the change will provide an operational level playing field for all news organisations, regardless of their ownership. Access and correction rights in respect of news activities can represent an unjustifiable limitation on freedom of information whether the broadcaster is privately or publicly owned. The status quo, in our view, is outdated and inconsistent (e.g. Māori Television benefits from the exemption).

Both the Privacy Commissioner and the Ombudsman are also concerned that the change would put the Bill out of step with the OIA. Companies would retain a right to access and seek correction of information about themselves under the OIA, while individuals would not under the Privacy Act (or Bill). People may also be able to use the OIA as a workaround for accessing personal information, if a third party requests information about a person under the OIA and that person signs a privacy waiver.

We acknowledge that making this change to privacy law ahead of complementary changes to the OIA will create a discrepancy between the two regimes. But a concurrent review of the OIA and privacy law is impractical, as the Privacy Bill is already well advanced. The Government has signalled its intent to carry out targeted consultation, commencing later this year, to inform a decision on whether to progress a formal review of the OIA. Such a review could consider the position of RNZ and TVNZ under the OIA, and thus provide an opportunity to realign the two regimes.

What other options have been ruled out of scope, or not considered, and why?

We have considered and dismissed the option of all media being required to respond to access and correction requests i.e. to comply with IPPs 6 and 7. We do not think this is a feasible option because it would represent too great a restriction on news activities.

What criteria, in addition to monetary costs and benefits, have been used to assess the likely impacts of the options under consideration?

The options for the four issues discussed above have been assessed against three or more of the following criteria, depending on which criteria are relevant to the particular issue.

Effectiveness – the extent to which the option's expected outcomes address the problem

Certainty – the option improves certainty and clarity of the law

Trust and confidence – the option promotes a reasonable expectation of people's privacy interests

International compatibility – the option aligns with international approaches and does not lead to unnecessary regulatory overlap

Freedom of expression – the option upholds the right to freedom of expression and the ability of the media to undertake its functions in a democratic society

Comity – the option aligns with broadly accepted principles governing the assertion of jurisdiction internationally

Impact Analysis

Key:	
++	much better than doing nothing/the status quo
+	better than doing nothing/the status quo
0	about the same as doing nothing/the status quo
-	worse than doing nothing/the status quo
- -	much worse than doing nothing/the status quo

(1) The threshold for a notifiable privacy breach

	Status quo	Option 1 (Increase the threshold to situations where the breach is likely to cause serious harm)	Option 2 (Incorporate an objective approach to assess the likelihood of harm occurring)
Effective	**0**	**++** Should reduce the risk of over notification. Penalty for non-notification may mean that agencies still take a cautious approach and over notify.	**+** Agencies will be able to objectively assess the likelihood of harm, which should make the assessment easier. But a low threshold and penalties for non-notification could still lead to risk of over-notification.
Certainty	**0**	**+** A clearer test than in the current Bill. Introduction of criteria for determining 'serious' harm should assist agencies to assess likelihood of harm occurring. Subjective determination of 'serious' harm could lead to inconsistencies.	**+** May provide more certainty for agencies needing to assess the risk of harm where the people affected may have differing tolerances for risk and harm.
Trust and confidence	**0**	**+** Expected to reduce over-notification and so notification fatigue. Should increase trust and confidence in the protection of privacy interests, if only serious breaches are notified and so make it more likely that individuals, when notified, will take steps to avoid further harm. There may be situations where agencies do not notify when they should.	**0** Risk of over notification could reduce confidence in the protection of privacy interests.
International compatibility	**0**	**+** Aligns with overseas comparative jurisdictions; including Australia, the EU, and Canada.	**+** Aligns with overseas comparative jurisdictions; including Australia, the EU, and Canada.
Overall assessment	**0**	**++** While increasing the threshold to serious harm should reduce risk of over-notification, a subjective determination of serious harm provides insufficient certainty for agencies needing to assess the risk of harm before any harm has occurred (and where there may be a number of affected people with differing tolerances for risk and harm).	**+** Objective determination of harm increases certainty for agencies, but threshold of harm is still low and could lead to over-reporting.

(2) The Bill's application to agencies based overseas

	Status quo	Option 1 (agencies resident in NZ or with an established place of business here)	Option 2 (agencies carrying on business in NZ; information collected in course of carrying on business)	Option 3 (all information collected from people resident in New Zealand)
Certainty	**0**	**+** Provides a clear test for agencies to apply.	**+** Provides a clear test for agencies to apply that is used in other domestic legislation.	**-** The test in the GDPR appears very broad; there is uncertainty as to how it will be interpreted.
Trust and confidence	**0**	**-** Provides insufficient privacy protection for New Zealanders whose information is often collected and held by agencies based overseas.	**+ +** Promotes expectation that Bill will apply to personal information that people submit to overseas agencies that conduct business in NZ.	**+** Promotes expectation that Bill will apply to personal information that people submit to overseas agencies. But could raise expectations too high due to significant practical difficulties with enforcement.
International compatibility and regulatory overlap	**0**	**-** Does not align with the approach taken in other jurisdictions, such as Australia and the EU. Less regulatory overlap but could leave regulatory gaps.	**+** Aligns with Australian approach. Regulatory overlap is not unreasonable – for agencies carrying on business the Privacy Act will only apply in respect of their NZ business.	**+** Approach adopted under GDPR. Potentially very large regulatory overlap if every country took that approach.
Comity	**0**	**0** No change from the status quo.	**0** Requires a degree of connection with NZ that makes it reasonable to regulate what is done by the entity within the jurisdiction.	**--** Potentially captures agencies that should not reasonably be required to comply with the Bill (e.g. online retailers that very occasionally have a NZ sale).
Overall assessment	**0**	**-** Insufficient privacy protection for New Zealanders whose information is often collected and held by agencies based overseas.	**++** Provides expressly when agencies are subject to the Bill and the extent of connection to New Zealand under this option makes it reasonable to regulate what the entity does here.	**0** Does not provide sufficient certainty on the test that should be applied. Raises comity concerns.

(3) Definition of news medium and news activity

	Status quo (Option 1)	Option 2 (broaden the definition of news activity)	Option 3 (broaden the definition of news activity and change the definition of news medium to recognise news media that are subject to standards)
Certainty	**0**	+ Provides greater clarity about 'news activity' but may not be sufficiently broad as to extend to books.	+ Provides greater clarity about 'news activity', but may not be sufficiently broad as to extend to books.
Trust and confidence	**0**	- Reduces privacy considerations for individuals because more forms of news media caught within the exemption, and these may not be subject to media standards. Complainants could only seek common law remedies.	+ Individuals still have access to remedies through the complaints procedure set up by the standards body.
Freedom of expression	**0**	+ Broad protections for all forms of news media.	**0** Media held to appropriate standards will be privileged; those not subject to an independent regulator will not be able to use the exemption any longer.
Overall assessment	**0**	**0** Insufficient privacy protections.	+ Balances freedom of expression and individuals' privacy protections, by ensuring there is effective oversight of media claiming the exemption, and that individuals have access to remedies if their privacy is breached.

(4) Applying the news medium exemption in full to RNZ and TVNZ

	Status quo	Option 1 (bring RNZ and TVNZ fully within the media exemption)
Certainty	**0**	+ Treats all media similarly.
Trust and confidence	**0**	- People will not have access and collection rights under IPPs 6 and 7. These rights are infrequently exercised.
Freedom of expression	**0**	+ Allows RNZ and TVNZ to undertake their news activities without reference to IPPs 6 and 7 which supports freedom of expression.
Overall assessment		+ Provides an operational level playing field for all media and supports journalistic freedom.

Conclusions

What option, or combination of options, is likely best to address the problem, meet the policy objectives and deliver the highest net benefits?

(1) The threshold for a notifiable privacy breach

The preferred option is a combination of options 1 and 2. The threshold for notification would be increased so that agencies would need to notify the Commissioner and affected people of breaches that a reasonable person would conclude are likely to cause serious harm.

The combination of 1 and 2 would most effectively respond to the concerns raised by submitters about over-notification and the need for increased certainty. Trust and confidence in the notification regime should be increased by ensuring that individuals are alerted to take any necessary action when notified of a serious risk of harm from a privacy breach. The preferred option should provide greater certainty about the workability of the regime, and the approach to assessing the potential harm arising from a breach. The preferred option may also encourage agencies to proactively take mitigating actions to minimise any serious risk of harm, if such steps may mean that notification is no longer needed.

(2) The Bill's application to agencies based overseas

Option 2: Clarify the territorial application of the Bill in a manner analogous to the Australian Privacy Act 1988. This option would, in particular, make it clear that the Bill applies to:

- agencies that are resident in New Zealand in respect of all of their conduct, inside *and outside* New Zealand, and
- agencies that carry on business in New Zealand in relation to conduct engaged in in the course of carrying on the agency's New Zealand business.

Carrying on business is a form of connection with New Zealand that involves systematically and deliberately taking advantage of the opportunity to engage in trade here, in a manner and to an extent that makes it reasonable to regulate what the entity does here. It aligns with the approach taken in Australia and in other New Zealand legislation.

(3) Definition of news medium and news activity

Option 3: broaden the definition of news activity and change the definition of news media to recognise news media that are subject to a standards body.

This option would broaden the definition of news activity, so that it could include books and online platforms such as blogs. The news media exemption is intended to support the free flow of news information; the content not the form is therefore the critical test. To ensure that there is effective oversight, and that individuals have access to remedies if their privacy is breached, we also recommend the broader definition of news activity apply only to news media that are subject to independent standards of conduct and complaints procedures.

(4) Applying the news media exemption in full to RNZ and TVNZ

Option 1: Bring RNZ and TVNZ fully within the news media exemption in the Bill. This option would allow RNZ and TVNZ to undertake their news activities freely, provide a level playing field for all news organisations, regardless of their ownership, and reduce compliance costs for RNZ and TVNZ.

Summary table of costs and benefits of the preferred approach for all issues identified above

Affected parties *(identify)*	**Comment**: *nature of cost or benefit (eg ongoing, one-off), evidence and assumption (eg compliance rates), risks*	**Impact** *$m present value, for monetised impacts; high, medium or low for non-monetised impacts*	**Evidence certainty** *(High, medium or low)*
Additional costs of proposed approach, compared to taking no action			
Regulated parties (all agencies)	Agencies that carry on business in New Zealand must comply with the Bill, whereas now that is not clear. This will increase compliance costs on some agencies. Agencies with poor privacy practices may need to improve them. There will also be some ongoing costs (e.g. they will have to notify the NZ Privacy Commissioner of privacy breaches related to their NZ business). News agencies currently exempt from the Privacy Act that are not subject to independent standards of conduct, will have to adopt appropriate standards to qualify for the Privacy Bill exemption.	Low-medium. This range is due to the wide range of agencies subject to the Act and the diverse nature of their activities, which directly influence their costs.	Low-Medium
Regulators (Privacy Commissioner)		Nil	Low-Medium
Wider government	None	Nil	Low-Medium
Other parties (individuals)	Individuals no longer have access and correction rights to information held by RNZ and TVNZ.	Low	Low-Medium
Total Monetised Cost	Unknown		Unknown
Non-monetised costs	Ongoing	Low-medium	Low-Medium
Expected benefits of proposed approach, compared to taking no action			
Regulated parties (all agencies)	Agencies are better able to judge when they need to notify a privacy	Low-medium	Low-Medium

	breach and need to notify less often – reducing compliance costs. Small reduced costs for TVNZ and RNZ in responding to complaints under both BSA and Privacy Act. TVNZ and RNZ on a level playing field with other media outlets. New media will benefit from clearly being able to claim the media exemption, provided they are subject to appropriate standards.		
Regulators (Privacy Commissioner)	Reduces costs of breach notification regime if fewer notifications of more serious privacy breaches.	Low	Low-Medium
Wider government	None	Nil	Low-Medium
Other parties (individuals)	The changes to mandatory breach notification and extra-territoriality contribute to increased trust and confidence in privacy protection. People are more likely to be able to take effective action in response to an interference with privacy as agencies carrying on business in NZ will clearly be subject to the Act.	Low	Low-Medium
Total Monetised Benefit	Unknown		Unknown
Non-monetised benefits	Ongoing	Low-medium	Low-Medium

What other impacts is this approach likely to have?
No impacts in addition to those outlined above.

Is the preferred option compatible with the Government's 'Expectations for the design of regulatory systems'?
Yes. The Bill includes reforms that will update and modernise New Zealand's privacy regime, including introducing new reforms such as the mandatory reporting of privacy breaches and a power for the Commissioner to issue compliance notices to require an agency to do something, or stop doing something. The Bill is expected to deliver significant benefits for New Zealanders. The additional reforms discussed in this RIS will further enhance the Bill and so support its overall objectives.

The changes to clarify the Bill's application to overseas agencies, or to align the breach notification threshold with comparable overseas jurisdictions meet the Government's expectations to maximise the benefits from trade and from cross border flows of people, capital and ideas. The changes to the news media exemption support the Government's expectation to produce consistent outcomes for regulated parties across time and place, and treat parties in a fair and equitable way.

Implementation and operation

How will the new arrangements work in practice?
The proposed changes to the Bill will be progressed through the Departmental report to the Justice Committee. The Ministry of Justice, the Office of the Privacy Commissioner and the Government Chief Privacy Officer will work together to communicate all the changes in the Bill to agencies. An implementation plan is being developed with implementation workstreams for each agency. The Commissioner will carry out his functions under the new laws from the date they are introduced. The Act is proposed to come into force six months after it receives Royal assent. This will provide agencies with the time needed to prepare for new procedures.

What are the implementation risks?
See above Section B: Summary Impacts: Benefits and Costs. No other risks have been identified.

Monitoring, evaluation and review

How will the impact of the new arrangements be monitored?
Monitoring and review arrangements for the impacts of all of the changes in the Bill as a whole are contained in the 2014 RIS and 2016 RIS, which details standard monitoring processes and legislative reporting requirements.

When and how will the new arrangements be reviewed?
See above.