

Regulatory Impact Statement: broadening notification requirement in the Privacy Act 2020

Coversheet

Purpose of Document	
Decision sought:	Analysis produced for the purpose of informing final Cabinet decisions.
Advising agencies:	Ministry of Justice
Proposing Ministers:	Hon. Kiri Allan, Minister of Justice
Date finalised:	28 March 2023

Problem Definition	
<p>There is an opportunity to further promote the principle of transparency in the Privacy Act 2020 (the Act) by ensuring that individuals are notified when their personal information is shared with other agencies. Currently, individuals are notified when their personal information is collected directly from them, but not when personal information about them is collected from another agency (the indirect collection issue).</p> <p>If no action is taken, there is risk of a widening ‘transparency gap’ where individuals are increasingly unaware of who holds their personal information. This is due to the increasing rate at which personal information is collected and shared, particularly given the growth of the digital economy. This in turn means New Zealanders will increasingly be unable to:</p> <ul style="list-style-type: none">• make informed privacy choices with respect to all of the agencies which have collected their information – for example to withdraw authority for their information to be shared with particular agencies;• hold agencies to account for their privacy practices; and• efficiently exercise their rights to access and correct their personal information as they may not know all of the agencies that have collected their information – these are fundamental rights under the Privacy Act and other international privacy regimes. <p>If no action is taken, a secondary problem is that New Zealand may become out of step with international best practice Section (9)(2)(f)(iv), Section 6(a), Section 9(2)(d).</p>	

Executive Summary	
<p>In May 2022, Cabinet agreed, in-principle, to amend the Act to address a gap Section (9)(2)(f)(iv) Section (9)(2)(f)(iv), Section 6(a), Section 9(2)(d) [CAB-22-MIN-0167]. EU adequacy is an assessment by the EU that a country’s domestic privacy regime offers an ‘adequate’ level of data protection as that afforded by the EU’s privacy framework. The gap relates to there being no requirement for agencies (public and private) to notify individuals when personal information has been collected about them from a source other than the individual themselves (‘indirect collection’). This means individuals may not know who holds their personal information in these circumstances.</p>	

The Ministry of Justice undertook public engagement on how best to address the gap between 24 August and 30 September 2022. Support for the proposals was mixed. While most submitters recognised the potential benefits to individual's privacy rights, there were concerns about the administrative burden of notifying individuals when their personal information is collected indirectly.

The Ministry of Justice recommends amending the Act to require agencies collecting personal information indirectly to notify individuals of the agency's name, contact details, and purpose for the collection. The notification would be broadly based on the current notification requirement for direct collection in the Act in Information Privacy Principle (IPP) 3. Agencies would be required to take reasonable steps to comply with the notification obligation as soon as practical after indirectly collecting the personal information.

This option would include a range of practical exceptions to the new notification obligation. These mirror many of the existing exceptions in IPP 3 to ensure efficient administration of certain public functions, ensure individuals are not overwhelmed with notifications, and protect against other unintended consequences.

The Ministry of Justice considers that this proposal will enhance the privacy rights of individuals and ensure New Zealand keeps up with international best practice. The new requirement will have some compliance costs for a range of public and private agencies. These include one-off costs associated with mapping information flows and in some cases setting up systems to notify individuals where their information has been collected indirectly.

Future guidance will be important in helping agencies understand which business practices will need to change. Some of these compliance costs, particularly in the private sector, are offset by the trade benefits these agencies enjoy from New Zealand having an internationally recognised privacy regime, including EU adequacy status.

Limitations and Constraints on Analysis

Previous Cabinet decisions

In May 2022, Cabinet agreed in-principle to amend the Act to address the transparency gap **Section (9)(2)(f)(iv), Section 6(a), Section 9(2)(d)**, subject to further policy work and consultation [CAB-22-MIN-0167].

Limited evidence on personal information flows

A key assumption underpinning our understanding of the problem is that individuals are currently unable to identify all agencies which collect their personal information indirectly. We assume this is quite widespread but are unable to quantify the scale of this in practice. One reason for this is that IPP 3 notifications already require notification of intended recipients. Feedback suggests that the level of detail when notifying individuals of intended recipients is highly variable. While some agencies may name the intended recipients, other agencies may list the types of intended recipients (e.g., marketing affiliates). However, given the scale of data sharing, and the fact that it is projected to increase, we consider a growing transparency gap to be a safe assumption.

Principle-based regulatory regime

In keeping with the information privacy principles in the Privacy Act, the options we have considered are principled in nature. While the options are also subject to a number of practical exceptions, we are unable to predict how the changes will apply in practice with great certainty. We anticipate operational guidance will be critical for giving agencies subject to the change sufficient detail to how the changes will impact their practices.

Compliance costs

The impact of the change is difficult to quantify due to:

- No precise data on the number of agencies which collect personal information indirectly. We estimate that most public agencies collect some personal information indirectly. Private sector agencies will share personal information to varying degree, however this practice is set to increase with the digitalisation of the economy and markets sustained by the trading of personal information.
- Uncertainty around changes each agency would need to do to comply with the change – some may already comply through their existing processes, while others may need to employ privacy and/or legal specialists and set up systems to notify individuals in order to ensure compliance. Our public and departmental engagement yielded limited insights into the actual costs for agencies. This may be because details of the proposed policy changes considered as part of these engagements were at a relatively high-level, and agencies will need time to determine which of their data transfers will be impacted.

Responsible Manager(s) (completed by relevant manager)

H Denoual

Hayley Denoual

Policy Manager

Electoral and Constitutional, Civil and Constitutional Policy

Ministry of Justice

30 March 2023

Quality Assurance (completed by QA panel)

Reviewing Agency:	Ministry of Justice
Panel Assessment & Comment:	The Ministry of Justice Regulatory Impact Analysis Quality Assurance Panel has reviewed the Regulatory Impact Statement prepared by the Ministry of Justice, and consider that the information and analysis summarised in the Regulatory Impact Statement (RIS) meets the Quality Assurance criteria. The RIS highlights that there is limited evidence on the problem leading to uncertainty on the exact level of compliance costs. The RIS clearly outlines how the proposal has been developed to consider as much as possible the practical concerns of stakeholders, and the benefits for stakeholders of ensuring our privacy regime in this area is sufficiently strong from an international perspective.

Section 1: Diagnosing the policy problem

What is the context behind the policy problem and how is the status quo expected to develop?

What is transparency?

1. Transparency regarding the collection, use, and disclosure of personal information is fundamental in protecting individuals' privacy rights and their dignity and autonomy. Transparency enables individuals to:
 - a. make informed privacy choices;
 - b. hold agencies to account for their privacy practices; and
 - c. exercise their privacy rights under the Privacy Act 2020 (the Privacy Act).
2. One of the keyways in which transparency is promoted in the Privacy Act is via Information Privacy Principle (IPP) 3. IPP 3 states that agencies are generally required to notify individuals when the agency is collecting their personal information ("direct collection of personal information").

How does the Privacy Act regulate the sharing of personal information in New Zealand?

3. The Act provides a framework for protecting individuals' rights to the privacy of their personal information, including the right of an individual to access their personal information.¹ It is a principles-based framework, consisting of 13 IPPs that govern how 'agencies' should collect, handle and use personal information. 'Agencies' in the Act refers broadly to public and private organisations and businesses.
4. The Act establishes the Privacy Commissioner as the regulator. The Commissioner has a range of functions including educating on the IPPs, ensuring compliance with the IPPs and issuing codes of practice (which allow certain groups of agencies to deviate from the IPPs among other things).
5. The Act provides particular information privacy principles for the collection and disclosure of personal information essential for the data flows described above. Relevantly:
 - **Information Privacy Principle 2** provides that when an agency collects personal information it must generally do so directly from the individual to whom that information relates ('the individual concerned'), unless certain exceptions apply. These exceptions include when the information is publicly available, for law enforcement purposes, or when it is not reasonably practicable in the circumstances to collect the personal information directly from the individual.
 - **Information Privacy Principle 3** provides that when an agency collects personal information directly from the individual, the agency must take reasonable steps to ensure the individual is aware of key matters immediately before the information is collected, or as soon as possible afterwards ('notification requirement'). This includes matters such as:

¹ See Privacy Act 2020, s.3.

- i. the fact that the information is being collected;
- ii. the purposes for collection; and
- iii. whether supplying personal information is voluntary or required by law.

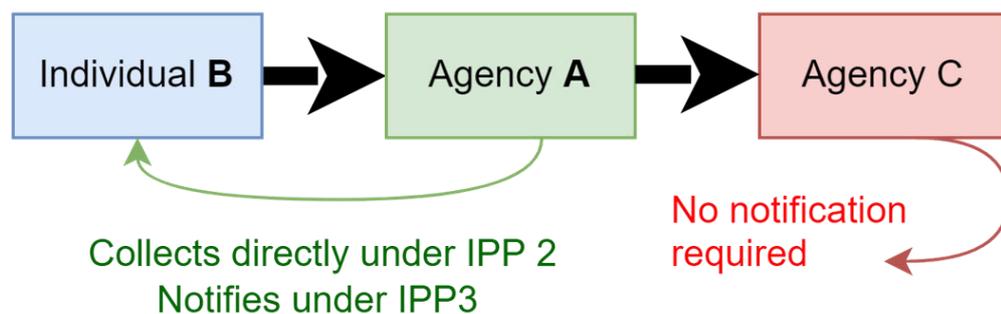
This notification might take the form of a statement on a paper document provided to the individual or stated on a website the individual can view.

As with IPP 2, exceptions to IPP 3 mean that agencies do not need to notify individuals of the collection of their personal information in certain cases, for example where an agency reasonably believes that non-compliance would not prejudice the interests of the individual concerned.

- **Information Privacy Principle 11** allows an agency to disclose personal information it holds, under specific conditions. Some disclosures involve the individual concerned being informed of the disclosure (such as when the individual authorised it) but others do not. For example, if the agency believes on reasonable grounds the disclosure is directly related to the purposes for which the information was originally obtained, it may disclose the information without informing the individual concerned.

What is indirect collection? What is the concern with indirect collection of information?

- 6. Indirect collection occurs when an agency collects information about an individual from a source other than the individual themselves.
- 7. Suppose Agency A already has Individual B’s personal information, as Agency A collected it for its own purposes. Agency A is now transferring it to Agency C who will use it for its own purposes. The transfer of information from Agency A to Agency C must comply with IPP 11 (disclosure) and IPP 2 (collection).



- ✓ Individual B informed about Agency A
- ✗ Individual B not informed about Agency C

- 8. Under current IPP 3 requirements, Agency C would not need to notify Individual B that it obtained their personal information from Agency A. Therefore, Individual B may not know that Agency C has their personal information, depending on the scope of Agency A’s initial notification and whether the disclosure to Agency C was authorised by the

individual.² While Agency A is generally required to notify Individual B of the agencies that it intends to share Individual B's personal information with, Agency A will not always be in a position to know all the future recipients of that information and intended recipients may change over time.

9. This creates a gap in the current notification regime, meaning the Act's transparency protections are less effective where personal information is not collected directly from the individual concerned. This poses risks of the following two outcomes occurring:
 - a. A widening 'transparency gap' where an individual's personal information is shared with and by third parties – this means individuals do not necessarily know which agencies have collected their personal information and so are less able to make informed privacy choices, hold the collecting agency to account and exercise their rights under the Privacy Act.
 - b. Becoming out of step with international best practice Section 9(2)(f)(iv), Section 6(a), Section 9(2)(d). This is discussed further in the next section.

International transfers

10. Sometimes New Zealand agencies are collecting personal information from overseas agencies. Suppose Agency A is an overseas agency and Agency C is a New Zealand based agency. Regardless of how Agency A came about collecting individual B's personal information (for example, under different privacy regulations), where practical, full transparency means the overseas individual should still be made aware about the collection of their personal information. The importance of targeting these kinds of cases is outlined in the following two sub-sections.

What are the notification requirements in other jurisdictions?

11. Many jurisdictions are considering or have already introduced broader notification requirements for indirect collection of personal information.
12. A significant example of this is the General Data Protection Regulation ('GDPR'), the key privacy law of the European Union ('EU'). The GDPR requires that an individual be informed of the processing of their personal information regardless of whether it is collected directly or indirectly, and in a clear and accessible form. This notification requirement is seen as a key protection for EU individuals when their personal information is shared.
13. Australia's Privacy Act 1988 Privacy Principle 5 provides generally for notification, regardless of the manner of collection.

² This example assumes a principal-principal transfer. We are not targeting principle-agent transfers. Sometimes Agency A asks Agency C to collect Individual B's personal information on its behalf. Agency C collects Individual's B personal information and then passes it on to Agency A. Agency C does not use this personal information for its own purposes, and it is only used by Agency A for its own purposes. In this scenario Agency A is the principal and Agency C is its agent, and the transfer of information from Agency C to Agency A is not considered a disclosure (Section 11 of the Privacy Act 2020).

Under a principal-agent relationship, Individual B's personal information is to be treated as being held by Agency A. Consequently, Agency A will be considered as the agency collecting such personal information, albeit through an intermediary. Therefore, the obligation to notify Individual B under IPP 3 lies with Agency A. Practically speaking, Agency A would often ask Agency C to notify Individual B on its behalf at the time of collection.

14. The United Kingdom Data Protection Act 2018 sets out a general notification obligation applicable to agencies collecting personal information, including collecting it indirectly (see Section 44(3)).
15. Both Japan and South Korea have recently introduced additional safeguards surrounding the notification rules for organisations indirectly collecting personal information of EU individuals.

Trade benefits of keeping up with international best practice

16. In addition to enhancing the privacy rights of individuals who benefit from the protection of the Privacy Act, having a strong privacy regime puts New Zealand in a stronger position when entering into trade negotiations and reduces barriers to trade.
17. A significant example of this is the trade benefits New Zealand enjoys from its EU adequacy status. EU adequacy is an assessment by the EU that a country's domestic privacy regime offers an 'adequate' level of data protection as that afforded by the EU's privacy framework.
18. New Zealand's EU adequacy status allows businesses and agencies to receive personal information from the EU in compliance with the EU's General Data Protection Regulation (GDPR), without the need for more onerous safeguards (such as contractual clauses committing them to EU-equivalent standards of data protection³).
19. It provides significant benefits to New Zealand, including lower costs for businesses trading with the EU, and a reputation for being a country with a strong commitment to protecting privacy. It also provides opportunities to streamline data transfers with other non-EU countries. A number of New Zealand's key trading partners already have or are working towards similar regimes in-line with the EU, [Section 9\(2\)\(f\)\(iv\), Section 6\(a\), Section 9\(2\)\(d\)](#)

Previous decisions

20. [Section 9\(2\)\(f\)\(iv\), Section 6\(a\), Section 9\(2\)\(d\)](#), in May 2022 Cabinet agreed 'in principle' to amend the Act to strengthen the level of transparency where an individual's personal information is collected indirectly by third parties, [Section 9\(2\)\(f\)\(iv\), Section 6\(a\), Section 9\(2\)\(d\)](#) (SWC-22-MIN-0079 and CAB-22-MIN-0167 refer). Cabinet noted that, subject to consultation, such amendments are likely to take the form of changes to the requirements in the Act to inform the individual concerned as to the collection of their personal information.

³ The average compliance costs of UK businesses setting up Standard Contractual Clauses in the absence of being able to use an adequacy decision were estimated in November 2020 as: £3,000 (\$6,000) for a micro business, £10,000 (\$20,000) for a small business, £19,555 (\$39,110) for a medium business and £162,790 (\$325,580) for a large business. See New Economics Foundation and UCL European Institute, ['The Cost of Data Inadequacy: the Economic Impacts of the UK Failing to Secure an EU Adequacy Decision'](#), pp. 2 and 26.

What is the policy problem or opportunity?

21. There is an opportunity to further promote the principle of transparency in the Privacy Act by ensuring that individuals are notified when their personal information is shared with other agencies.
22. If no action is taken, there is risk of a widening ‘transparency gap’ where individuals are increasingly unaware of who holds their personal information. This is due to the increasing rate at which personal information is collected and shared, particularly given the growth of the digital economy, and the current inadequacy of regulatory mechanisms (specifically IPP 3 notices) to ensure individuals are aware of the agencies which have collected their information. This in turn means New Zealanders will increasingly be unable to:
 - make informed privacy choices with respect to all of the agencies which have collected their information – for example to withdraw authority for their information to be shared with particular agencies;
 - hold agencies to account for their privacy practices; and
 - efficiently exercise their rights to access and correct their personal information as they may not know all of the agencies that have collected their information – these are fundamental rights under the Privacy Act and other international privacy regimes such as the GDPR.
23. The benefits of addressing this gap for international trade are discussed above [paras 16-19].

Changing information landscape

24. The sharing (collection and disclosure) of personal information is an essential part of doing business both worldwide and in New Zealand. Businesses need to be able to collect personal information in order to offer or provide a wide range of goods and services to customers (such as running processes such as cloud-based email, Software-as-a-Service or file storage). Although some of this data will be collected directly from the individuals involved, large amounts of personal information is collected indirectly when it is shared by one business to another. This often occurs because agencies have sought agreement from the individual via their terms and conditions to share that person’s personal information in exchange for the goods or services they are providing – a practice which is widespread.
25. Market forces mean that the sharing of personal information is set to increase. Furthermore, the Government has committed to growing New Zealand’s digital economy, with an aspiration for businesses and organisations to innovate and increase productivity using digital technologies and data, and through enhancing digital trade and the exporting of services. We expect that this will mean a corresponding growth in the flow of personal information between businesses and public agencies both domestically and internationally.
26. Transfers of personal information are also widespread in the public sector and is essential to providing a joined-up approach to public services envisioned in the Public Service Act 2020.
27. When the IPPs were first developed, the point at which personal information was collected directly from the individual may have been considered the most important

point to ensure individuals are aware of what is happening with their personal information. Indeed, direct collection is the point at which an individual has the most control over what happens with their personal information. IPP 3 promotes some transparency as to future collectors of an individual's personal information by requiring agencies to make individuals aware of any intended recipients of that personal information. However, we know from engagement that agencies will often list the *kinds* of agencies they intend to share personal information with rather than specific agencies. It is also likely that intended recipients can change over time.

Stakeholder views

28. Public engagement was conducted between 24 August and 30 September 2022. The purpose of engagement was to identify risks, opportunities, and options for addressing the notification gap in the Act. The focus of the discussion document was on how best to plug the transparency gap and minimise unintended negative impacts rather than on the relative value of EU adequacy to New Zealand. For the engagement document and summary of engagement see: Ministry of Justice, '[Possible changes to notification rules under the Privacy Act 2020](#)', August 2022 and Ministry of Justice, '[Possible changes to notification rules under the Privacy Act 2020: Summary of Engagement](#)', December 2022.
29. We received 53 written submissions: 12 from public agencies; seven from private sector representative bodies; 21 businesses; four privacy lawyers/legal organisations; four academics/privacy experts; two NGOs; one university and two individuals. We also met with several government agencies including a session hosted by the Government Chief Privacy Officer where we discussed the changes with several government privacy officers and a session with representatives from Te Kāhui Raraunga Charitable Trust.⁴
30. Support for making a legislative amendment was mixed:
 - a. 24 submitters were positive about the change citing its benefits for improving transparency and enhancing consumer rights whilst calling for careful consideration of the exemptions.
 - b. 12 submitters had concerns about introducing a new obligation with most citing concerns about compliance costs and notification fatigue.
 - c. 14 submitters were from real estate industry and echoed the concerns of REINZ that the change would impact on the collection of unconditional sales data.
 - d. Three submitters were neutral about the proposals or asked further questions.
31. A few of the submissions opposing a change noted that their opposition was conditional on NZ maintaining EU adequacy.
32. The most commonly discussed implementation risks included:
 - a. **Notification fatigue.** If individuals receive too many notifications about collection of their personal information, they may simply ignore it or 'tune out'.

⁴ Te Kāhui Raraunga is a group that was set up to support the actions of the Data Iwi Leaders Group. Te Kāhui Raraunga has a partnership with Statistics New Zealand.

Instead of feeling that they better understand what is happening with their information, some individuals could feel overwhelmed and confused.

- b. **Compliance costs.** There will be costs associated with a new requirement to notify individuals of indirect collection. Businesses and other organisations may need to create new policies and processes to ensure they comply. There could also be practical difficulties in notifying an individual with whom an organisation does not have a direct relationship.
 - c. **Frustration of public functions.** There are a range of scenarios where a requirement to notify individuals of indirect collection could frustrate the public interest. For example, where personal information is collected in the course of a criminal investigation it will often be inappropriate to notify the individual concern that their information has been collected.
 - d. **Risks to other privacy principles.** If not designed correctly, a requirement to notify individuals of indirect collection could undermine other information privacy principles. For example, IPP 1 talks about personal information only being collected as necessary to fulfil some lawful purpose. This connects to the basic principle of information minimisation and minimises the adverse risks associated with an agency holding more information than it needs. For example, a privacy breach could harm an individual more than necessary if the agency was holding excess information about the individual.
33. A couple of the groups we engaged with discussed Treaty of Waitangi obligations in the context of the new change, in particular the need to ensure that additional administrative burdens to create a barrier to sharing of personal information with Māori groups for the benefit of Māori.
34. Submitters concentrated on a number of exceptions that could mitigate these risks (e.g., creating an exception where an individual has already been notified). Several submitters also discussed the standard for notification e.g., whether the requirement to notify could be subject to notification being reasonable in the circumstances.

What objectives are sought in relation to the policy problem?

35. There are two overarching objectives:
- a. Enhance individual's privacy rights. This primarily includes addressing the transparency gap when an individual's personal information is collected indirectly. Individual's need to know who has collected their information in order to exercise their other privacy rights (e.g., to correction).
 - b. Keeping up with international best practice. Keeping up with best practice enhances New Zealand's global trade influence. It gives overseas jurisdictions and customers confidence in engaging New Zealand-based services.

Section 2: Deciding upon an option to address the policy problem

What criteria will be used to compare options to the status quo?

- 37. The following criteria will be used to compare options to the status quo:
 - a. **Transparency** – to what degree is the individual kept informed of which agencies are indirectly collecting their personal information?
 - b. **International equivalence and associated trade benefits** – to what extent is the option equivalent to other internationally recognised privacy regimes and likely to confer trade influence? Further information about notification requirements in the EU, UK and Australia is provided in Appendix 1.
 - c. **Ease of administrating new notification obligation** – to what extent does the option add compliance costs and/or inhibit the transfer of data between agencies?
- 38. There are trade-offs to be made with these criteria. An option which scores highly on ‘transparency’, and ‘international equivalence’ is likely to impose additional burdens on agencies which mean that the option scores lower on ‘ease of administration’. We have weighted each criterion roughly the same in terms of its contribution to the best option overall.

What scope will options be considered within?

Options considered but discounted

Non-legislative changes

- 39. We have ruled out considering non-regulatory options, or existing mechanisms under the Privacy Act. Section (9)(2)(f)(iv), Section 6(a), Section 9(2)(d) [redacted]. OPC guidelines serve as a recommendation and best practice only; they are limited by the substantive provisions in the Act. In addition, the Code of Practice mechanism which is used under the Privacy Act for specified industries, agencies or activities, is unsuitable as a means of addressing the transparency issue.

Narrow application of change to data transfers to overseas information only

- 40. We have ruled out making a change to the Act that would only apply to personal information transferred from overseas. This would give other jurisdictions confidence that transfers of personal information to New Zealand would be transparent for their citizens without additional compliance costs for agencies handling New Zealanders personal information. We have ruled this option out because it does not meet the primary objective and would be administrable complex. We have also been guided by the engagement feedback which overwhelmingly supported a universal approach.

Narrowing grounds for indirect collection or disclosure

- 41. We have considered an option to narrow the grounds under which an individual’s information can be either collected indirectly or disclosed to another agency. This would involve narrowing the exceptions to IPP2 and/or 11. One public agency suggested narrowing one of IPP2 - (2)(a), (b) or (f). For example, IPP2(f) allows an agency to

collect information indirectly if doing so directly would not be reasonably practicable. This threshold could be raised so that direct collection would need to be impossible. This option effectively blocks transfers of personal information where a transparency interest cannot be satisfied. This option was ruled out because the current grounds for collecting indirectly and disclosing are relied on widely. We considered broadening the notification requirement in the Act provides more certainty to agencies than narrowing the grounds for collection or disclosure.

What options are being considered?

Option 1 – Counterfactual – No notification requirement for indirect collection of personal information

42. Under this option, the current regulatory regime for the collection of personal information under IPP 2 would apply. Although the individual will be made aware of intended future recipients of their information through the IPP 3 notice, it cannot be guaranteed that the IPP 3 notice will identify all the recipients.

Option 2 – Introduce a notification requirement for indirect collection

43. Under this option, individuals should generally be notified when their personal information is transferred from one agency to another. The obligation could sit with either the disclosing agency (option 2a), or the indirect collecting agency (option 2b). The sub-options are discussed further below. Importantly, options 2a and 2b align with the intent of many current privacy practices (e.g., the presumption of a relationship between agency and individual in order for the individual to exercise their privacy rights).

Content of the notification

44. Individuals should be made aware of the collecting agency's name, contact details and the purpose of collection. This is a narrower list of items than current IPP3 notifications which also include the fact that information is being collected and an individual's privacy rights (for example, the right to correct their personal information). We consider that name, contact details, and purpose are the minimum an individual should be provided with in order to promote transparency and not necessitate overly long notifications that would exceed, for example, the length of a standard text message. In practice, agencies will often list other relevant information as well in the new notification.

Circumstances of the notification

45. In line with IPP 3, the notifying agency would be expected to take reasonable steps to comply with the notification obligation. This rules out the need to notify individuals in situations where the notification obligation would be incredibly difficult to comply with. For example, where there is reason to believe that the individual's contact details are out-of-date, and it would involve disproportionate effort to update those details. The data minimisation principle (expressed in IPP 1) will likely colour the reasonableness standard such that an agency should not generally collect contact details solely for the purpose of meeting the notification obligation.
46. Where the transfer of similar personal information is routine, it is intended that agencies will be able to make an assessment about whether notification is reasonable on a use-case by use-case assessment rather than strict case-by-case assessment. Business rules or, in the case of public sector agencies, policy directives, can be used to set up the criteria and parameters for sharing so that approaches for particular classes of information can be streamlined.

Circumstances where notification is not necessary

47. In accordance with the current IPP 3, the notification requirement for indirect collection:
- a. would not be breached if the action of an agency is authorised or required under New Zealand law
 - b. may be exempted or modified in an Approved Information Sharing Agreement (AISA) approved or amended after the notification obligation commences
 - c. may be modified, exempted or its compliance prescribed by the Privacy Commissioner when issuing a Code of Practice; and
 - d. does not apply to an intelligence and security agency.
48. We consider notification for the transfer of personal information should not be required where notification is not currently required for direct collection. In line with IPP 3, the notifying agency is exempt from compliance with the notification obligation where it believes on reasonable grounds:
- a. *notification is not reasonably practicable in the circumstances of the particular case* (for example, if contact details are out of date and such details will be difficult to update) (IPP3 (4)(d)).
 - b. *lack of notification would not prejudice the interests of the individual concerned* (IPP3 (4)(a));
 - c. *not notifying is necessary: to avoid prejudice to the maintenance of the law; enforcement of law imposing a pecuniary penalty; for protection of public revenue and the conduct of court proceedings* (IPP3 (4)(b));
 - d. *notifying would prejudice the purposes of the collection* (IPP3 (4)(c));
 - e. *the information (I) will not be used in a form which identifies the individual concerned; or (II) will be used for statistical or research purposes and not published in a form that could be reasonably expected to identify the individual concerned* (IPP3 (4)(e));
49. Notification for the transfer of personal information raises further public interest concerns and so we consider additional exceptions should apply to the notification for indirect collection. These include:
- a. *The individual concerned already has the notification information or the notifying agency has recently taken reasonable steps to notify the individual of the notification information in respect of the same or similar information.* If an individual has already been notified that an agency will collect their personal information, for example as part of a current IPP3 notice, it is not necessary that they are notified again. Further, if personal information is routinely collected about an individual and the individual has been made aware of the agency's identity in recent notice relating to a similar collection, notification would not be necessary again.

This exception creates an incentive for agencies to 'frontload' notifications in IPP 3 notices where they can. Many agencies will already be complying with the requirement as the individual has already been provided details about intended recipients under the IPP 3 notice or when they authorise collection of their personal information under IPP 2. However, where this has not occurred, agencies will be able to reduce their administrative burden by 'frontloading' notifications through the IPP 3 notice provided when information is collected directly from the individual concerned by the primary collecting agency. Such

a notice could name not just the agencies the primary collecting agency will disclose the information to, but also the agencies which other agencies in the chain will disclose the information to.

This is likely to require a contractual arrangement between the various collecting agencies, but we understand is an approach used by agencies subject to the GDPR. It may also be facilitated by the records of disclosures which some agencies may keep for the purposes of complying with the requirement to inform all agencies when a correction of personal information is made under IPP 7. Such an approach will mean minimal additional notifications are required beyond the original IPP 3 notice and reduce the impact of 'notification fatigue' among the individuals concerned.⁵

- b. *Serious threat to life/health.* We propose another exception to address concerns that a notification to an individual about the collection of their personal information could pose risks to other people. This could occur, for example, where a vulnerable person discloses personal information about someone else to an organisation and a notification could threaten the vulnerable person's well-being. We propose an additional exception where notification poses risks to the interests of another person. This would be modelled on the current IPP 11(1)(f) which allows disclosure of personal information where there is a threat to someone's health.

The information is publicly available information. Publicly available information is currently exempt from the requirement to collect personal information directly from an individual under IPP 2(2)(d). Agencies are also free to disclose such information under IPP 11, subject to a fairness and reasonableness test. We consider publicly available information should not require notification when transferred in order to preserve the current position in the Act. Subjecting publicly available information to the new notification obligation would be a significant departure from the status quo.

- c. *Contrary to the interests of a child exception.* It is important that the interests of children are built into the design of the new notification obligation. We consider that particular consideration should be given to notification that might impact the interests of a child. We propose that the notification obligation would not apply where notification would be contrary to the interests of a child. This exception would be based on section 49 of the Privacy Act which is a ground for refusing a child's access to personal information.
- d. *Personal information is archived in the public interest and the archived information is not used for measures or decisions about particular individuals.* It will often not be practical to notify individuals when personal information about them is archived due to the age and number of individuals' personal information

⁵ We considered making it a requirement that agencies list the name and contact details of intended recipients in the original IPP3 notice (i.e., at the point of direct collection). This would minimise the impact of the notification requirement for indirect collection by requiring agencies to provide more information to the individual when their personal information is first collected. If individuals were told the name of all the agencies that their information will be shared with, then, when that information is eventually shared, the indirect collecting agency would not need to notify again. However, we consider that this approach could have some unintended consequences, including significant practical implications beyond the current proposed change. For example, if the intended recipients are uncertain or likely to change, then agencies collecting information directly from the individual may feel obliged to provide the individual with an exhaustive list of all the agencies they may possibly share the information with.

being processed. Archiving is often authorised and required by law and so will not be subject to the notification obligation. Nonetheless, for the avoidance of doubt, we propose an explicit exception where personal information is archived in the public interest and the archived information is not used for measures or decisions about particular individuals.

Agency responsible for making notification

50. The notification obligation could sit with either the disclosing agency (Option 2a), or the indirect collecting agency (Option 2b). In practice, and depending on the circumstances, either of the two agencies could agree that the other agency discharge the notification requirement. The question is one of legal responsibility. Another sub-option we considered but discounted was to place an obligation on both the disclosing and indirect collecting agency. This would ensure individuals know who holds their personal information by placing legal liability on both agencies involved in a transfer of personal information. This option also has strong equivalence with the GDPR. We have discounted this option because it creates complexity when an agency comes to consider an exception. The disclosing and collecting agencies may not be aligned when considering whether an exception applies. It is also more burdensome than either option 2a or 2b and would require more divergence from the current IPP framework.
51. **Option 2a - disclosing agency obligation.** Under this sub-option, an agency disclosing personal information about an individual to a collecting agency would be under an obligation to notify the individual of the indirect collecting agency's name, contact details and purpose of collection. The agency which collects the personal information will be under no obligation to notify the individual concerned but will still be bound to ensure the circumstances of that collection meet the requirements of IPP 2. The notification would apply before, or as soon as practicable after the personal information is disclosed.
52. **Option 2b - indirect collecting agency obligation.** Under this sub-option, an agency collecting personal information would be under an obligation to inform an individual of its identity, contact details and purpose of collection where it collects their personal information from disclosing agency. The disclosing party will be under no obligation to notify the individual concerned but will still be bound to ensure the circumstances of that disclosure meet the requirements of IPP 11 or another statutory provision. The notification would apply as soon as practicable after the personal information is collected.

Key for options analysis on pages 16 and 17

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

How do the options compare to the status quo/counterfactual?

	Option 1 – counterfactual	Option 2a – Obligation on disclosing agency	Option 2b - Obligation on collecting agency
Transparency	<p>0 There is some transparency through the notification requirement at the point of collection from the individual. However, there is a transparency gap when it comes to indirect collection.</p>	<p>+ Provides more transparency than the status quo by providing a presumptive requirement that individuals are notified when their personal information is disclosed to another agency.</p> <p>+ The agency disclosing personal information for the first time may already have a relationship with the individual concerned as they are the agency that collected the information directly from the individual. This relationship with the individual may make the notification more likely or more meaningful. Therefore, this option could provide slightly more transparency than option 2b. However, this consideration does not apply to further disclosures.⁶</p>	<p>+ Provides more transparency than the status quo by providing a presumptive requirement that individuals are notified when their personal information is collected from another agency.</p> <p>+ The receiving agency may be able to give the individual concerned a more informative explanation about what they are doing with the information.</p>
International equivalence associated benefits and trade	<p>Section (9)(2)(f)(iv), Section 6(a), Section 9(2)(d)</p> <p>██</p> <p>██</p> <p>██</p> <p>██</p>	<p>+ This option would bring New Zealand into alignment with other comparable jurisdictions, including those with EU adequacy status which require notification when personal information is disclosed by an agency.⁷</p>	<p>+ This option would bring New Zealand into alignment with other comparable jurisdictions, including those with EU adequacy status which require notification for indirect collection. Also, most similar to the Australian standard.⁸</p>

⁶ Option 2a may allow individuals to more efficiently exercise their privacy rights. The disclosing agency could be required to make notification before or as soon as practical after the transfer. When notification happens before the transfer, individuals may be in a better position to exercise their privacy rights especially if their personal information is transferred to multiple agencies. It would not be practical to have the indirect collecting agency make notification before it collects the personal information because the personal information will often include details necessary to make the notification such as contact details.

⁷ Alignment with Art 14 subsection 4.

⁸ Alignment with GDPR Art 14 subsections 1 – 3, and Australian Privacy Principle 5.

<p>Ease of administrating notification obligation of new</p>	<p>0</p>	<p>-- Costs for agency making notification</p>	<p>- Costs for agency making notification There are several reasons why this option may be easier to administer than option 2a including:</p> <ul style="list-style-type: none"> • Indirect collecting agency is in better position than disclosing agency to know whether notification to the individual concerned is necessary (or is exempted from notification). • Agencies not collecting contact details will generally not need to make notification. • This option is most similar to the Australian standard (APP 5) which may make it easier for New Zealand agencies who hold existing relationships with Australian agencies. • Agencies would uniformly be required to turn their mind to whether notification is necessary whether they are collecting directly or indirectly (as opposed to disclosing).
<p>Overall assessment</p>	<p>0</p>	<p>+</p>	<p>++</p>

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

53. Our preferred option is 2b. We first discuss why options 2a and 2b are preferable to option 1 (the counterfactual) and then discuss why option 2b is preferable than option 2a.

Options 2a and 2b provide greater net benefits than option 1

54. We consider the increase in transparency and international equivalence of options 2a and 2b outweigh the potential administrative burden. Options 2a and 2b have been designed to minimise the compliance burden on agencies by: subjecting the obligation to a reasonable test, including a number of practical exceptions, allowing the notification to be made in a flexible and context-sensitive way. Options 2a and 2b have certain equivalence to the requirements in other jurisdictions and New Zealand agencies can follow business practices developed overseas. Section 9(2)(f)(iv), Section 6(a), Section 9(2)(d)

[Redacted text block]

Option 2b provides greater net benefits than option 2a

55. Options 2a and 2b both ensure that individuals are aware of who holds their personal information in a wide range of scenarios. These options differ in where they place the legal obligation (i.e., with the disclosing or indirect collecting agency). In practice agencies involved in information transfers can enter contractual arrangements to have the other agency fulfil the notification obligation on its behalf.⁹ However, the design of these options means that they may differ in the level of transparency and the level of administrative ease.

Transparency

56. Overall, options 2a and 2b both provide a good level of transparency. There are very slight differences in the way that each option achieves transparency.

Administrative ease

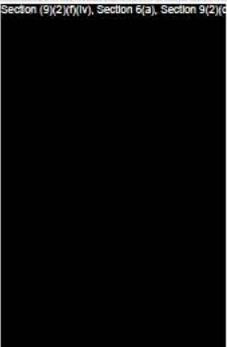
57. We think that option 2b performs better than option 2a with respect to administrative ease of compliance. The indirect collecting agency will often be in a better position than the disclosing agency to know whether an exception to notification should apply with respect to a particular transfer of personal information. For example, the indirect collecting agency will have a better idea about whether the personal information will be used in such a way that the individual concerned can be identified. Therefore, placing the obligation on the indirect collecting agency will minimise the need to communicate and negotiate whether notification is necessary in a particular case.

⁹ The distinction would make a more material difference where, for example, personal information is collected from publicly available sources. In this scenario, individuals may not be informed about who holds their personal information if the disclosing rather than indirect collecting agency was required to notify. However, we have proposed an exception to notification when information is collected in this way.

58. We evaluated option 2a as significantly worse than the counterfactual in order to show that option 2b is worse than the status quo but better than option 2a. However, given the design of option 2a, this potentially overstates the level of administrative burden.

What are the marginal costs and benefits of the option?

Affected groups (identify)	Comment <i>nature of cost or benefit (eg, ongoing, one-off), evidence and assumption (eg, compliance rates), risks.</i>	Impact <i>\$m present value where appropriate, for monetised impacts; high, medium or low for non-monetised impacts.</i>	Evidence Certainty <i>High, medium, or low, and explain reasoning in comment column.</i>
Additional costs of the preferred option compared to taking no action			
Public and private agencies regulated by the Privacy Act.	Initial costs for agencies associated with mapping information transfers and setting up systems to provide notification where necessary. Ongoing costs associated with making notification. The development of guidance and case-law will influence the intensity of the administrative burden.	Medium non-monetised costs. Most private and public sector agencies that collect personal information indirectly will incur some costs in order to comply. The compliance burden for these agencies are difficult to quantify owing to the range of ways that current obligations are fulfilled. Agencies will need to have an awareness of their data flows, recipients and intended uses of the personal information they collected. If they do not have a sufficient awareness to comply, their privacy officer and/or lawyers will need to assess the required level of compliance. However, this is not intended to be a strict case-by-case assessment. Business rules or, in the case of public sector agencies, policy directives, can be used to set up the criteria and parameters for sharing within each exception so that approaches for particular classes of information can be streamlined. Other agencies will need to create new policies and systems to notify individuals. This may involve, for example, sending emails to individuals when their personal information has been collected.	Low, both the number of agencies impacted and the impact on any given agency are unknown.
Office of the Privacy Commissioner (OPC)	One-off costs associated with producing guidance and communications, then small ongoing costs for OPC associated with	Low, OPC has a resourced policy function.	High, OPC have dealt with changes of similar magnitude in the past.

	ensuring compliance with higher standard.		
Individuals whose information is shared by agencies	Potential for notification fatigue on part of individuals.	Low un-monetised impact. Exceptions and business incentives should minimise excessive notifications.	Medium, we have some confidence that the exceptions and general customer-service incentives will mitigate impacts of notification fatigue.
Total monetised costs			
Non-monetised costs		<i>Medium</i>	
Additional benefits of the preferred option compared to taking no action			
Individuals whose information is shared by agencies	Individuals' privacy rights are enhanced.	Medium, changes represent a modest enhancement of transparency-related privacy rights.	Medium, while we do not know to what extent current IPP3 notices are providing full transparency, the change will create an important backstop even if IPP3 notices are promoting transparency well.
Exporting agencies	Agencies engaged in transfer of personal information from overseas will benefit from lower transaction costs associated with international equivalence. Other private agencies will benefit from the easier access to foreign markets associated with having a robust privacy regime.	Section 9(2)(f)(iv), Section 6(a), Section 9(2)(d) 	Section 9(2)(f)(iv), Section 6(a), Section 9(2)(d) 
Total monetised benefits			
Non-monetised Benefits		<i>Medium</i>	

Section 3: Delivering an option

How will the new arrangements be implemented?

Office of the Privacy Commissioner will lead on implementation

59. OPC will be the main agency responsible for implementation in accordance with its functions under the Privacy Act. This includes issuing guidance, educating agencies on compliance and ultimately monitoring compliance.

Agencies will benefit from a 6-month preparation period

60. We have proposed a 6-month commencement delay to give OPC time to develop guidance and agencies to become familiar with the change. Changes are expected to come into effect in early 2025.

Compliance tools and cost mitigations

61. The most significant assumption is the compliance burden on agencies. Feedback from private and public agencies was mixed on the impact of these changes on their operations. As discussed in the table above, most agencies will need to map their information flows and create systems to make notification where appropriate.
62. However, there are a range of mitigations which will be available to agencies which will assist with reducing the compliance costs associated with the notification obligation.
63. Primarily there is flexibility in how an individual may be notified, and reasonable periods within which it may occur meaning consolidated notices could be provided should the same individual require more than one notification.
64. Many agencies will already be complying with the requirement as the individual has already been provided details about intended recipients under the IPP 3 notice or when they authorise collection of their personal information under IPP 2. However, where this has not occurred, agencies will be able to reduce their administrative burden by 'frontloading' notifications through the IPP 3 notice provided when information is collected directly from the individual concerned by the primary collecting agency. Such a notice could name not just the agencies the primary collecting agency will disclose the information to, but also the agencies which other agencies in the chain will disclose the information to. This is likely to require a contractual arrangement between the various collecting agencies, but we understand is an approach used by agencies subject to the GDPR. It may also be facilitated by the records of disclosures which some agencies may keep for the purposes of complying with the requirement to inform all agencies when a correction of personal information is made under IPP 7. Such an approach will mean minimal additional notifications are required beyond the IPP 3 notice and reduce the impact of 'notification fatigue' among the individuals concerned.
65. There are also tools to assist agencies to comply with their obligations, for example, completing a Privacy Impact Assessment (PIA) in relation to their indirect collecting. This will help them to think about practical steps they can take to comply with a broadened IPP 3. In addition, OPC would expect agencies to have already conducted PIAs in respect of certain classes of information meaning there would be no additional costs in these circumstances.

How will the new arrangements be monitored, evaluated, and reviewed?

Office of the Privacy Commissioner

66. OPC will be responsible for issuing guidance, monitoring compliance in accordance with its functions under the Privacy Act.

Ministry of Justice

67. The Ministry of Justice will continue to have responsibility for ensuring New Zealand privacy law is achieving its objectives and will work with the Privacy Commissioner to ensure the change is working as intended. The Ministry of Justice (facilitated by MFAT) will continue to ensure New Zealand's privacy regime meets international standards.
68. We do not think that the implementation risks are high enough to justify an explicit post-enactment evaluation timeframe. Instead, the change will be monitored as part of continuous monitoring of the Privacy Act to ensure it is fit for purpose. In addition, and as discussed above, a notification requirement for indirect collection is common in comparable jurisdictions and the proposed change has a number of exceptions to mitigate against unintended consequences.

Appendix 1 - Notification requirements in the EU, UK and Australia

The EU

1. Article 14 to the EU's General Data Protection Regulation ('GDPR') requires agencies collecting personal information indirectly to notify the individual concerned of certain matters (e.g. the data agency's contact details, purposes of collection, individual's GDPR rights), all within a month of collection. This obligation is subject to the following exemptions:
 - 1.1. the individual concerned already has the information;
 - 1.2. the provision of such information proves impossible or would involve a disproportionate effort;
 - 1.3. obtaining or disclosure is expressly laid down by Member State law and which provides appropriate measures to protect the individual's legitimate interests;
 - 1.4. the personal data must remain confidential subject to an obligation of professional secrecy, including a statutory obligation of secrecy.
2. Article 14 further requires the agency to provide further information to the individual where processing of personal information for a purpose other than that for which it was originally collected is envisioned.
3. A different piece of EU legislation, rather than the GDPR, applies to the processing of personal information by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.
4. EU Member states may exempt certain activities from the GDPR, so long as such exemptions are specific and respect the essence of the fundamental rights and freedoms and are a necessary and proportionate measure in a democratic society to safeguard certain public functions.¹⁰

The UK

5. The UK's privacy laws currently mirror the GDPR, although it is expected the UK is likely to take a different approach to data protection in the future.
6. The UK exempted certain public functions from specific articles of its privacy laws. Under Schedules 2 and 3 of the Data Protection Act 2018, exemptions apply where compliance would prejudice the effective operation of the following functions:
 - 6.1. preventing or detecting crime, prosecution of offenders and collection of tax, including risk assessment systems;
 - 6.2. maintaining effective immigration control

¹⁰ These are (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; (e) other important objectives of general public interest of the Union or of a Member State; (f) the protection of judicial independence and judicial proceedings; (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; and (h) a monitoring, inspection or regulatory function connected to (a) to (e) and (g).

- 6.3. information required to be disclosed by law or in connection with legal proceedings
- 6.4. statutory functions or functions of a public nature designed to protect the public against financial loss, and to protect charities against misconduct or mismanagement
- 6.5. the statutory functions of commissioners such as the Public Service Ombudsman when investigating issues such as the maladministration of public bodies;
- 6.6. auditing functions;
- 6.7. the functions of the Bank of England; and
- 6.8. boards considering complaints regarding legal, health or children's services and health data processed by a court.

Australia

7. The Privacy Act 1988 applies to most entities ('APP entities') aside from small business operators ('small business' meaning businesses with a turnover of \$3 million or less in the previous financial year).
8. Under Australian Privacy Principle 5 (APP 5), an APP entity that collects personal information about an individual (either directly from that individual or indirectly from a third party) must take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters, including of the APP entity's identity and contact details, the fact and circumstances of the collection, its purposes and intended recipients.
9. The Office of the Australian Information Commissioner provided guidance on when it may be reasonable for an APP entity to not take any steps to provide a notice or ensure awareness of all or some of the APP 5 matters, such as:
 - 9.1. the individual is aware personal information is being collected and is informed of the purpose of such collection (e.g. when a doctor informs a patient a specialist to whom the patient is referred will obtain the patient's health information);
 - 9.2. an entity collects personal information from an individual on a recurring basis in relation to the same matter;
 - 9.3. Notification may pose a serious threat to the life, health or safety of an individual or pose a threat to public health or safety, or may jeopardise the purpose of collection (e.g. a law enforcement agency undertaking lawful covert surveillance in a criminal investigation);
 - 9.4. Notification would be inconsistent with another legal obligation (e.g. a statutory secrecy provision);
 - 9.5. The impracticability of notification, including the time and cost, outweighs the privacy benefit of notification (e.g. where an entity collects personal information about the individual's next of kin for emergency contact purposes).