MINISTRY OF JUSTICE
Tāhū o te Ture

Justice Centre | 19 Aitken Street
DX SX10088 | Wellington
T 04 918 8800 | F 04 918 8820
contactus@justice.govt.nz | www.justice.govt.nz

20 December 2022

Section (9) (2) (a)
Section (9) (2) (a)

Our ref: OIA 99969

Tēnā koe Section (9

Official Information Act request: Broadening the Privacy Act's notification rules

Thank you for your email of 12 October 2022, requesting under the Official Information Act 1982 (the Act), information regarding broadening the Privacy Act 2020's notification rules. Specifically, you requested:

> *...all responses or other feedback received in response to this recent consultation: justice.govt.nz/justice-sector-policy/key-initiatives/broadening-the-privacy-acts-notification-rules/.*

On 21 October 2022, you were advised of an extension on the timeframe for the request to enable additional time for the necessary consultations to take place.

The documents found that are in scope of your request are listed in the appendix. Copies of the documents themselves are attached. Some information has been withheld under section 9(2)(a) of the Act to protect privacy of natural persons.

In accordance with section 9(1) of the Act, I have considered the public interest in making available the information being withheld and determined that it does not outweigh the need to withhold the information at this time.

Please note that this response, with your personal details removed, may be published on the Ministry of Justice website at: justice.govt.nz/about/official-information-act-requests/oia-responses.

If you are not satisfied with this response, you have the right to make a complaint to the Office of the Ombudsman under section 28(3) of the Act. The Ombudsman may be contacted by phone on 0800 802 602 or by email to info@ombudsman.parliament.nz.

Nāku noa, nā

Kathy Brightwell
General Manager, Civil & Constitutional

MINISTRY OF JUSTICE
Tāhū o te Ture

Justice Centre | 19 Aitken Street
DX SX10088 | Wellington
T 04 918 8800 | F 04 918 8820
contactus@justice.govt.nz | www.justice.govt.nz

Appendix: Documents in scope

Number	Title	Comment
1	ACC – Submission on proposed changes to the notification requirements under the Privacy Act 2020	Released in full
2	ADLS – Possible changes to notification rules under the Privacy Act 2020	Some information withheld under s9(2)(a) of the Act
3	Allen-Baines – Re: Privacy Feedback	Some information withheld under s9(2)(a) of the Act
4	AWS – Re: AWS comments on possible changes to notification rules under the Privacy Act 2020	Some information withheld under s9(2)(a) of the Act
5	AREINZ – Proposed changes to notification rules under the Privacy Act 2020	Some information withheld under s9(2)(a) of the Act
6	Richard Best Law – Response to Ministry engagement on possible changes to the Privacy Act's notification obligations	Some information withheld under s9(2)(a) of the Act
7	BDO – Our Submission on the Proposed Changes to Notification Rules under the Privacy Act 2020	Some information withheld under s9(2)(a) of the Act
8	BNZ – BNZ's Submission to Possible Changes to Notification Rules Under the Privacy Act 2020	Some information withheld under s9(2)(a) of the Act
9	Bonnevie – Feedback on the Possible Changes to Notification Rules Under the Privacy Act 2020	Released in full
10	Centrix – Possible changes to notification rules under the Privacy Act 2020 Centrix Group Limited (Centrix) Submission	Some information withheld under s9(2)(a) of the Act
11	Chen – Submission on possible changes to notification rules under the Privacy Act 2020	Released in full
12	Chorus – Possible changes to notification rules under the Privacy Act 2020	Released in full
13	Crockers – Proposed changes to notification rules under the Privacy Act 2020	Some information withheld under s9(2)(a) of the Act
14	New Zealand Customs Service – Broadening the Privacy Act's notification rules	Released in full
15	Data Insight – Feedback on changes to Privacy Act 2020	Some information withheld under s9(2)(a) of the Act

16	Paul Davies Law – Feedback	Some information withheld under s9(2)(a) of the Act
17	Property Brokers – Feedback submission regarding third party authorization	Some information withheld under s9(2)(a) of the Act
18	Dentons Kensington Swan – Feedback – Possible changes to the notification rules under the Privacy Act 2020	Some information withheld under s9(2)(a) of the Act
19	Department of Internal Affairs – Feedback - possible changes to notification rules under Privacy Act 2020	Some information withheld under s9(2)(a) of the Act
20	Ministry of Education – Ministry of Education submission to the Ministry of Justice on the proposed changes to notification rules under the Privacy Act 2020	Released in full
21	Equifax – RE: Possible changes to notification rules under the Privacy Act 2020	Released in full
22	Financial Services Federation – Re: Broadening the notification requirements under the Privacy Act 2020	Some information withheld under s9(2)(a) of the Act
23	Harcourts – Submission on changes to notification rules under the Privacy Act 2020	Some information withheld under s9(2)(a) of the Act
24	ICNZ – Submission on Broadening the Privacy Act's notification rules	Some information withheld under s9(2)(a) of the Act
25	IR – Inland Revenue submission in response to the Ministry of Justice consultation on the broadening of the Privacy Act's notification obligations	Released in full
26	Feedback on your Privacy engagement document	Some information withheld under s9(2)(a) of the Act
27	New Zealand Marketing Association – Observations on the possible changes to notification rules under the Privacy Act 2020	Some information withheld under s9(2)(a) of the Act
28	MBIE – Submission in response to the Ministry of Justice's consultation on possible changes to notification rules under the Privacy Act 2020	Released in full
29	MSD – Ministry of Social Development Response - Introduction	Released in full
30	NZ Realtors Network Ltd – Submission: Possible changes to notification rules under the Privacy Act 2020	Some information withheld under s9(2)(a) of the Act
31	NZBA – Engagement Document: Possible changes to notification rules under the Privacy Act 2020	Released in full
32	NZSIS – RE: Privacy Act changes	Released in full

33	NZT – Proposed changes to the Privacy Act 2020	Released in full
34	Ombudsman – Consultation on indirect collection of personal information by third parties	Released in full
35	OT – Oranga Tamariki—Ministry for Children feedback on proposed changes to notification rules under Privacy Act 2020	Released in full
36	Plasier – Subject: Privacy act notification rules	Some information withheld under s9(2)(a) of the Act
37	Atamira Platform Trust – Feedback on the possible changes to notification rules under the Privacy Act 2020	Some information withheld under s9(2)(a) of the Act
38	Privacy Commissioner – Submission in response to the Ministry of Justice consultation on the broadening of the Privacy Act's notification obligations	Released in full
39	Privacy Foundation NZ - Submission on Proposed Amendments to the Privacy Act	Released in full
40	Property Brokers – Proposed changes to notification rules under the Privacy Act 2020, Submission in support of REINZ submission	Some information withheld under s9(2)(a) of the Act
41	RayWhite – Proposed changes to notification rules under the Privacy Act 2020	Some information withheld under s9(2)(a) of the Act
42	REINZ – REINZ Submissions: Proposed changes to notification rules under the Privacy Act 2020	Some information withheld under s9(2)(a) of the Act
43	Restaurant Association of New Zealand – Submission Broadening the Privacy Act's notification rules	Released in full
44	Proposed changes to the notification requirements in the Privacy Act 2020	Released in full
45	Dr Paul Roth – Privacy Act Notification Submission	Released in full
46	Monarch Real Estate Limited – Proposed Changes To Notification Rules Under Privacy Act 2020	Some information withheld under s9(2)(a) of the Act
47	REINZ Ambassador South Auckland – Privacy Act Engagement	Some information withheld under s9(2)(a) of the Act
48	RayWhite Greerton – Possible Changes to Notification Rules Under the Privacy Act 2020	Some information withheld under s9(2)(a) of the Act
49	Spark – Possible changes to notification rules under the Privacy Act 2020	Released in full
50	Stewart – Possible changes to notification rules under the Privacy Act 2020	Some information withheld under s9(2)(a) of the Act

51	Te Whatu Ora – Proposed changes to notification rules under Privacy Act 2020	Released in full
52	Thom – MOJ submission	Released in full
53	Unity – Unity Submission - Broadening the Privacy Act's Notification Rules	Some information withheld under s9(2)(a) of the Act
54	University of Canterbury – Broadening the Privacy Act's notification rules - Submission	Released in full
55	Draft submission for broadening of notification requirements of the Privacy Act	Released in full

He Kaupare. He Manaaki.
He Whakaora.
prevention. care. recovery.

Submission on proposed changes to the notification requirements under the Privacy Act 2020

Executive Summary

ACC welcomes the opportunity to provide feedback on the proposed reforms to the notification requirements of the Privacy Act 2020 (**the Act**).

ACC also welcomes any appropriate measures aimed at balancing the needs and rights of individuals with the regulatory burden on agencies covered by the Act.

ACC is supportive of the Ministry of Justice (**the Ministry**) continuing to ensure the requirements of the Act are appropriate in light of the expanding use of technology, the internet, internet browsers, social networks and remote data storage solutions. ACC is also supportive of any appropriate measures that increase jurisdictional consistency.

Notice is a fundamental privacy tool and done well can be very effective. Its function and purpose, however, needs to be understood. It supports the principles of transparency and accountability. It also enhances trust. While improvements to the notice model are in principle welcome, any reform needs to be fit for purpose for the collection, use and disclosures of all agencies who are covered by and must comply with the Act.

Individuals are increasingly aware of and concerned by the sharing of their personal information with third parties, particularly in the absence of notice. Individuals are likely to lose trust in agencies which use their personal information for other purposes without prior notice.

We should also not lose sight of the fact that significant reform to the Act has recently been enacted. It is important that affected agencies are not overloaded, particularly in these challenging economic times and in the shadow of the COVID-19 pandemic.

The law is always being challenged by advancements in technology. With these advancements comes an increasing ability to collect, use and disclose personal information. The Act has – broadly speaking – been able to effectively respond. The increased digitisation of government and consumer centric services (including as a result of COVID-19) means the privacy protection framework will need to be reflective of how we all work in the "new normal".

It is in this complex and dynamic environment that the proposed review must proceed. Accordingly, clarity of the purpose of the reform is paramount. The concern about the heightened privacy risks to individuals stemming from the use and disclosure of personal information collected by third parties without the awareness of the individual is a valid one. However, what is unclear is how agencies are doing this, how often and in what sectors.

The justification for implementing a broader notification requirement to include indirect collection is unclear.

The Argument for change

As with any potential legislative reform there are two critical questions to consider. First, what are the key objectives of the reform and second, what is the most effective and fair approach to achieve those objectives?

Central to these considerations is how the reform will assist in providing a regulatory framework that strengthens (or at least maintains) privacy protection principles, clarifies obligations, protects the rights of individuals but also minimises the imposition of further regulatory burdens on agencies. Balancing these considerations will achieve a net benefit for all stakeholders.

The key features that underpin the current New Zealand privacy regulatory framework is that it is a principles-based and technology neutral law. This remains appropriate. Some prescription is helpful and code-making, guidance and advice is the preferred method of enabling compliance – particularly with sector specific issues.

Reform of the Act can also serve to address peoples changing expectations relating to privacy. There is a steady increase in the privacy awareness of people over a number of years, particularly in relation to the personal information that they share and the transparency expected from the organisations that they interact with[1].

What is unclear from the feedback requested is why the proposed reform is necessary at all. Put another way what is the problem that is trying to be corrected? Without this background it is difficult to provide constructive feedback.

The current notification requirements

In summary, the Act's current model is to require advice if the information is collected direct from the individual concerned, and authorisation if it is collected from a third party.

IPP2 makes it clear that unless an exemption applies the collection of personal information must be from the individual concerned. At times, agencies may collect personal information about an individual from another organisation or source, rather than from the individual the information relates to. To cover this situation IPP2 (2) (c) states that an individual may authorise the collection of their personal information from someone else. Accordingly, collection should therefore only be undertaken with the consent of the individual concerned unless another exemption applies[2].

It is clearly within the spirit of the Act (if not expressly prescribed) that agencies that collect personal information indirectly should take reasonable steps to make the individual aware of the IPP3 requirements as part of the authorisation they receive to do so. Doing so promotes transparency about information collection and ensures individuals are aware of their rights of access to the personal information that has been collected. Agencies are also currently not able to disclose information to a third party or use it in a manner other than the purpose for which it is collected without authorisation of the individual concerned[3].

ACC agrees that a generic statement on indirect collection or disclosure will have little effect on the positive promotion of transparency. This is because these types of generic statements fail to specify the type of information collected or its intended use, and who the information is being disclosed to.

---

[1] Deloitte Australia Privacy Index surveys.
[2] Unless one of the other exceptions apply which would also apply to the notice requirements of IPP3.
[3] Pursuant to IPP11 (gain unless an exception applies).

It is ACC's view that any reform should focus on the content of the "authorisation" required to collect information from a source other than the individual and narrowing the general exceptions to this to specific situations rather than imposing more burdensome notification requirements.

The Proposed Reforms

What is the concern with indirect collection of information?

ACC understands that the Ministry's concern relates to the interplay between IPP 2 and IPP 3, in that in some circumstances, when certain exceptions to IPP 2 or IPP 3 are utilised by an agency, personal information will not be collected directly from the individual concerned under IPP2, and there will be no notification requirement under IPP 3. As a result the individual concerned will no be aware of the indirect collection of their personal information and they will not be able to exercise their full privacy rights under the Act.

The Ministry give the following as an example of this: When an individual provides personal information via the website of a New Zealand agency, the terms and conditions of the website might indicate that the individual authorises the collection and sharing of their information when agreeing to use the website. That website may then share the individual's personal information with an advertising agency for advertising purposes. The advertising agency may not be required to notify the individual under IPP 3 because it did not collect the personal information directly, but rather received it from the website. This means the individual may be unable to exercise their full privacy rights (such as the right to request access to their personal information) under the Act from the advertising agency.

In ACC's submission the issue in this scenario is the extent of authority the individual gave to the website to share the information rather than notification of the collection by the advertising agency. It is always open to the individual to enquire with the website as to who it has shared, or intends to share, their personal information with and it is an obligation on the website to inform them. The website is not able to disclose the personal information to the advertising agency unless that was the purpose of its collection (in which case it will have advised the individual of this) or that disclosure is authorised by the individual[4]. The agency is also unable to collect the information indirectly without the authorisation of the individual concerned[5]. The issue identified here would only arise if there was reliance by both the website and advertising agency on exceptions to the requirements of IPP 2, 3 and 11.

This scenario does not appear to be one which justifies significant reform of the Act to address. If the outcome of this scenario is – as suggested by the Ministry – that the individual does not know about the collection by the advertising agency then either:

- the notification given by the website to the individual was insufficient[6] or
- the disclosure to the advertising agency by the website was unauthorised or
- the reliance on the exceptions was inappropriate.

The Ministry appears to be taking a very narrow and extreme interpretation of the privacy obligations of the agencies involved in this scenario and the associated lack of transparency.

[4] IPP 11 – Limits on disclosure of personal information.
[5] Unless an exception applies.
[6] In that it did not make the individual aware of the disclosure to the advertising agency.

The Feedback Requested

Question 1 – what factors do you think are most important when considering changes to indirect collection of personal information?

Requiring notification to the individual concerned where information is collected from a third party would be a very significant change to the collection principles, and should require a significant level of support from stakeholders to proceed.

No change was recommended when this was last considered in 2011.[7]In fact the word "directly" was removed from IPP 2 (1) and 3 (1) following the Law Commission's Review in 2011. It was considered that the word added nothing to the clarity of the IPPs and made no difference to the assessment of whether or not information can be collected from someone other than the individual concerned. Adding this back along with the word "indirectly" would similarly add no further clarity to the IPPs.

As indicated above, any response to any perceived problem needs to be proportionate. It does not appear that the Ministry has identified any general issue at present, and any problems in particular. It would be of great concern to ACC if the benefits of the change do not warrant the compliance costs that would be necessarily be involved.

For an agency such as ACC (and many other government agencies) that collects vast amounts of personal information (including health information) from various sources increased notification requirements would be impracticable in many instances and impossible in some. Agencies who collect information indirectly will not always have the contact information of the individual involved. To do so would require the collection of additional personal information – unrelated to the original purpose of collection – simply to address the notification requirement.

A requirement to notify people in cases where information is being collected from a third party could lead to further privacy breaches, as notification that particular information has been collected might go to the wrong person due to out of date contact details or human error.

The definition of "indirect collection" will also require significant consideration. As pointed out in the Law Commission report "indirect collection" could be as far reaching as the collection of images via CCTV cameras. It will need to be carefully constructed. There does not appear to have been any thought given to how this broader notification requirement would apply to Approved Information Sharing Agreements and MOU's (both current and future) through which government agencies share data. Exemptions from any notification requirements for these activities will be required in any reform.

ACC agrees with the Ministry that notification, consent and information fatigue is a real concern. An individual could be subjected to numerous notifications from various agencies in the course of the provision of a single low value or even free service. Where the information is health information it would be particularly distressing to an individual to receive repeated notifications about the collection of their sensitive information by other parties even when an essential part of providing the service requested.

The resources required to respond to communications from individuals (and associated complaints) following notification also needs to be carefully considered.

---

[7] 2011 Law Commission Report: Review of the Privacy Act 1993. Review of the Law of Privacy Stage 4. Pg 80.

Question 2 – What are the advantages or benefits of broadening the notification requirements?

It is accepted that broader notification requirements would support greater transparency, by helping individuals know what is happening with their personal information. This would give individuals more control of how their personal information is collected, used and shared by agencies, particularly online, which would also promote trust and safety. However, this will only be achieved if the proposed information to be conveyed in the notification has not already been provided to the individual as part of the authorisation to collect the information indirectly (as it should be).

That this is so is confirmed by the exceptions to the GDPR Article 14 notification requirements where the individual already has the information required. It is also accepted that greater consistency between the New Zealand and EU privacy regimes will be of benefit.

Question 3 - What form do you think the proposed changes to notification rules under the Privacy Act should take?

In ACC's view if the proposed reforms are to take place it should be in the form of an amendment to the current IPPs. This should take the form of a narrowing of exceptions (a), (b) and (f) of IPP2 as opposed to the addition of a new separate privacy principle or a new notification requirement to IPP3.

This could then be coupled with some prescription on the matters to be advised to the individual as part of an agency obtaining the authorisation required by IPP 2 (c). The desired protection could be achieved by amending IPP (2) (c) to state that in obtaining the individuals authorisation for the indirect collection they are to be informed of the matters in IPP (3) (1).

Narrowing the IPP 2 exceptions (a), (b) and (f) would reduce the type of conduct that it is assumed this proposed reform is attempting to address. As they currently stand, the exceptions require a subjective assessment by the agency who is not really in a position to assess what would prejudice the interests of the individual concerned and what constitutes reasonable practicability. If collection of the information directly would prejudice the purposes of collection this raises the issue as to whether the purpose is a proper one[8]. They could be replaced with similar notification exceptions to those contained in Article 62 of the GDPR being that the provision of information to the data subject proves to be impossible or would involve a disproportionate effort and that the individual has already received the information.

To be effective consent[9] the requirements of IPP3 should be included in the authority obtained by agency to ensure it is informed and meaningful. Consideration of the issue of consent is dealt with later in this response, however, as indicated above this appears to be the real issue in the scenario dealt with in Question 1 above.

Limiting the circumstances in which notification must be provided is also encouraged. An exemption in line with Article 14 of the GDPR which exempts the collector from the notification requirements where the provision of the notification proves impossible or would involve a disproportionate effort, is also supported.

It goes without saying that the notification requirements should not apply when the individual concerned already has the information that the agency is required to provide under the Act.

---

[8] Leaving aside legitimate indirect collections like for law enforcement purposes.

[9] Which is the purpose of the authorisation.

Indirect collection by law enforcement, for the protection of public revenue, legal proceedings, and to avoid threats to life should also continue to be facilitated without notification.

The proposed broader notification requirements should also not apply to circumstances in which an Approved Information Sharing Agreement or MOU exists.

Please elaborate on your preferred option and explain why you think the other options are not appropriate.

ACC's preferred amendment option would reduce the compliance burden on agencies.

Introducing new IPPs or adding additional blanket notification requirements for indirect collection will only add to the compliance burden on agencies. This burden would be disproportionate to any benefit and the perceived problem (if there is one). It will necessitate the collection and storage of additional personal information (to undertake the notification) and most likely lead to an increase in privacy breaches (by sending notifications to the wrong person), complaints and communications which the agency will need resources to deal with. This will be particularly so for agencies who hold vast amounts of personal information such as ACC.

The alternative proposal to expand IPP 3 to have generic notification requirement by changing the notification requirements to (for example) "if an agency directly or indirectly collects personal information about the individual concerned" would require additional exceptions, which, along with the current exceptions would mean the change would have little effect. It may, however, serve to allay some of the concerns in respect of GDPR adequacy.

Question 4 – if you are a New Zealand business or agency, are there any practical implementation issues you can identify in complying with the proposed changes?

The answer to this question is heavily dependent upon what the extent of the changes are. A blanket notification requirement for agencies who collect information "indirectly" would be a significant change, introducing a significant compliance burden and require the collection of additional personal information to meet these requirements.

The proposed reforms would significantly impact on data sharing under existing MOUs and AISAs that are in place and adversely affect the implementation of future arrangements. Government agencies are already providing transparency about this collection and use via their privacy policies and privacy statements which are publicly available and could provide further transparency by publishing MOUs (if they not already doing so).

A requirement for example that resulted in an obligation to make individual notifications to members of a shared data set ranging into the hundreds of thousands would be an absurd outcome. It is hard to envisage how this would practically work where there is ongoing sharing of information. Agencies would also not easily be able to pick up small changes to individual's personal information made in real time data sharing.

It is also of concern that these notification requirements may cause unnecessary alarm and information overload for individuals if they were to receive a notification every time a government agency shared their information. Government agencies are doing so to meet their statutory obligations rather than for commercial purposes.

Agencies wouldn't necessarily know who the individuals are in order to notify prior to collection from another agency. The personal information they collect initially may not include their contact details. The agency would then need to collect these details to meet these notification requirements.

There does not appear to be any principled basis for notification to be required where the shared info is only being used for statistical or research purposes.

Finally, any reform would also require amendments to be made to the various Codes of Practice including the Health Information Privacy Code.

Question 5 – are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?

In addition to the huge potential for notification and information overload and the compliance burden the practicality of implementing indirect collection notification requirements is another risk.

ACC agrees that if individuals receive too many notifications about collection of their personal information, they may simply ignore them, 'tune out' or worse choose not to purchase a service at all. Instead of feeling that they better understand what is happening with their information, some individuals could feel overwhelmed and confused. Where the information is sensitive this could cause distress and anxiety.

Obviously, the compliance costs associated with a new requirement to notify individuals of indirect collection is also of concern. Agencies will need to create new policies and processes to ensure they comply with the new requirements. There will also be additional resources required to deal with the correspondence generated by the agencies notifications and dealing with the practical difficulties in notifying an individual with whom an agency does not have a direct relationship.

The Act does not currently include explicit measures to mitigate the potential for information overload, however a number of regimes have established mechanisms aimed at reducing complexity and supporting a reduction in information burden.

GDPR Article 60 allows information to be provided to individuals 'in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing'.

In Australia, current OAIC guidance for APP 5 provides that 'a notice may also be provided in layers, from a full explanation to a brief refresher', and that 'privacy notices on forms or signs may be supplemented by longer notices made available online or in brochures'. In addition, OAIC guidance on data analytics suggests that organisations consider 'just-in-time' notices, video notices and privacy dashboards as a method of providing notice to individuals.

As indicated above, the practicality of notifying affected individuals in circumstances where there has been information/data sharing pursuant to an information sharing agreement needs to be considered. Agencies collecting data pursuant to these agreements simply do not have the required information to make the notification.

Some flexibility in the proposed notice requirements must be retained for situations where notice is unnecessary – such as where the individual is already aware of the matters that would be notified - and where providing notice would be impossible or would involve disproportionate effort or may actually be harmful.

Notification may also be unnecessary where third party collections occur exclusively to facilitate another agency's purpose[10]. It is not uncommon for agencies to engage specialist contractors to assist them with their business operations, where the purpose for which the personal information is being used has not

[10] Section 11 of the Privacy Act 2020.

materially changed and the risk of an individual getting notification fatigue from receiving multiple notices is high.

Question 6 – should the proposed changes only apply to personal information collected indirectly from individuals *overseas*, or should they also apply to personal information collected indirectly from individuals in *New Zealand?*

The proposed changes must include NZ individuals and not be limited to information collected indirectly from individuals overseas. Attempting to limit protections on a jurisdictional or country of origin basis is fraught.

It is noted that a New Zealand entity can fall under the scope of the GDPR currently when it offers goods or services to individuals in the EU. For example a New Zealand based web shop with a website that is available in German, French and English may process multiple orders a day from individuals within the EU and ship products to them. This will make them fall in the scope of the GDPR, even though they have no establishment in the EU and are not performing any data processing activities within the EU.

Another situation in which non-EU organisations can fall within the scope of the GDPR is when they are monitoring the behaviour of individuals inside the EU. This means that a NZ provider of a social network allowing users from within the EU to join, will fall within the scope of GDPR. The same goes for an app developer that decides to gather location data of EU citizens from their smartphones.

If the decision is made to apply the requirement only to information collected either from individuals overseas then this would risk placing New Zealand in contravention of Article 26 of the UN Covenant on Civil and Political Rights. This Article states that all people are entitled to equal protection under the law regardless of their national origin. New Zealand became a signatory to this covenant in 1968 and ratified it in 1978.

If there is an issue with indirect collection of personal information there does not appear to be any principled basis for restricting the increased protections to overseas individuals only.

Question 7 – is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback.

The purpose of notification

The notice requirements in IPP3 are intended to embed the provision of clear, transparent and concise notice of the collection of personal information and is an important component of a robust privacy regulatory regime. Effective notice can better align individuals expectations with the objectives and practices of agencies. It also helps to build trust.

Effective notice is also important for agencies seeking to receive meaningful informed consent from individuals, by supporting an individual to understand how their personal information will be used and disclosed prior to making the choice to authorise it.

Individuals place significant value on transparency and notice, particularly in relation to the collection, use and disclosure of their personal information[11]. When delivered effectively, notice will provide an individual

[11] See for example the Deloitte DPI survey undertaken in Australia where sseventy percent of respondents to the 2018 Privacy Index suggested that they have greater trust in brands with transparent and clear privacy notices. The 2019 Privacy Index found that 97% of Australians consider it important for organisations to provide clear and transparent notice of how their personal information will be used or disclosed.

with clear and concise information about matters including the identity of the organisation collecting their personal information, the purpose of collection as well as intended disclosures to other entities.

The provision of clear, concise, transparent and accessible notification when individuals authorise the sharing of their information would have the potential to reduce the existing discretion provided to agencies in the way that they communicate with individuals whilst significantly increasing the likelihood that they will understand the way that their personal information will be used and disclosed following its collection.

Making consent meaningful

It is acknowledged that the New Zealand privacy protection framework is not consent based. However, it is clearly contemplated as part of the authorisation of indirect collection, use and disclosure.

Meaningful authorisation/consent processes are important and effective tools for empowering individuals to control and manage their personal information. Providing consumers with greater control over their personal information fosters trust, which in turn results in positive outcomes for both individuals and agencies.

It appears that this is the real issue that the Ministry is attempting to address. This could be done within the current framework without major reform.

Meaningful consent should at least require a clear affirmative act that is freely given, specific, unambiguous and informed. This would align with the GDPR, which defines consent to be 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.

In 2018, our Chief Justice stated that privacy consents will prove to be a significant issue. In her lecture commemorating the first New Zealand Privacy Commissioner, Sir Bruce Slane, she said:

> *There is good reason for proceeding with caution when weighing the significance to be given to consent when assessing whether the individual expected privacy or had waived it. These are standard contracts people must agree to if they are to access services, sometimes essential services. Most do not read the full content of any such contract. That is especially so with online service providers. Although the privacy policy must be agreed to before services can be accessed, acceptance is easy — simply click on the accept button.*
>
> *Often the consequential authorised collection of data will occur in the course of a very low to no value transaction. Few would spend time reading a privacy policy before using a search engine or purchasing food to go. And yet by clicking accept, we are agreeing to all of the terms and conditions, if expressed in suitably plain English, contained in the privacy policy of the service provider. Even if we do read the privacy policy, it is doubtful we will have a full understanding of the implications of what we have agreed to. There is a very substantial asymmetry in technical understanding between the customer and most who operate business in an online world*

Long and complex privacy policies and notice requirements will more likely obscure rather than enhance transparency. Caution should also be exercised against introducing overly prescriptive notice requirements. The regulatory framework should provide enough flexibility to permit, and indeed encourage, a range of design practices that may be appropriate across a variety of contexts.

Final comment

ACC welcomes reforms to the Privacy Act that will increase transparency, promote privacy, better protect personal information and foster trust between consumers and agencies that collect their personal information.

In considering how the current system responds to the issue of indirect collection, any reforms to the notification requirements needs to remain practicable. Simply broadening the notification requirements in IPP3 would not resolve the perceived problem and would place a greater burden on industry while also overwhelming individuals who may subsequently suffer from 'notice fatigue' and 'information overload'.

The "indirect notification issue" should not be looked at in isolation. Due consideration should be given to the current authority requirements contained in IPP2 in respect of indirect collection and the restrictions on use and disclosure contained in IPP10 and the information contained in agencies privacy policies and statements.

Any amendments to the Privacy Act must ensure the regulatory burden is not disproportionate to the resultant benefit. It is difficult to identify the issue the Ministry is attempting to address and simply broadening the notification requirements may not have the desired effect. Any amendments will obviously have different effects on government agencies as opposed to commercial entities and striking a balance between these two sectors will also need careful consideration.

ACC thanks the Ministry for the opportunity to provide feedback on the proposals and looks forward to participating in future consultations.

ADLS
Connecting New Zealand Lawyers

Chancery Chambers
2 Chancery Street
Auckland 1010

PO Box 58
Shortland Street
Auckland 1140

DX CP24001

T 09 303 5270
F 09 309 3726
adls.org.nz

Possible changes to notification rules under the Privacy Act 2020

Submissions from the ADLS Technology and Law Committee

30 September 2022

1. INTRODUCTION

Direct collection of information occurs when information is collected directly from the individual whom the information is about. Indirect information collection occurs when information is obtained from someone other than the individual upon whom the information is about. While it is preferable to directly collect information from individuals, we submit that it is not always possible or practical.

The indirect collection of information can occur in numerous ways. For example:

a) Electricity suppliers indirectly collect information about the presence of dogs on the properties of account holders through its employees. This indirect collection of information contributes directly to the safety of workers and in some instances, improves the accuracy of information on file, thus possibly mitigating risks of physical harm.

b) One-time indirect collectors of information have been au horized when programs are moved between public bodies or from private sector organizations to a public body. The authority for indirect collections may also be sought, for example, to expand databases or to merge two databases to develop a more robust description of a particular population.

c) The collection of data by Statistics New Zealand is authorised under the Data and Statistics Act, 2022 and the information is provided to purchasers as well as subscribers.

d) Advertisers may gain access to data that is provided under advertising schemes from social media, as well as scraping technology.

e) Information is regularly and indirectly obtained in the collection and review by securities to verify and confirm investor and company securities behaviour.[1]

The above examples illustrate merely a few instances of the indirect collection of information. We submit that many other forms of indirect data collection also exist and in most instances, may fall short of the Information Privacy Principles Notification Rules[2] under the Privacy Act, 2020. In many instances, we are also aware that Government organisations are heavily involved in indirectly collecting information through data sharing and the cross checking of information for enforcement.

The Information Privacy Principles (IPPs)[3] provide clear information on how data is to be handled and collected, as well as the authorised means upon which data is to be handled

[1] Policies Procedures & Standards - Province of British Columbia (2022) *Section 27 - How personal information is to be collected* https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/how-personal-information-collected ; https://www.lawinsider.com/clause/indirect-collection-of-personal-information ; https://www.ipc.on.ca/wp-content/uploads/2016/11/num-14.pdf ; https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information

[2] With reference to Information Privacy Principles (IPP) 1 to 3 and 11.

[3] Ibid.

under the direct collection of information rules (which are subject to notification requirements). However, as identified, the IPP rules provide no guidance relating to obtaining information indirectly.

Currently, the Privacy Act, 2020 ("**the Act**") requires that agencies who directly collect personal information are generally required to notify the individual of such collection.[4] The notification requirement, however differs in the case of the indirect collection of personal information from agencies; namely when information is collected by an agency via a third party. Currently, a third-party obtaining information, does not have any obligation to inform an individual of the collection of said information.[5]

The Act is administered by the Ministry of Justice ("**the Ministry**") to create greater transparency and best practice, regarding the form and scope of the proposed changes regarding the indirect collection of personal information.

2. PROCESS OF ENGAGEMENT SO FAR

The Convenor of the ADLS Technology and Law Committee (**the Committee**) has actively engaged with members of the Committee regarding the commentary required. The members of the Committee are attorneys, policy advisors and practitioners who are skilled in the field of law and technology.

A contribution to this submission also been made by a member of the ADLS Immigration & Refugee Law Committee, who has contributed to this submission under the scope of information which is collected directly and indirectly in their area of expertise.

Due to a range of issues, both technical and legal, the ADLS Technology and Law Committee consider it appropriate to present submissions in this regard.

3. SUMMARY OF RECOMMENDATIONS IN THIS DOCUMENT

3.1 The definition of a "notice requirement" should be drafted to give effect to its intended meaning under the proposed submission. Also, the legislation must give effect to the understanding of the steps to followed when personal information is collected, both directly and indirectly.

3.2 The circumstances and situations upon which notice requirements arise, should be clearly articulated. Thus, the role of an agent must be clearly defined in respect of Information Pri acy Principle (IPP)2.[6]

3.3 The circumstances which give rise to a notification requirement by an agent must be clearly established. Such establishment would enable the process flow upon which the notification requirements under IPP3[7] would be applicable and thus creating certainty as

Privacy Act, 2020, Information Privacy Principle (IPP) 2.
[5] Ibid, Information Privacy Principle (IPP) 2 read together with Information Privacy Principle (IPP) 3.
[6] Ibid, Information Privacy Principle (IPP) 2.
[7] Ibid, Information Privacy Principle (IPP) 3.

to when IPP3[8] would come into effect, compared to that of direct collection of information.

3.4 The Committee suggests that the proposed enhanced requirement under IPP3[9], be dealt with under separate regulation/s, detailing specific requirements relating to the indirect collection of information. Due to the challenges relating to interpretation, as detailed in question one (1) above, the Committee avers that separate regulation/s would create clarity as to the expectations from an agent who receives personal information indirectly.

3.5 Ultimately, however due to the difficulties posed in all suggested changes by the Ministry of Justice, we contend and it is our preference is that the Information Privacy Principles remain as is.

4. DETAILED SUBMISSION

The Ministry has requested responses to seven (7) questions relating to the issue at hand. The feedback from the Committee has been directed to answering the questions posed.

4.1 What factors do you think are most important when considering changes to indirect collection of personal information?

From the outset, the Committee puts forward that the definition of a "notice requirement" should be drafted to give effect to its intended meaning under the proposed submission. Also, the legislation must give effect to the understanding of the steps to followed when personal information is collected, both directly and indirectly. This would inevitably assist the reasonable person in determining when a notification requirement is to be sent for the purposes of indirect collection of person information. At the forefront we submit that fairness, in proportion to the nature of the information, the context of collection and its potential use, are key factors in relation to the indirect collection of personal information.

The Committee further avers that the circumstances and situations upon which notice requirements arise should be clearly articulated. Thus, the role of an agent must be clearly defined in respect of Information Privacy Principle (IPP)2.[10] Further, the circumstances which give rise to a notification requirement by an agent must be clearly established. Such establishment would enable the process flow upon which the notification requirements under IPP3[11] would be applicable and thus creating certainty as to when IPP3 would come into effect, compared to that of the direct collection of information.

Should the above changes be affected, there would be significant understanding as to the definition and requirements for the indirect collection of personal information.

---

[8] Ibid.
[9] Privacy Act, 2020, Information Privacy Principle (IPP) 3.
[10] Privacy Act, 2020, Information Privacy Principle (IPP) 2.
[11] Ibid, Information Privacy Principle (IPP) 3.

4.2 What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?

The Committees puts forward that the general indirect collection of personal information from third parties, has inevitably less safe-guards and thus lower disclosure regimes. Legislated heightened controls would thus cast a greater safety net over the protection of personal information. The obvious advantage is to ensure informed consent when information is directly collected.

A major disadvantage identified, which has already been addressed in the Consultation Document for *Possible changes to notification rules under the Privacy Act 2020*,[12] is "notification fatigue". Where, in summary, an individual could experience largely negative connotations, based on an influx of privacy notifications.

A further disadvantage noted would include practicality controlling third-party actions to ensure that the holder of the information is notified in a meaningful way. Secondary collectors of information therefore may not have the ability to contact the individual providing the information. The overall consideration should be the proliferation of privacy related warnings and notices.

Further, the Commissioner proposes that the IPP rules are insufficient to handle indirect collection of data, and suggest the following amendment options:

1. ***An amendment to IPP 3 to introduce a notification requirement for all agencies covered by the Act. IPP 3 would be broadened so that it no longer applies only when an agency collects personal information directly from the individual concerned. It would apply when the agency collects the personal information indirectly from other sources.***

   We contend that an amendment to IPP3 would still leave gaps, a level of complication as well as burdensome execution. The sharing of information between organisations, such as Government departments can be voluminous, and may pose significant burden on an organisation confirming data for proper notification requirements. In addition, the data collected may be of an insignificant nature that does not trigger the refusal regime under s49 to 53 of the Act, but this cannot be discovered without a review of that data.

   We therefore consider that the proposed amendment to IPP3 is unworkable.

2. ***An amendment to one of the other IPPs, for example, an amendment to IPP 2 to narrow exceptions that allow agencies not to collect information directly from the individual concerned (i.e. that allow agencies to collect the information indirectly); or an amendment to IPP 11 to require a disclosing agency to notify the individual concerned that their information has been disclosed to a third party (regardless of whether or not the disclosure itself is allowed).***

[12] Refer to Page 4 .

The proposed amendment under option two provides a better way forward. The handling of information by a third party, or via an indirect collection of information, is better served where the handling party (since they are aware of what data they collected), informs individuals that that information has been passed to the new collecting agency. However, this is also fraught with difficulty as Government departments may inadvertently be hampered from law enforcement investigations through a disclosure of this nature.

Further, many advertising systems today provide indirect information release and terms of service contract out of that notification regime, if it is in fact enforceable at all due to jurisdictional considerations. Therefore, this option also has seve al areas instances it becomes unworkable.

4.3 Introducing a new separate privacy principle dealing with notification of indirect collection. In determining the notification rules, the following questions must be answered: If indirect information is collected, in what form was it collected?

It is our opinion that this option presents the best way forward. Based on several complexities to simply amend existing rules, a third rule needs to be developed that would separate and directly trigger a response regime of the notification requirements for data collected under indirect collection.

4.4 What form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate.

As detailed above, the Committee suggests that the proposed enhanced requirement under IPP3, be dealt with under separate regulation/s, detailing specific requirements relating to the indirect collection of information, refer to the discission points raised in point 2 (two) above.

Due to the mentioned challenges relating to interpretation, the Committee avers that separate regulation/s would create clarity as to the expectations from an agent who receives personal information indirectly.

4.5 If you are a New Zealand business, are there any practical implementation issues you can identify in complying with the proposed changes?

This aspect is not applicable to the submissions made by the Committee.

4.6 Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?

Such contentions have been detailed above.

4.7 Should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?

We submit that the proposed changes should be applicable to all who collect information, both onshore and offshore.

4.8 Is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback.

4.8.1 In consideration of the matter at hand, our preference is that the IPP rules remain as is. In this regard we refer to the Canadian based "Data Standards for the Identification and Monitoring of Systemic Racism"[13] which was established to "assist in the identification and monitoring of systemic racism and racial disparities within the public sector."[14]

These standards are said to "set out requirements for the collection, use, disclosure, de-identification, management, publication and reporting of information, including personal information."[15]

Interestingly, the agency holding the information and if such information is to be used, will automatically trigger the notification principals. In this regard, the Anti-Racism Act, 2017 (ARA) requires public sector organizations (PSOs) to provide different types of notice for direct[16] and indirect collection[17], and before they use personal information already in their possession that was collected for another lawful purpose.[18]

The applicable sections of such requirements are detailed below:

Part 2 - Notice – Indirect Collection

The ARA (s. 7(5)) requires that when personal information is collected indirectly, before collecting the information, the PSO must first publish the following information on a website:

- That the collection is authorized under the ARA;
- The types of personal information that may be collected indirectly and the circumstances in which personal information may be collected in that manner;

[13] Data Standards for the Identification and Monitoring of Systemic Racism (2022) https://www.ontario.ca/document/data-standards-identification-and-monitoring-systemic-racism
[14] Ibid *Introduction* https://www.ontario.ca/document/data-standards-identification-and-monitoring-systemic-racism/introduction
[15] Ibid.
[16] Refer to s. 7(4) of the Anti-Racism Act, 2017.
[17] Ibid s. 7(5)
[18] Ibid s. 9(5) *Notices* at https://www.ontario.ca/document/data-standards-identification-and-monitoring-systemic-racism/collection-personal-information#

- The purpose for which the personal information collected indirectly is intended to be used, including whether it will be combined with other information, including personal information; and
- The title and contact information, including an email address, of an employee who can answer an individual's questions about the collection.

Part 3 - Notice - Personal Information Already Collected Under Another Act

If the PSO is required or authorized to collect personal information under regulation, the organization may use for an ARA purpose other personal information it has lawfully collected. Before using the other personal information, the ARA s. 9(5) requires that PSOs provide public notice on a website stating that the use is authorized under the ARA, and:

- *The types of information that may be used and the circumstances it would be used, including whether it will be combined with other information, including personal information;*
- *The purpose for which personal information may be used; and*
- *The title and contact information, including an email address, of an employee who can answer an individual's questions about the use of the personal information.*

Part 4 - Notice - Individual Authorizes Another Person to Provide Their Personal Information

If an individual authorizes a PSO to indirectly collect their personal information from another person, the PSO must provide notice to the authorized individual in the same manner as in the case of direct collection (Part 1, above)

Part 5 – Notice of Rights to Access, Correct and Withdraw Consent

When giving notice, PSOs must also provide notice that individuals may access and correct their personal information, or withdraw their consent.

In the case of POI, notice must be provided that individuals may access the POI that relates to them and may request that a statement of disagreement be attached to the POI.

Thus, both direct and indirect collection, notice informs individuals about why their information is being collected and how it will be used. The process followed that enables those individuals to contact PSOs to obtains clarity regarding the collection and subsequent use of the information of their information.

It is important to highlight that notice is a critical aspect of obtaining express consent from the individual to collect and use personal their information.

Therefore, the individual understands the purpose of the collection, use and accept that providing their personal information is voluntary.[19]

4.8.2 Also, Information Privacy Principle Eight (8) relates to the accuracy of personal information held and places an obligation on an agent that holds personal information to ensure that such information is not used or disclosed without the agent taking reasonable steps to ensure that "the information is accurate, up to date, complete, relevant, and not misleading."

We submit that a test of reasonableness and proportionality in view of IPP8, could be extended from a heightened accountability perspective to include the following:

Such steps that are reasonable in the circumstances having regard to the nature and sensitivity of the information, the context of collection including any implied consent and its potential use.

---

[19] Ibid.

These standards also content the following in respect of Guidance:

Guidance

Notice may be given orally, in written form, or both. PSOs collecting POI (indirect collection) must give notice on their websites.

PSOs should provide individuals with supporting materials, such as nformative pamphlets or responses to frequently asked questions, particularly if notice is given orally.

PSOs should provide notice in a way that is inclusive and respon ive to the individual's needs and respects individual dignity. Notices should be:

- Concise and accessible, in accordance with the *Accessibility for Ontarians with Disabilities Act, 2005* (AODA) and its regulations;
- In plain language and readily understandable; and
- Available in alternative format and translations, as necessary.

Notices should inform individuals about what they are consenting to and why. PSOs should clearly explain the following:

- What information is being collected under the ARA;
- Why it is being collected;
- How it will be used, and whether it will be combined with other personal information; and
- Who will have access and how privacy will be protected.

- Forms used to collect personal information, if separate from the notice, should also state clearly that the collection is voluntary, and that no program, service, or benefit will be withheld if the individual does not provide or refuses to provide the information requested.
- Where a PSO's interaction with Indigenous peoples requires the application of a distinct legal analysis or process, PSOs should ensure that the client is also informed of the applicable provisions.
- The ARA provides that nothing in the ARA limits the right of an individual to access and correct personal information held by the PSO in accordance with the access and correction provisions of another Act (e.g. FIPPA or MFIPPA). In providing notice with respect to both direct and indirect collections, PSOs should inform individuals about any limitations to accessing or correcting their personal information or withdrawing their consent, if such limitations exist under another Act. Similarly, individuals should be informed of their ability to access and request a statement of disagreement to POI information held by a PSO. Individuals should be informed that the correction and removal of personal information does not have retroactive effect.

We content that the extension of the above reasonableness and proportionality test will sufficiently protect an agent from a potential floodgate effect of over-burdening obligations.

The ADLS acknowledges the contributions to this submission by the following members:

- Lloyd Gallagher (ADLS Technology and Law Committee)
- Andrew Easterbrook (ADLS Technology and Law Committee)
- Arran Hunt (ADLS Technology and Law Committee)
- Philip McHugh (ADLS Technology and Law Committee)
- Richard Small (Immigration and Refugee Law Committee)
- Vaheeni Naidoo (Committee Secretary)

5. CONCLUSION

Thank you for the opportunity to make submissions in respect of the proposed notification requirements.

To contact the ADLS Technology and Law Committee for clarification on any matters raised in this submission please contact me as the Committee Convenor:
s9(2)(a)

Lloyd Gallagher
Convenor, ADLS Technology and Law Committee

Carter, Adam

From: Greg Allen-Baines s9(2)(a)
Sent: Wednesday, 28 September 2022 1:37 pm
To: Privacy Feedback
Subject: Privacy Feedback

Re: Privacy Feedback

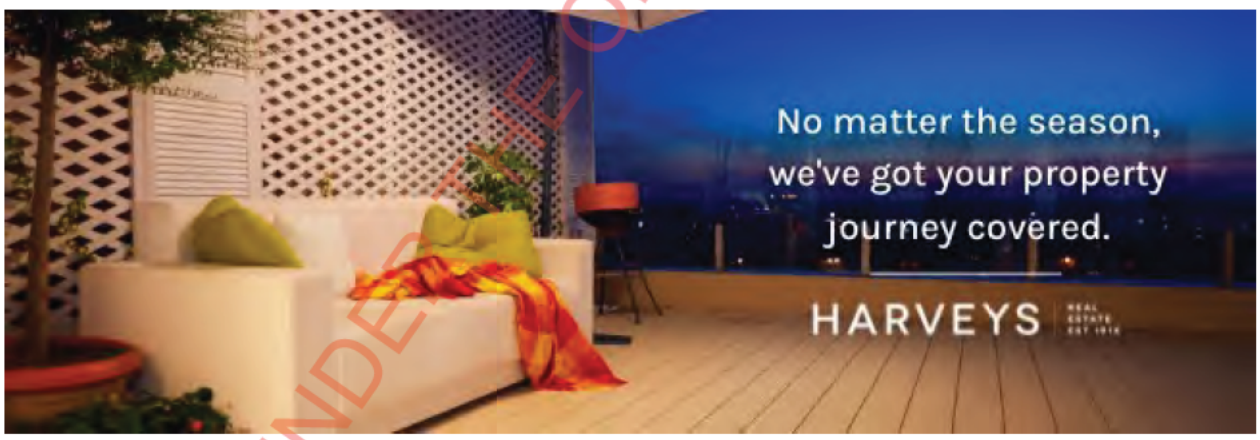
The response from the REINZ is, in my view, a very thorough response to the points raised by the Ministry of Justice, and I agree strongly with their (REINZ) response to all the points raised.

My contribution follows, and supports the things already said emphasising:

- We already have permission from our customers and clients to record, retain and use the information and this is contained in our Agency Agreements and the various Sale and Purchase do uments.
- With reference to New Zealand's effort to retain our adequacy status with the EU. It is my view that when the guidelines/rules, were put in place by the EU, it was to contain those countries that are less regulated than ours, in terms of our (New Zealand's) privacy laws. Anything further to what we have would definitely be too much, and in my view, work against our ability to go about our business as we are required to and to meet our statutory obligations, as we are required to.
- There is no need to reinvent the wheel.

Kind regards,

Greg Allen-Baines AREINZ
Licensed Agent REAA 2008
s9(2)(a)



Please do not print this email unless it is necessary. Every unprinted email helps the environment

Ministry of Justice
Justice Centre
Aitken Street
[by email privacyfeedback@justice.govt.nz]

30 September 2022

Re: AWS comments on possible changes to notification rules under the Privacy Act 2020

Dear Sir/Madam,

Amazon Web Services (AWS) is pleased to respond to the Ministry of Justice's *possible changes to notification rules under the Privacy Act 2020* consultation document which will inform the New Zealand government's review of the Privacy Act 2020. Please see two sets of comments from AWS at this time:

1. Importance of flexible, principles based notification requirements and practical guidance materials

The consultation paper notes that The Privacy Act 2020 may need to be revised to tighten the notification requirements in certain cases where a third party receives personal information and is currently exempt from having to notify that person. Increased notification requirements would seem appropriate if these exemptions are creating the gaps identified in the paper. If additional notification requirements are introduced into the Privacy Act 2020, we recommend that the Ministry of Justice aim to keep these sufficiently flexible and principles-based to allow for coverage of a wide range of situations. We also recommend that it be made clear that notification requirements relate to controllers of personal information, i.e. those that collect and use personal information.

We recommend that any changes to the Act be accompanied by clear practical guidance and examples for collectors of personal information. We note that the paper outlines some examples from Information Privacy Principles (IPPs) 2, 3 and 11, and we recommend that further examples be developed to help agencies better understand how to tighten their notification practices in order to minimise risks and enhance their privacy practices.

2. AWS Shared Responsibility Model

AWS does not have particular concerns about enhanced protection of personal information through additional notification requirements where personal information is being shared between controllers of information.

The Ministry of Justice may also find it useful to review material we have available about how the AWS Shared Responsibility Model operates with respect to privacy obligations of AWS customers that use AWS to store personal information as their own customer content. To help clarify customer and AWS responsibilities under the New Zealand Privacy Act 2020 we have provided detailed guidance for customers in our attached Whitepaper (appendix 1) *Using AWS in the Context of New Zealand Privacy Considerations, August 2021* (see especially pp.12-19). This Whitepaper can be found on our New Zealand Data Privacy website. Under the AWS Shared Responsibility Model, AWS customers retain ownership and control of their content when using AWS services. Customers determine what content they store or process using AWS services as well as where they choose to store their information. Given that the customer determines the purpose for collecting personal information, and controls the use and disclosure

of content that contains personal information, the customer is responsible for ensuring how such personal information is used or disclosed. AWS customers have the relationship with the individuals whose personal information they have collected and used , and therefore it is customers who are able to provide notifications in the event they share that information to a third party.

Thank you for the opportunity to comment in the early stages of this important work on the protection of personal information in New Zealand. We look forward to remaining engaged as the work continues.

Yours sincerely,

s9(2)(a)

Paul Keating
Head of Public Policy, New Zealand
Amazon Web Services

Using AWS in the Context of New Zealand Privacy Considerations

First published September 2014

Updated August 17, 2021

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

This document provides information to assist customers who want to use Amazon Web Services (AWS) to store or process content containing personal information, in the context of key privacy considerations and the New Zealand Privacy Act 2020 (NZ). It helps customers understand:

- The way AWS services operate, including how customers can address security and encrypt their content.
- The geographic locations where customers can choose to store content and other relevant considerations.
- The respective roles the customer and AWS each play in managing and securing content stored on AWS services.

Introduction

This whitepaper focuses on typical questions asked by AWS customers when they are considering the implications of the New Zealand Privacy Act on their use of AWS services to store or process content containing personal information. There will also be other relevant considerations for each customer to address. For example, a customer may need to comply with industry-specific requirements and the laws of other jurisdictions where that customer conducts business, or contractual commitments a customer makes to a third party.

This paper is provided solely for informational purposes. It is not legal advice, and should not be relied on as legal advice. As each customer's requirements will differ, AWS strongly encourages its customers to obtain appropriate advice on their implementation of privacy and data protection requirements, and on applicable laws and other requirements relevant to their business.

When we refer to content in this paper, we mean software (including virtual machine images), data, text, audio, video, images and other content that a customer, or any end user, stores or processes using AWS services. For example, a customer's content includes objects that the customer stores using Amazon Simple Storage Service (Amazon S3), files stored on an Amazon Elastic Block Store (Amazon EBS) volume, or the contents of an Amazon DynamoDB database table.

Such content may, but will not necessarily, include personal information relating to that customer, its end users, or third parties. The terms of the AWS Customer Agreement, or any other relevant agreement with us governing the use of AWS services, apply to customer content.

Customer content does not include information that a customer provides to us in connection with the creation or administration of its AWS accounts, such as a customer's names, phone numbers, email addresses and billing information—we refer to this as account information and it is governed by the AWS Privacy Notice. Our business changes constantly, and our Privacy Notice may also change. We recommend checking our website frequently to see recent changes.

Considerations relevant to privacy and data protection

Storage of content presents all organizations with a number of common practical matters to consider, including:

- Will the content be secure?
- Where will content be stored?
- Who will have access to content?
- What laws and regulations apply to the content and what is needed to comply with these?

These considerations are not new and are not cloud-specific. They are relevant to internally hosted and operated systems as well as traditional third-party hosted services. Each may involve storage of content on third-party equipment or on third-party premises, with that content managed, accessed or used by third-party personnel. When using AWS services, each AWS customer maintains ownership and control of their content, including control over:

- What content they choose to store or process using AWS services.
- Which AWS services they use with their content.
- The AWS Region or Regions where their content is stored.
- The format, structure and security of their content, including whether it is masked, anonymized or encrypted.
- Who has access to their AWS accounts and content, and how those access rights are granted, managed, and revoked.

Because AWS customers retain ownership and control over their content within the AWS environment, they also retain responsibilities relating to the security of that content as part of the AWS Shared Responsibility Model. This shared responsibility model is fundamental to understanding the respective roles of the customer and AWS in the context of privacy and data protection requirements that may apply to content that customers choose to store or process using AWS services.

AWS shared responsibility approach to managing cloud security

How is customer content secured?

Moving IT infrastructure to AWS creates a shared responsibility model between the customer and AWS, as both the customer and AWS have important roles in the operation and management of security. AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the AWS services operate.

The customer is responsible for management of the guest operating system (including updates and security patches to the guest operating system) and associated application software, as well as the configuration of the AWS-provided security group firewall and other security-related features.

The customer will generally connect to the AWS environment through services the customer acquires from third parties (for example, internet service providers). AWS does not provide these connections, and they are therefore part of the customer's area of responsibility. Customers should consider the security of these connections and the security responsibilities of such third parties in relation to their systems. The respective roles of the customer and AWS in the shared responsibility model are shown in Figure 1.

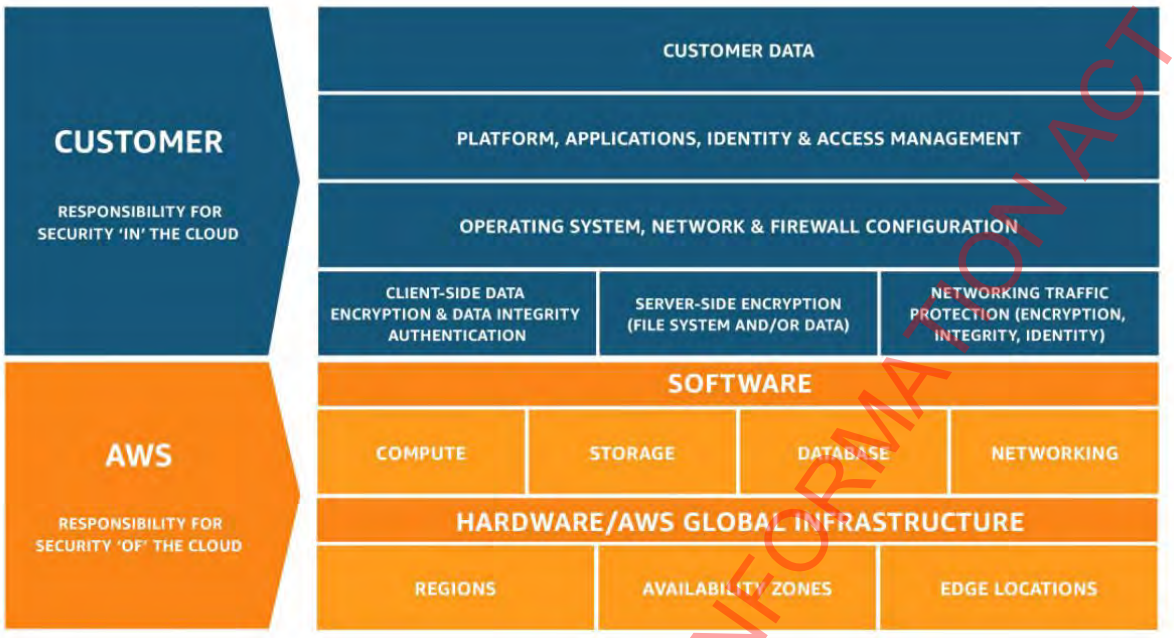


Figure 1 – AWS Shared Responsibility Model

What does the shared responsibility model mean for the security of customer content?

When evaluating the security of a cloud solution, it is important for customers to understand and distinguish between:

- Security measures that the cloud service provider (AWS) implements and operates – security of the cloud.
- Security measures that the customer implements and operates, related to the security of customer content and applications that make use of AWS services – security in the cloud.

While AWS manages security *of* the cloud, security *in* the cloud is the responsibility of the customer, as customers retain control of what security they choose to implement to protect their own content, applications, systems and networks – no differently than they would for applications in an on-site data center.

Understanding security OF the cloud

AWS is responsible for managing the security of the underlying cloud environment. The AWS Cloud infrastructure has been architected to be one of the most flexible and

secure cloud computing environments available, designed to provide optimum availability while providing complete customer segregation. It provides extremely scalable, highly reliable services that enable customers to deploy applications and content quickly and securely, at massive global scale if necessary.

AWS services are content agnostic, in that they offer the same high level of security to all customers, regardless of the type of content being stored, or the geographical Region in which they store their content. AWS' world-class, highly secure data centers utilize state-of-the-art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7 by trained security guards, and access is authorized strictly on a least privileged basis. For a complete list of all the security measures built into the core AWS Cloud infrastructure, and services, see Best Processes for Security, Identity, & Compliance.

We are vigilant about our customers' security and have implemented sophisticated technical and physical measures against unauthorized access. Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS System & Organization Control (SOC) 1, 2[1] and 3[2] reports, ISO 27001[3], 27017[4], 27018[5], and 9001[6] certifications and PCI DSS[7] Attestation of Compliance. Our ISO 27018 certification demonstrates that AWS has a system of controls in place that specifically address the privacy protection of customer content.

These reports and certifications are produced by independent third-party auditors and attest to the design and operating effectiveness of AWS security controls. AWS compliance certifications and reports can be requested on the AWS Compliance Contact Us page. For more information on AWS compliance certifications, reports, and alignment with best practices and standards, see AWS Compliance.

Understanding security IN the cloud

Customers retain ownership and control of their content when using AWS services. Customers, rather than AWS, determine what content they store or process using AWS services. Because it is the customer who decides what content to store or process using AWS services, only the customer can determine what level of security is appropriate for the content they store and process using AWS. Customers also have complete control over which services they use and whom they empower to access their content and services, including what credentials will be required.

Customers control how they configure their environments and secure their content, including whether they encrypt their content (at rest and in transit), and what other security features and tools they use and how they use them. AWS does not change

customer configuration settings, as these settings are determined and controlled by the customer. AWS customers have the complete freedom to design their security architecture to meet their compliance needs. This is a key difference from traditional hosting solutions where the provider decides on the architecture. AWS enables and empowers the customer to decide when and how security measures will be implemented in the cloud, in accordance with each customer's business needs.

For example, if a higher availability architecture is required to protect customer content, the customer may add redundant systems, backups, locations, network uplinks, etc. to create a more resilient, high availability architecture. If restricted access to customer content is required, AWS enables the customer to implement access rights management controls both on a systems level and through encryption on a data level.

To assist customers in designing, implementing, and operating their own secure AWS environment, AWS provides a wide selection of security tools and features customers can use. Customers can also use their own security tools and controls, including a wide variety of third-party security solutions. Customers can configure their AWS services to leverage a range of such security features, tools, and controls to protect their content, including sophisticated identity and access management tools, security capabilities, encryption, and network security. Examples of steps customers can take to help secure their content include implementing:

- Strong password policies, assigning appropriate permissions to users, and taking robust steps to protect their access keys.
- Appropriate firewalls and network segmentation, encrypting content, and properly architecting systems to decrease the risk of data loss and unauthorized access.

Because customers, rather than AWS, control these important factors, customers retain responsibility for their choices, and for security of the content they store or process using AWS services, or that they connect to their AWS infrastructure, such as the guest operating system, applications on their compute instances, and content stored and processed in AWS storage, databases, or other services.

AWS provides an advanced set of access, encryption, and logging features to help customers manage their content effectively, including AWS Key Management Service (AWS KMS) and AWS CloudTrail. To assist customers in integrating AWS security controls into their existing control frameworks and help customers design and run security assessments of their organization’s use of AWS services, AWS publishes a number of whitepapers relating to security, governance, risk and compliance; and a number of checklists and best practices. Customers are also free to design and conduct

security assessments according to their own preferences, and can request permission to conduct scans of their cloud infrastructure as long as those scans are limited to the customer's compute instances and do not violate the AWS Acceptable Use Policy.

AWS Regions: Where will content be stored?

AWS data centers are built in clusters in various global Regions. We refer to each of our data center clusters in a given country as an AWS Region. Customers have access to a number of AWS Regions around the world[8], including an Asia Pacific (Sydney) Region. Customers can choose to use one Region, all Regions or any combination of AWS Regions. Figure 2 shows AWS Region locations as of April 2021.[9]

Figure 2 – AWS global Regions

AWS customers choose the AWS Region or Regions in which their content and servers will be located. This allows customers with geographic specific requirements to establish environments in a location or locations of their choice. For example, AWS customers in New Zealand can choose to deploy their AWS services exclusively in one AWS Region such as the Asia Pacific (Sydney) Region and store their content onshore in Australia, if this is their preferred location. If the customer makes this choice, AWS will not move their content from Australia without the customer's consent, except as legally required.

Customers always retain control of which AWS Regions are used to store and process content. AWS only stores and processes each customer's content in the AWS Region(s), and using the services, chosen by the customer, and otherwise will not move customer content without the customer's consent, except as legally required.

How can customers select their Region(s)?

When using the AWS Management Console, or in placing a request through an AWS Application Programming Interface (API), the customer identifies the particular AWS Region(s) where they want to use AWS services.

Figure 3 provides an example of the AWS Region selection menu presented to customers when uploading content to an AWS storage service or provisioning compute resources using the AWS Management Console.

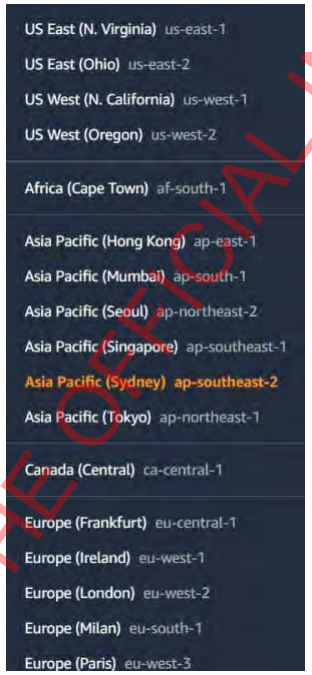


Figure 3 – Selecting AWS Global Regions in the AWS Management Console

Customers can prescribe the AWS Region to be used for their AWS resources. Amazon Virtual Private Cloud (VPC) lets the customer provision a private, isolated section of the AWS Cloud where the customer can launch AWS resources in a virtual network that the customer defines. With Amazon VPC, customers can define a virtual network topology that closely resembles a traditional network that might operate in their own data center.

Any resources launched by the customer into the VPC will be located in the AWS Region designated by the customer. For example, by creating a VPC in the Asia Pacific (Sydney) Region, all resources launched into that VPC would only reside in the Asia Pacific (Sydney) Region. This option can also be leveraged for other AWS Regions.

Transfer of personal information cross border

In 2016, the European Commission approved and adopted the new General Data Protection Regulation (GDPR). The GDPR replaced the EU Data Protection Directive, as well as all local laws relating to it. All AWS services comply with the GDPR. AWS provides customers with services and resources to help them comply with GDPR requirements that may apply to their operations.

These include adherence to the CISPE code of conduct, granular data access controls, monitoring and logging tools, encryption, key management, audit capability, adherence to IT security standards and Cloud Computing Compliance Controls Catalogue (C5) attestations. For additional information, visit the AWS General Data Protection Regulation (GDPR) Center and see the *Navigating GDPR Compliance on AWS* whitepaper.

When using AWS services, customers may choose to transfer content containing personal information cross border, and they will need to consider the legal requirements that apply to such transfers. AWS provides a Data Processing Addendum that includes the Standard Contractual Clauses 2010/87/EU (often referred to as *Model Clauses*) to AWS customers transferring content containing personal data (as defined in the GDPR) from the EU to a country outside of the European Economic Area (EEA).

With our EU Data Processing Addendum and Model Clauses, AWS customers who want to transfer personal data—whether established in Europe or a global company operating in the European Economic Area—can do so with the knowledge that their personal data on AWS will be given the same high level of protection it receives in the EEA. The AWS Data Processing Addendum is incorporated in the AWS Service Terms and applies automatically to the extent the GDPR applies to the customer's processing of personal data on AWS.

Who can access customer content?

Customer control over content

Customers using AWS maintain and do not release effective control over their content within the AWS environment. Customers can perform the following:

- Determine where their content will be located, for example, the type of storage they use on AWS and the geographic location (by AWS Region) of that storage.
- Control the format, structure and security of their content, including whether it is masked, anonymized or encrypted. AWS offers customers options to implement strong encryption for their customer content in transit or at rest; and also provides customers with the option to manage their own encryption keys or use third-party encryption mechanisms of their choice.
- Manage other access controls, such as identity, access management, permissions, and security credentials.

This enables AWS customers to control the entire lifecycle of their content on AWS, and manage their content in accordance with their own specific needs, including content classification, access control, retention, and disposal.

AWS access to customer content

AWS makes available to each customer the compute, storage, database, networking, or other services, as described on our website. Customers have a number of options to encrypt their content when using the services, including using AWS encryption features such as, AWS KMS, managing their own encryption keys, or using a third-party encryption mechanism of their own choice. AWS does not access or use customer content without the customer's consent, except as legally required. AWS never uses customer content or derives information from it for other purposes such as marketing or advertising.

Government rights of access

Queries are often raised about the rights of domestic and foreign government agencies to access content held in cloud services. Customers are often confused about issues of data sovereignty, including whether and in what circumstances governments may have access to their content. The local laws that apply in the jurisdiction where the content is located are an important consideration for some customers. However, customers also

need to consider whether laws in other jurisdictions may apply to them. Customers should seek advice to understand the application of relevant laws to their business and operations.

AWS policy on granting government access

AWS is vigilant about customers' security and does not disclose or move data in response to a request from the U.S. or other government unless legally required to do so in order to comply with a legally valid and binding order, such as a subpoena or a court order, or as is otherwise required by applicable law.

Non-governmental or regulatory bodies typically must use recognized international processes, such as Mutual Legal Assistance Treaties with the U.S. government, to obtain valid and binding orders. Additionally, our practice is to notify customers where practicable before disclosing their content so they can seek protection from disclosure, unless we are legally prohibited from doing so or there is clear indication of illegal conduct in connection with the use of AWS services. For additional information, see the Law enforcement Information Requests page.

Privacy and data protection in New Zealand: The Privacy Act

This section discusses aspects of the New Zealand Privacy Act 2020 (NZ) (Privacy Act) effective from December 1, 2020.

The main requirements in the Privacy Act for handling personal information are set out in the Information Privacy Principles (IPPs). The IPPs impose requirements for collecting, managing, using, disclosing, and otherwise handling personal information collected from individuals in New Zealand. The New Zealand Privacy Commissioner may also issue codes of practice which apply, prescribe, or modify the application of IPPs in relation to an activity, industry, or profession (or classes of them).

The Privacy Act recognizes a distinction between “principals” and “agents”. Where an entity (the *agent*) holds personal information for the sole purpose of storing or processing personal information on behalf of another entity (the *principal*) and does not use or disclose the personal information for its own purposes, the information is deemed to be held by the *principal*. In those circumstances, primary responsibility for compliance with the IPPs will rest with the *principal*.

AWS appreciates that its services are used in many different contexts for different business purposes, and that there may be multiple parties involved in the data lifecycle of personal information included in customer content stored or processed using AWS services. For simplicity, the guidance included in the table below assumes that, in the context of the customer content stored or processed using the AWS services, the customer:

- Collects personal information from its end users, and determines the purpose for which the customer requires and will use the information.
- Has the capacity to control who can access, update, and use the personal information.
- Manages the relationship with the individual about whom the personal information relates, including by communicating with the individual as required to comply with any relevant disclosure and consent requirements.
- Transfers the content into the AWS Region it selects. AWS does not receive customer content in New Zealand.

Customers may in fact work with or rely on third parties to discharge these responsibilities, but the customer, rather than AWS, would manage its relationships with those third parties.

We summarize in the following table the IPP requirements that are particularly important for customers to consider if using AWS to store personal information collected from individuals in New Zealand. We also discuss aspects of the AWS services relevant to these IPPs.

Table 1 — IPP requirements and considerations

IPP	Summary of IPP requirements	Considerations
IPP 1 – Purpose of collection of personal information	Personal information may be collected only for lawful and necessary purposes.	**Customer** — The customer determines and controls when, how, and why it collects personal information from individuals, and decides whether it will include that personal information in
IPP 2 – Source of personal information	Personal information may only be collected directly from the individual, unless an exception applies.	

IPP 3 – Collection of Information	Reasonable steps must be taken to ensure that when an individual's personal information is collected, they are aware of the purposes for which it is collected and certain other matters.	customer content it stores or processes using AWS services. The customer may also need to ensure it discloses the purposes for which it collects personal information to the relevant individuals; obtains the personal information from a permitted source; and, that it only uses the personal information for a permitted purpose. As between the customer and AWS, the customer has a relationship with the individuals whose personal information the customer stores or processes on AWS, and therefore the customer is able to communicate directly with them about collection of their personal information. The customer, rather than AWS, will also know the scope of any notifications given to, or consents obtained by the customer from, such individuals relating to the collection of their personal information. **AWS** — AWS does not know when a customer chooses to upload to AWS content that may contain personal information. AWS also does not collect personal information from individuals whose personal information is included in content a customer stores or processes using the AWS services, and AWS has no
IPP 4 – Manner of collection of personal information	Personal information may only be collected fairly, and in a lawful and non-intrusive manner.	

		contact with those individuals. Therefore, AWS is not required and is unable in the circumstances to communicate with the relevant individuals. AWS only accesses or uses customer content as necessary to provide the AWS services and does not access or use customer content for any other purpose without the customer's consent.
IPP 5 – Storage and security of personal information	Reasonable steps must be taken to protect the security of personal information.	**Customer** — Customers are responsible for security in the cloud, including security of their content (and personal information included in their content). **AWS** — AWS is responsible for managing the security of the underlying cloud environment. For a complete list of all the security measures built into the core AWS Cloud infrastructure and services, see Best Practices for Security, Identity, & Compliance.
IPP 6 – Access to personal information	Individuals are entitled to access personal information about them, unless an exception applies.	**Customer** — Customers are responsible for their content in the cloud. When a customer chooses to store or process content containing personal information using the AWS services, the customer has control over the quality of that content and the customer retains access to and can correct it.
IPP 7 – Correction of personal information	Individuals may request correction of personal information about them.	

		In addition, as between the customer and AWS, the customer has a relationship with the individuals whose personal information is included in customer content stored or processed using the AWS services. Therefore, the customer, rather than AWS, is able to work with relevant individuals to provide them access to, and the ability to correct, their personal information. **AWS** — AWS uses customer content to provide the AWS services selected by each customer to that customer and does not use customer content for other purposes without the customer's consent. AWS has no contact with the individuals whose personal information is included in content a customer stores or processes using the AWS services. Given this, and the level of control customers enjoy over customer content, AWS is not required, and is unable in the circumstances, to provide such individuals with access to, or the ability to correct, their personal information.
IPP 8 - Accuracy to be checked before use or disclosure	Reasonable steps must be taken to check accuracy, completeness, and relevance of personal information before it is used or disclosed.	**Customer** — When a customer chooses to store or process content containing personal information using the AWS services, the customer has control over the quality of that content and the customer retains access to and can

		correct it. This means that the customer must take all required steps to ensure that personal information included in customer content is accurate, complete, not misleading, and kept up to date. **AWS** — AWS does not collect personal information from individuals whose personal information is included in con ent a customer stores or processes using the AWS services, and AWS has no contact with those individuals. Given this, and the level of control customers enjoy over customer content, AWS is not required, and is unable in the circumstances, to confirm the accuracy, completeness, and relevance of personal information before it is used or disclosed.
IPP 9 - Personal information must not be kept longer than necessary	Personal information should not be kept for longer than is required for the purposes for which the information may be lawfully used.	**Customer** — Because only the customer knows the purposes for collecting the personal information contained in the customer content it stores or processes using AWS services, the customer is responsible for ensuring that such personal information is not kept for longer than required. The customer should delete the personal information when it is no longer needed. **AWS** — AWS services provide the customer with controls to enable the customer to delete content

		stored on AWS, as described in AWS documentation
IPP 10 - Limits on use of personal information **IPP 11 - Limits on disclosure of personal information**	Personal information may only be used or disclosed for the purpose for which it was collected, for reasonable directly related purposes, in a way which does not identify the individual, or if another exception applies.	**Customer** — Given that the customer determines the purpose for collecting personal information, and controls the use and disclosure of content that contains personal information, the customer is responsible for ensuring how such personal information is used or disclosed. The customer also controls the format, structure, and security of its content stored or processed using AWS services. **AWS** — AWS uses customer content to provide the AWS services selected by each customer to that customer and does not use customer content for other purposes without the customer's consent. **General** — AWS services are structured such that customers maintain ownership and control of their content when using the AWS services, regardless of which AWS Region they use.
IPP 12 – Disclosure of personal information outside New Zealand	Personal information may only be disclosed outside of New Zealand if the recipient is subject to similar safeguards to those under the Privacy Act.	**Customer** — The customer can choose the AWS Region or Regions in which their content will be located and can choose to deploy their AWS services exclusively in a single AWS Region if preferred. AWS services are structured so that a customer maintains effective control of customer content regardless of what AWS Region they

		use for their content. The customer should consider whether it should disclose to individuals the locations in which it stores or processes their personal information and obtain any requi ed consents relating to such locations from the relevant individuals if necessary. As between the customer and AWS, the customer has a relationship with the individuals whose personal information is included in customer content stored or processed using the AWS services, and therefore the customer is able to communicate directly with them about such matters. **AWS** — AWS only stores and processes each customer's content in the AWS Region(s), and using the services chosen by that customer, and otherwise will not move customer content without that customer's consent, except as legally required. If a customer chooses to store content in more than one AWS Region, or copy or move content between AWS Regions, that is solely the customer's choice, and the customer will continue to maintain effective control of its content, wherever it is stored and processed. **General** — It is important to highlight that an entity is only required to comply with IPP 12 when that entity discloses personal information to an overseas person or entity. The Privacy Act states that where an agency (Entity A),

		holds information as an agent for another agency (Entity B) - for example for safe custody or processing - then (i) the personal information is to be treated as being held by Entity B and not Entity A, (ii) the transfer of the information to Entity A by Entity B is not a use or disclosure of the information by Entity B, and (iii) the transfer of the information, and any information derived from the processing of that information, to Entity B by Entity A is not a use or disclosure of the information by Entity A. It also does not matter whether Entity A is outside New Zealand or holds the information outside New Zealand. Using the AWS services to store or process personal information outside New Zealand at the choice of the customer may not be a disclosure of customer content. Customers should seek legal advice regarding this if they feel it may be relevant to the way they propose to use the AWS services.

Privacy breaches

Given that customers maintain control of their content when using AWS, customers retain the responsibility to monitor their own environment for privacy breaches and to notify regulators and affected individuals as required under applicable law. Only the customer is able to manage this responsibility.

A customer's AWS access keys can be used as an example to help explain why the customer rather than AWS is best placed to manage this responsibility.

Customers control access keys, and determine who is authorized to access their AWS account. AWS does not have visibility of access keys, or who is and who is not authorized to log into an account. Therefore, the customer is responsible for monitoring use, misuse, distribution, or loss of access keys.

The Privacy Act introduced a notifiable privacy breach scheme that is effective from December 1, 2020. The scheme aims to give affected individuals the opportunity to take steps to protect their personal information following a privacy breach that has caused, or is likely to cause, serious harm. AWS offers two types of New Zealand Notifiable Data Breaches (NZNDB) Addenda to customers who are subject to the Privacy Act and are using AWS to store and process personal information covered by the scheme.

The NZNDB Addenda address customers' need for notification if a security event affects their data. The first type, the Account NZNDB Addendum, applies only to the specific individual account that accepts the Account NZNDB Addendum. The Account NZNDB Addendum must be separately accepted for each AWS account that a customer requires to be covered. The second type, the Organizations NZNDB Addendum, once accepted by a management account in AWS Organizations, applies to the management account and all member accounts in that AWS Organization. If a customer does not need or want to take advantage of the Organizations NZNDB Addendum, they can still accept the Account NZNDB Addendum for individual accounts.

AWS has made both types of NZNDB Addendum available online as click-through agreements in AWS Artifact (the customer-facing audit and compliance portal that can be accessed from the AWS management console). In AWS Artifact, customers can review and activate the relevant NZNDB Addendum for those AWS accounts they use to store and process personal information covered by the scheme. NZNDB Addenda frequently asked questions are available online at AWS Artifacts FAQs.

Considerations

This whitepaper does not discuss other New Zealand privacy laws, aside from the Privacy Act, that may also be relevant to customers, including state-based laws and industry-specific requirements. The relevant privacy and data protection laws and regulations applicable to individual customers will depend on several factors including where a customer conducts business, the industry in which it operates, the type of

content they want to store, where or from whom the content originates, and where the content will be stored.

Customers concerned about their New Zealand privacy regulatory obligations should first ensure they identify and understand the requirements applying to them, and seek appropriate advice.

At AWS, security is always our top priority. We deliver services to millions of active customers, including enterprises, educational institutions, and government agencies in over 190 countries. Our customers include financial services providers and healthcare providers and we are trusted with some of their most sensitive information.

AWS services are designed to give customers flexibility over how they configure and deploy their solutions as well as control over their content, including where it is stored, how it is stored, and who has access to it. AWS customers can build their own secure applications and store content securely on AWS.

Further reading

To help customers further understand how they can address their privacy and data protection requirements, customers are encouraged to read the risk, compliance and security whitepapers, best practices, checklists, and guidance published on the AWS website. This material can be found at AWS Compliance and AWS Cloud Security.

As of the date of publication, specific whitepapers about privacy and data protection considerations are also available for the following countries or regions:

- Australia
- California
- Germany
- Hong Kong
- Japan
- Malaysia
- Singapore
- Philippines
- Using AWS in the Context of Common Privacy & Data Protection Considerations

AWS Artifact

Customers can review and download reports and details about more than 2,500 security controls by using AWS Artifact, the automated compliance reporting portal available in the AWS Management Console. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including the NZNDB Addenda and certifications from accreditation bodies across geographies and compliance verticals.

AWS also offers training to help customers learn how to design, develop, and operate available, efficient, and secure applications on the AWS Cloud and gain proficiency with AWS services and solutions. We offer free instructional videos, self-paced labs, and instructor-led classes. For more information on AWS training, see AWS Training and Certification.

AWS certifications certify the technical skills and knowledge associated with the best practices for building secure and reliable cloud-based applications using AWS technology. For more information on AWS certifications, see AWS Certification.

If you require further information, please contact AWS or contact your local AWS account representative.

Document revisions

Date	Description
August 17, 2021	Updated for technical accuracy
November 2020	Fifth publication
May 2018	Fourth publication
December 2016	Third publication
January 2016	Second publication
September 2014	First publication

Notes

[1] https://aws.amazon.com/compliance/soc-faqs/

[2] http://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf

[3] http://aws.amazon.com/compliance/iso-27001-faqs/

[4] http://aws.amazon.com/compliance/iso-27017-faqs/

[5] http://aws.amazon.com/compliance/iso-27018-faqs/

[6] https://aws.amazon.com/compliance/iso-9001-faqs/

[7] https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

[8] AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. AWS China (Beijing) and AWS China (Ningxia) are also isolated AWS Regions. Customers who want to use the AWS China (Beijing) and AWS China (Ningxia) Regions are required to sign up for a separate set of account credentials unique to the China (Beijing) and China (Ningxia) Regions.

[9] For a real-time location map, see https://aws.amazon.com/about-aws/global-infrastructure/

5

Carter, Adam

From: Lyn Beere s9(2)(a)
Sent: Tuesday, 27 September 2022 3:54 pm
To: Privacy Feedback
Subject: Lyn Beere - Proposed changes to notification rules under the Privacy Act 2020

Hi Electoral and Constitutional Team – Ministry of Justice

I have had the opportunity to read the REINZ submission regarding the Ministry of Justice **(MoJ),** Proposed changes to notification rules under the Privacy Act 2020 and I strongly endorse the REINZ submission, in particular our obligations under our Real Estate Agents Act 2008 and 10.2 of the Real Estate Agents Act (Professional Conduct and Client Care) Rules 2012 under the act which we are required to provide a prospective Vendor with a Current Market Appraisal **(CMA).** This CMA gives the Vendor the most up to date information ava lable about the prices at which comparable properties (Usually in the same area) have sold.

Should collection of this data be compromised the entire Real Estate Indus ry w ll not be able to give any prospective Vendor an indication of where their property sits, price wise, in the current market. The implications would be severe with huge legal ramifications for all concerned, if this was the case.

I am really hoping common sense will prevail.

Lyn Beere - AREINZ
National Compliance Manager s9(2)(a)

nzsothebysrealty.com | Watch our brand movie here

Best Real Estate Agency 2022-23
New Zealand 5-20 Offices

Facebook Instagram YouTube

RICHARD BEST LAW

Level 8, 23 Waring Taylor Street
Wellington 6011
Mobile: s9(2)(a)
Email s9(2)(a)

Ministry of Justice
PO Box 180
Wellington 6140
By email: privacyfeedback@justice.govt.nz

27 September 2022

To whom it may concern

Response to Ministry engagement on possible changes to the Privacy Act's notification obligations

1. Introduction

1.1 Thank you for the opportunity to comment on possible changes to the notification obligation under the Privacy Act 2020. I make some general comments, and then comment on each of the specific questions asked in the engagement document.

2. General comments

2.1 From a transparency perspective, I support a change to the Privacy Act that would require agencies that collect personal information from third parties to notify individuals that they are doing so. The rubber hits the road, though, when considering the means by which collecting agencies would be able to meet this requirement, and the exceptions that would justify non-compliance with the requirement. Without knowing these things, the proposal is somewhat abstract and it is difficult to assess the practical issues and potential compliance burden to which such a reform may give rise, particularly for public sector agencies that routinely collect personal information from other agencies.

3. What factors do you think are most important when considering changes to indirect collection of personal information?

3.1 **Factors**

(a) In my view, the most important factors are:

(i) the permitted means by which collecting agencies would be able to meet the new requirement; and

(ii) the exceptions that would justify non-compliance with the requirement.

(b) I also suggest it will be important to consider whether reliance on one or more exceptions is likely to occur in the majority or a high percentage of cases and, if so, the implications of that for pursuit of the suggested changes, at least in relation to their application to certain spheres of activity.

3.2 **Permitted means**

(a) Starting with the means by which collecting agencies would be able to meet this requirement, questions that arise include:

(i) whether the notification would need to be made directly to individuals or whether, at least in some situations, the requirement could be satisfied by public posting of a privacy statement or transparency statement (for example on the agency's main website); and

(ii) whether the requirement could be met by disclosures by the third party agency from whom the collecting agency collects the personal information (the rationale being that, in many cases, the disclosing agency will have the direct relationship with the individuals concerned).[1]

3.3 **Exceptions**

(a) I turn now to the exceptions that would justify non-compliance.

Individuals already on notice

(b) If a collecting agency can be confident that the disclosing agency has informed individuals (when collecting the personal information from them) that their information either will or may be shared with the collecting agency for specified purposes and that this will continue to be the case for future collections, then those individuals will already be on notice that their information will or may be shared with the collecting agency (assuming they were told directly or could access a plain English privacy statement).

(c) The same applies when the individuals have expressly authorised the sharing with the collecting agency.

(d) In these circumstances, I suggest it would not make sense to impose a burden on the collecting agency to inform the individuals of all matters in IPP3 if the purposes of collection are the same as the purposes already communicated to the individuals (and doubling up the notification could be annoying or confusing to them).

(e) For these reasons I suggest it would be desirable to have an exception that addresses this situation. I suggest there would be a need either for the current IPP3(3) to be amended or for an equivalent provision to be included that addresses the indirect collection context. The exception could be along the lines that, when a collecting agency collects personal information from another agency, the collecting agency is not required to inform individuals of the matters listed in IPP3 if it believes, on reasonable grounds, that the disclosing agency has already done so or will do so in relation to the information to be collected.

Practicability

(f) I also suggest that questions of practicability will need to considered. This is particularly important for public sector agencies, because a reform along the lines suggested could, depending on the legislative approach, affect public sector agencies significantly more than most private sector agencies. That could be the case regardless of whether public sector agencies are collecting information from

[1] To be clear, I am *not* referring here to imposing an obligation on disclosing agencies under IPP11.

other agencies in reliance on an IPP2 exception or whether – as is often the case – they are relying on specific statutory powers of collection.

(g) The question that arises is how practical or desirable is it to require public sector agencies that collect personal information from other agencies for public sector purposes to inform individuals of IPP3-type matters, both generally, and specifically in the context of legislative regimes that authorise information collection and disclosure?

(h) It is difficult to determine whether, in a majority of cases, it would not be practicable for the collecting agency to inform agencies of IPP3-type matters. That is an issue that depends on the context and it's an issue on which similarly placed minds can differ (I note that a court in Europe has recently taken a strict approach to a similar issue under article 14 of the GDPR). However, if, in a majority of cases, it were likely not to be practicable, and if the amended IPP3 were to have a 'not practicable' exception (as per the current IPP3(4)(d)), that may raise questions as to whether the suggested reform is desirable in the first place, either at all or at least for public sector agencies or certain spheres of activity.

(i) This line of thinking can be expanded out to consider other exceptions already in IPP3, on the assumption that public sector agencies would often be able to rely on one or more of these exceptions. Again, if, in a majority or a higher proportion of cases, agencies are likely to be able to rely on one or more exceptions, does the suggested reform make sense, at least for public sector agencies? I appreciate there are international comity issues to consider and I appreciate that greater transparency is in principle desirable, but if reliance on exceptions is likely to be frequent, does the reform make sense when agencies may still need to change their processes, procedures and systems to accommodate situations where an exception might not apply? Does the cost-benefit analysis stack up?

(j) A potential solution here is to make it clear that the new IPP3-style obligation does not apply in certain spheres of public sector activity. This could be done in a generalised way, thereby avoiding the need for the case-by-case assessment that IPP3 usually requires when an agency wishes to rely on an exception. I note in this context that the Ministry's engagement document refers to the GDPR as a significant example of jurisdictions that have introduced notification requirements for indirect collection of personal information, but it does not mention the ability for EU member states to derogate from GDPR provisions in their national laws.[2] In the area I'm focusing on here, this is frequently done, and doing so has clearly required considerable thought on the part of member states. For a good example of this, see Schedule 2 to the United Kingdom's Data Protection Act 2018.[3] It contains a number of public sector-oriented derogations that limit the application of Article 14. See also White & Case's useful summary of EU states' restrictions on the GDPR Chapter 3 rights (Article 14 is in Chapter 3).[4]

---

2 See, for example, Article 23 of the GDPR.

3 As you will appreciate, whilst the UK is no longer an EU member state, it still has a UK version of the GDPR.

4 At https://www.whitecase.com/insight-our-thinking/gdpr-guide-national-implementation#q8

Interaction with specific statutory collection and disclosure powers

(k) Another issue that arises is the interaction between the suggested reform and specific statutory collection and disclosure powers. Specific statutory powers of collection, including Approved Information Sharing Agreements, are often put in place because a collecting agency needs the ability to collect personal information from another agency, in circumstances where collection from individuals is not feasible or desirable and where reliance on IPP2 may be challenging or otherwise undesirable.

(l) All of these statutory powers (and there are thousands of them)[5] were drafted at a time when IPP3 was in its current form (or, in some cases, before the Privacy Act 1993 came into force). The policy considerations that informed the drafting, and therefore the drafting itself, might have differed had the suggested reform been in place. I suspect there are tens if not hundreds of situations where, had the proposed reform been in place, the Government of the day and ultimately Parliament may have wished to override the provision

(m) My concern is that the suggested reform may unwittingly add complexity to a range of statutorily-authorised or -required sharing situations where there is currently no need for the collecting agency to inform individuals or, significantly, even think about whether they're able to and wish to rely on an exception to IPP3-style transparency requirements. To my mind, to say that this wouldn't be a problem because exceptions will often apply, would not be sufficient, at least not as IPP3 is currently worded, because reliance on exceptions is usually a case-specific exercise that requires the formation of a particular belief on reasonable grounds. To require agencies that currently collect personal information under specific statutory powers to do this on each occasion could, at least for some agencies, be unworkable.

(n) It may be possible to address these concerns by taking the approach suggested in paragraph 3.3(j) above, but I suspect considerable analysis would be required to ensure that all relevant areas of activity are considered and that the right balance is struck.

4. What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?

4.1 Individuals

(a) The potential advantages of broadening the notification requirements are identified in the Office of the Privacy Commissioner's submission.[6] In essence, the Privacy Commissioner says the changes "would contribute to enhancing the privacy of individuals and assisting individuals to exercise their privacy rights (including rights of access to and to request correction of their personal information)".

---

5 I am aware there are thousands because I've reviewed nearly all of them for an Info-Provisions database and search tool at StopLookGo Privacy (stoplookgo.co.nz).

6 Available at https://privacy.org.nz/publications/reports-to-parliament-and-government/submission-in-response-to-the-ministry-of-justice-consultation-on-the-broadening-of-the-privacy-acts-notification-obligations/

(b) It would be interesting to know whether there is any empirical evidence that the changes will contribute to "enhancing individuals' privacy". Much may turn on what one means by that. However, if the notification requirement is to be met after the point of collection,[7] and bearing in mind that (unlike under the GDPR) New Zealand's Privacy Act does not have a right to object to processing or an express right to withdraw consent, it may well be that individuals' privacy is not enhanced that much. In a subset of situations people may know more about which agencies hold and use their information (and of course that's desirable), and that will enable them to better exercise their IPP6 and IPP7 rights, but whether it will enhance individuals' 'privacy' seems speculative.

(c) Turning to disadvantages, I agree with the Ministry that, for individuals, the main disadvantage would likely be notification fatigue. I also agree that, in some situations, such as where sensitive information is being shared, an individual may become overwhelmed or confused, or perhaps worried or even frightened about what may be done with it or who may see it. In some situations, whether these feelings materialise may depend on how the message is communicated. In other situations, the feelings may materialise regardless of how the message is communicated.

(d) I suggest the Ministry consider whether there should be an exception to the effect that the collecting agency does not need to make IPP3-type disclosures if:

(i) doing so would be likely to pose a serious threat to the life, health, or safety of any individual, or to public health or public safety; or

(ii) the agency is satisfied, after consultation (where practicable) with the individual's health practitioner, that the information relates to the physical or mental health of the requestor, and compliance with IPP requirements would be likely to prejudice the health of the individual; or

(iii) the individual is under the age of 16 and disclosure would be contrary to their interests.

(As you will appreciate, this wording in (i)-(iii) is taken (with some modifications) from section 49 of the Privacy Act.)

4.2 **Agencies**

(a) For agencies, greater transparency may foster greater trust in them on the part of individuals whose information they collect, although that is speculative.

(b) If the proposed reforms are necessary for New Zealand to receive continuing 'adequacy status' from the European Commission, then there would be obvious advantages for New Zealand enterprises doing business in Europe where that business involves the handling of significant volumes of personal information of EU residents.

(c) For agencies, the disadvantages would likely be:

(i) compliance costs, not only for the reasons outlined by the Ministry but also due to the need to train agency staff and, in some cases, update agency

[7] This is how Article 14 of the GDPR works, unless individuals already have the information.

systems and privacy statements;

(ii) potential impacts on agency efficiencies due to the extra compliance requirement; and

(iii) the issues identified under question 1 above relating to practicability and the interaction with specific statutory collection and disclosure powers.

5. What form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate.

5.1 If amendments are to be made then I agree with the Privacy Commissioner that amendments to IPP3 would probably be the preferable approach.

5.2 That said, the changes could also take the form of a new IPP (e.g., IPP3A) that deals with notification of indirect collection (as is the case under the GDPR with its Article 14). I suggest any new IPP would need to come after IPP3 and, for a range of reasons, I suggest it would be highly undesirable to change the current IPP numbering to accommodate a new IPP.

5.3 I do not see any justification for narrowing the IPP2 exceptions.

5.4 Amending IPP11 along the lines described in the engagement document could place an undue burden on, for example, NGOs, and potentially damage relationships they have built with individuals (especially where the collecting agency is collecting the information after the NGO has collected it and is doing so under a statutory power of collection).

6. If you are a New Zealand business, are there any practical implementation issues you can identify in complying with the proposed changes?

6.1 I am not a New Zealand business that collects individuals' personal information in any way that would be affected by the suggested changes. However, as someone who advises New Zealand agencies, I foresee that New Zealand businesses in this position may need to:

(a) update their stocktakes of the circumstances in which they collect personal information from third parties;

(b) update internal policies and procedures;

(c) update privacy statements;

(d) train relevant staff on the changes; and/or

(e) make changes to relevant IT systems or tools.

6.2 All of these activities are likely to increase a business's costs.

7. Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in the engagement document?

7.1 Please see my answer to question 1 on the topic of the interaction of the suggested changes with specific statutory collection and disclosure powers. To my mind this is an acutely significant topic. I maintain a database of summaries of specific statutory collection and sharing powers at stoplookgo.co.nz, categorised by agency and subject matter. If it would assist, I would be happy to provide the Ministry with free access to that

database and/or with agency-specific or subject-specific volumes of the summaries of provisions.

7.2 I also note that government policies and procedures, like the Data Protection and Use Policy and the Privacy Maturity Assessment Framework, would probably need to be updated.

7.3 In addition, government agencies that collect large volumes of personal information from other agencies would need to consider each sharing scenario to determine whether compliance with the new IPP is required or whether they could rely on an exception (in all likelihood this would be the case regardless of whether they collect in reliance on an IPP2 exception or under a specific statutory power). Unless the approach suggested in paragraph 3.33.3(j) above is taken, this could be very time-consuming for the likes of:

(a) Police;

(b) Ministry of Business, Innovation & Employment;

(c) Department of Internal Affairs;

(d) Ministry of Social Development;

(e) New Zealand Customs Service;

(f) Ministry of Health;

(g) Inland Revenue;

(h) Corrections;

(i) Ministry of Justice; and

(j) Ministry for Primary Industries.

My analysis of statutory collection and disclosure provisions affecting Government departments suggests that these departments are the top 10 (in terms of the number of provisions affecting them). The same applies to a number of Crown entities.[8]

8. Should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?

8.1 If broader notification requirements are to be added to the Act, I suggest it would be undesirable to confine them to personal information collected indirectly about individuals who are overseas. Having different regimes that depend on where a person is based would create added complexities, and New Zealand agencies would be treated differently depending on whether the people concerned are overseas or in New Zealand. Having different regimes may also make the reform appear premised on appeasing overseas regulators (like the European Commission) rather than being focussed on the privacy interests of all New Zealanders.

[8] For more information, see "Which Government departments have the most information collection, use and sharing provisions?" at https://stoplookgo.co.nz/which-departments-of-the-crown-have-the-most-information-collection-use-and-sharing-powers/

9. Is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback.

9.1 In my view, there is another IPP3-oriented issue that is just as important as the potential reform referred to in the engagement document. The issue concerns disclosures by collecting agencies to disclosing agencies.

9.2 At the moment, IPP3 only applies to agencies that collect personal information from individuals. There is no principle that expressly requires the collecting agency to inform the disclosing agency of the range of matters referred to in IPP3. In my view, this is a weakness in the Act.

9.3 The purpose of collection will, of course, usually be central to whether, under IPP2, the collecting agency is able to collect the personal information from the disclosing agency or whether the collecting agency is able to rely on a specific statutory collection power. Similarly, purpose will usually be central to whether a disclosing agency can rely on an exception in IPP11 or whether the disclosure is permitted or required by a specific statutory collection/disclosure power. In the normal course one can expect responsible agencies, who have thought of everything they need to think of, to be clear about such matters with one another.

9.4 However, this does not always happen with the level of particularity that the disclosing agency may require. The risk of this is probably greatest when a powerful governmental agency is collecting personal information from other agencies (often under specific statutory collection powers) who depend on the government agency for funding or other forms of assistance or cooperation, and especially when the sharing occurs without the formality of an information sharing MOU or similar document.

9.5 History has shown us that NGOs can be particularly vulnerable to not getting the level of information they may need. They need information on the collecting agency's purposes of collection, how the information will be used, and with whom the information may be shared, in order to assess the legality of their disclosure and to comply with their own obligations under IPP3 to the individuals from whom they directly collect the personal information. IPP3 compliance is particularly important where the collection by the collecting agency from the disclosing agency is not a one-off, that is, where the collecting agency will be collecting the same kind of information from the disclosing agency periodically. This is because as soon as the disclosing agency knows of the collecting agency's collection, the disclosing agency is bound by IPP3 to inform individuals from whom it collects the information in the future, of (among other things) the intended recipients of the information.

9.6 I suggest the Ministry consider whether IPP3 should be strengthened by requiring an agency that collects personal information from another agency, to inform that other agency of:

(a) the collecting agency's purpose(s) of collection;

(b) the intended recipients of the information (within and beyond the collecting agency); and

(c) whether the supply of the information by the disclosing agency is voluntary or mandatory and, if the collecting agency is relying on a specific statutory power of collection, what that power is.

I would be happy to discuss any of my comments above with the Ministry if that would be helpful.

Kind regards

Yours sincerely

s9(2)(a)

Richard Best

BDO New Zealand Limited
PO Box 33005, Takapuna 0740
Auckland, New Zealand
Tel: +64 9 486 2125

29 September 2022

Electoral and Constitutional
Ministry of Justice

By email: privacyfeedback@justice.govt.nz

Our Submission on the Proposed Changes to Notification Rules under the Privacy Act 2020

We are grateful to the Ministry of Justice for providing an opportunity to agencies, like us, to share their feedback on the possible changes to the notification rules under the Privacy Act 2020.

As an accountancy and advisory firm, we collect and process personal information of our clients, suppliers, employees, and applicants. We are building a robust privacy culture and complying with our obligations under the Privacy Act 2020 and the 13 Information Privacy Principles.

As an agency, we have been investing time, effort, and money towards our privacy programme and the proposed amendment raises some challenges for us, which are as following:

1. **Collection of Information from third parties:** While we generally collect information directly from our data subjects, sometimes it is necessary that the information is collected from a third party. Some of the examples of the same can be verification of identity, PEP checks, checking references from applicants etc. In most cases, we already seek consent from the data subject and notifying them about the collection will become and extra step.

2. **Clarity regarding the notification requirement:** It is difficult for us to predict how much extra cost and effort will go into meeting the requirement as there is no clarity on how broad the requirement will be. We will be grateful to the Ministry of Justice if there is more information shared regarding compliance with the notification requirement.

3. **Trust and Transparency:** We understand that the notification requirement is to increase transparency on part of the agencies which, in turn, should lead to increase in trust in the agency. Studies assert that individuals are more likely to trust services which have more disclosure-based transparency (Vorm and Combs, 2022)[1]. However, the principle of transparency is already embedded within the Privacy Act and agencies are under an obligation to inform the data subjects why their personal information is being collected. Additionally, agencies have adopted privacy policies, privacy statements and privacy notices to ensure that data processing is transparent. Finally, the data subjects have also been given the right to access their information and seek confirmation about the agency holding a certain information.

[1] Vorm, E. S., & Combs, D. J. (2022). Integrating Transparency, Trust, and Acceptance: The Intelligent Systems Technology Acceptance Model (ISTAM). *International Journal of Human-Computer Interaction*, 1-18.
See also - Bitzer, T., Wiener, M., & Morana, S. (2021, August). Algorithmic Transparency and Contact-tracing Apps-An Empirical Investigation. In *AMCIS*.

BDO New Zealand Limited
PO Box 33005, Takapuna 0740
Auckland, New Zealand
Tel: +64 9 486 2125

Hence, the notification requirement will not introduce transparency, but merely supplement it.

Trust, in itself, takes many forms and is affected by multiple factors. Process-based trust is tied to repeated access to services or product purchases, while Institutional-based trust is tied to the formal social structure (Luo, 2002[2]). Introduction of notifications, or its lack thereof, will not be the sole factor is enhancement or reduction of trust towards the agencies.

4. **Clarity in relation to a new Information Privacy Principle:** As an agency, we require more information in relation to incorporation of the proposed amendment as a privacy principle. Does the amendment propose a change in the existing principles or propose a new 14th Information Privacy Principle? From the perspective of an agency, it requires a lot of effort to train the staff about the privacy principles. Privacy Act's Information Privacy Principles are more spread out compared to the GDPR and hence, it will get more difficult for the staff and employees to understand and implement additional requirements.

5. **Notification Fatigue:** There is abundance of research which indicates that notification fatigue is quite real and when data subjects are constantly nudged with notifications, they start to tune it out. Mandatory notifications produce notification fatigue which is a real danger that people will ultimately ignore notifications when there is, in fact, a significant risk of harm (Burdon, 2011[3]). Moreover, notification fatigue may also be a prominent concern as individuals appear to treat notifications as marketing material and do not read them. Hence, notification is a limited remedy[4].

To conclude, while we appreciate the thought behind the proposed amendment and we ourselves are striving towards developing a robust privacy culture, implementation of the notifications when personal information is collected from third parties will require significant cost and effort to achieve something which might generate limited benefit. We propose that agencies should, instead, incorporate better privacy statements and notices and train their employees better.

Yours sincerely
BDO New Zealand
s9(2)(a)

Doug Haines
Director/National Privacy Officer

Email: s9(2)(a)
DDI: s9(2)(a)

---

[2] Luo, X. (2002). Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory. *Industrial marketing management*, *31*(2), 111-118.
[3] (Burdon, M. (2011). *The conceptual and operational compatibility of data breach notification and information privacy laws* (Doctoral dissertation, Queensland University of Technology); J T Soma, J Z Courson and J Cadkin, 'Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets' (2009) 25(4) Richmond Journal of Law & Technology 1, 7)
[4] *ibid* Note 3; PONEMON INSTITUTE, NATIONAL SURVEY ON DATA SECURITY BREACH NOTIFICATION (2005)

Regulatory Affairs
T. +64 4 474 9028 F. +64 4 4746628
E. paul_hay@bnz.co.nz
Private Bag 39806, Wellington Mail Centre, Lower Hutt, 5045

30 September 2022

Electoral and Constitutional
Ministry of Justice
PO Box 180
Wellington 6140
Email: privacyfeedback@justice.govt.nz

Dear Sir or Madam

BNZ's Submission to Possible Changes to Notification Rules Under the Privacy Act 2020

Introduction

The Ministry of Justice ('the Ministry') is considering possible changes to the notification rules for collecting personal information under the Privacy Act 2020. The suggested changes would broaden notification requirements from direct collection only to also applying when an agency collects personal information indirectly via a third party.

The following represents BNZ's submissions to the Ministry on possible changes to the notification rules under the Privacy Act 2020, prepared by BNZ's Privacy & Data Ethics team. The Ministry sought consultation on seven questions, which are outlined below, along with BNZ's response to each question.

1. What factors do you think are most important when considering changes to indirect collection of personal information?

The proposed changes should consider where notification of indirect collection sits on the sliding scale of transparency versus practicality, with a particular emphasis on how far an agency would need to go to satisfy the requirements.

How should indirect collection of personal information be communicated to individuals: Clarification is required as to whether notification could be satisfied by an agency updating its overriding privacy statement or policy, or whether it would need to provide individuals with a point in time privacy notice. If the changes require 'point in time' notices to be provided to individuals, agencies will need to update privacy notices on all forms where information is collected and send further notifications out to customers each time they wish to collect information from a third party or change the third party vendor. For customer centric businesses, there is a real risk the customer experience will be undermined, with customers experiencing notification fatigue by being inundated with notifications and lengthy privacy notices that they are ultimately likely to ignore.

Many agencies already inform individuals of indirect collection of personal information: Many agencies, including BNZ, already refer to indirect collection as part of their privacy policy, although in BNZ's case these third parties are listed by 'type' and not outlined explicitly. For example, BNZ's Master Privacy Policy ('MPP') states that BNZ collects personal information indirectly from credit reporting agencies, but the MPP does not specify which agency it collects from. The reason for this is that third party agreements are constantly being entered into as others end – continually notifying customers of these small changes (especially where the identical information is collected for the same purposes) would be burdensome for both agencies and individuals. It would require constant updating of privacy policies and forms containing a privacy notice to be meaningful to the individuals affected. We recommend that the Ministry considers whether most agencies are currently transparent with this indirect collection or whether individuals are unaware of this collection.

Clarification on whether personal information is being collected from each individual, or whether it may be collected: Indirect collection of personal information is often dependent on the circumstances of each individual. The guidance will need to specify whether it is sufficient to state that indirect collection may be required in certain circumstances or whether notification is explicitly required when the circumstances trigger the collection of additional information for a particular individual. For agencies with large customer bases, being explicit with each individual is not practicable.

Exceptions: The Ministry will need to consider potential exceptions to the rule, what these exceptions will be and how they interact with the other IPPs. For example, there might be exceptions where an agency is required by law to collect personal information, where personal information is publicly available, where it is being collected covertly (e.g. investigating fraud or threats), or where an agency may not practically be able to notify the individual that the information is being collected.

The compliance burden for agencies must be balanced with the need for individuals to have better transparency around where their information sits. The Ministry should consider requiring notification of indirect collection only where it is reasonable to expect the individual would need to know.

2. **What are the advantages or benefits of broadening the notification requirements, for both Individuals and agencies? What might the disadvantages be?**

Individuals
The main advantage to the changes is that individuals will be able to exercise better control over their personal information. With increased visibility over which agencies hold their information and what it is used for, individuals will be in a better position to exercise their rights of access and correction under the Privacy Act 2020.

In contrast, implementing the notification requirements creates a real risk of 'notification fatigue' (depending on the requirements and how the changes are implemented by agencies). Some individuals may not wish to be notified and would be required to go through an opt out process for all agencies who are collecting their personal information indirectly. Much like the unsubscribe function on marketing and promotional emails, this has the potential to become very frustrating from a customer experience perspective.

Agencies
The changes would encourage agencies to create a clearer picture of what data they are collecting from where. However, for large agencies, highly regulated agencies or agencies that are required to collect significant amounts of personal information indirectly, there could be a high administrative burden for achieving and maintaining compliance.

3. **What form do you think the proposed changes to notification rules under PA should take?**

The Ministry should first consider whether the rules apply to all agencies, or only those that process personal information about individuals based overseas.

If the former approach is taken, it would make sense for the collecting agency to provide the notice to the individual at the point of collection and this requirement could be incorporated into IPP3. This would also make sense as the same IPP3 exceptions could apply.

If the latter approach is taken, a new principle would probably be the tidiest approach and would remove the burden from agencies that only operate in New Zealand.

4. **If you are a New Zealand business or agency, are there any practical implementation issues you can identify in complying with the proposed changes?**

We recommend that the Ministry provides clarity to agencies regarding how it expects this to be implemented and the level of detail required. As discussed above, we do not consider that it is practical to specify a specific vendor, a category of vendor would be more reasonable. We also suggest that this information could be included in a privacy policy, rather than a 'point in time' notice. For example, if the requirement was to provide 'point in time' notices, BNZ would need to review and update several hundred customer facing forms relating to the various products and services – this could require a significant financial commitment and is not likely to be well received by customers. We are concerned that customers may be overwhelmed by such notifications leading to notification fatigue and reduced engagement in relation to privacy issues.

5. **Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?**

   No comments.

6. **Should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in NZ?**

   It appears that a significant driver behind the proposed changes is to achieve equivalency with privacy laws in other jurisdictions and to reflect international best practice. To achieve this, the changes would only need to apply to personal information collected from individuals in jurisdictions that require notification of indirect collection.

   However, if we consider this from an individual's perspective, it seems unreasonable that individuals based outside of New Zealand should have greater protection under the New Zealand Privacy Act 2020 than the individuals based inside New Zealand.

   If the financial and administrative burden for agencies can be mitigated and this requirement can be implemented (a) though privacy policies, rather than 'point in time' notices; and (b) on a general, rather than specific agency, basis; BNZ supports this protection extending to all individuals.

7. **Is there any other feedback you would like to provide on these proposed changes?**

   BNZ has no further feedback on the proposed changes.

   All enquiries on this submission may be directed to Rachel O'Brien, Head of Privacy and Data Ethics at Rachel_A_O'Brien@bnz.co nz or Paul Hay, GM Regulatory Affairs at paul_hay@bnz.co.nz, or s9(2)(a) .

Yours sincerely

s9(2)(a)

Paul Hay
GM, Regulatory Affairs

Feedback on the Possible Changes to Notification Rules Under the Privacy Act 2020

In response to a Ministry of Justice Consultation Paper

Rebecca Bonnevie[1]

30 September 2022

Summary of Feedback

In summary:

- Factors to consider when examining indirect collection include
    - whether the circumstances of the original collection (including the relationship to the collecting party and any disclosures) define the obligations of the agency receiving it and
    - whether the individual understands the existence of the indirect collection and can exercise their rights in relation to their impacted information.
- There are a variety of scenarios where indirect collection by a party is bound by an IPP 3 disclosure by another party. There may be benefit in further scoping of particular scenarios of concern to the Ministry of Justice (MOJ) to establish whether notification amendments effectively address those concerns of whether other regulatory tools or guidance is needed. In the scenarios presented here, there may be benefit in the creation of a regulation or Code to address the privacy risks fourth party agency indirect collection carries.
- There would be benefit in strengthening the content and form of existing Information Privacy Principle (IPP) 3 disclosures to make them easier to understand and to include naming of third parties that will receive their information.
- The MOJ could use this opportunity to clarify the relationships between different roles under the Privacy Act (agency, joint-agency and "agent" under s11) and clarify the responsibilities of different roles. In doing this, it may become clearer how the principal agency's IPP 3 obligation affects the other roles that could be seen to be "indirect" collectors of information. In doing this analysis the MOJ needs to consider all personal information collection points in all types of digital devices and tools.

[1] I hold a LLB/BA from Victoria University of Wellington and a LLM from Columbia University in the City of New York which I attended as a Fulbright Scholar and recipient of the Yvonne AM Smith Scholarship. I have experience working in privacy compliance and am a contributing author to the upcoming 3rd edition of Privacy Law in New Zealand (Thompson Reuters, publication forthcoming), in which I write about privacy and business and privacy in light of emerging technologies. Some of the feedback provided in this document echo the content of those chapters. Feedback is based on my own personal views.

- MOJ may wish to examine the interaction between IPP 1, 4 and 13 in this space to refine the core functions and activities of an agency that limit the purposes for which personal information can be collected. MOJ may also wish to take this opportunity to consider the impact of indirect collection, or the scenarios of concern, on children and young persons.

Introduction

Throughout my experience in privacy compliance and through research I have become increasingly concerned at the way privacy frameworks rely on an individual's understanding and engagement with a privacy disclosure. In my writing this is referred to as the "Disclosure Model", which was created in a mostly analogue world, and now places the responsibility on the data subject to understand and address the collection methods and data uses present in the digital world. I was delighted to see the Ministry of Justice (MOJ) release this consultation and would be more than happy to discuss any of the points I make with officials at a later opportunity.

This paper contains my own personal views. References to the Privacy Act are to the Privacy Act 2020 unless stated otherwise.

Definitions

One of the challenges with these discussions is the terminology used in the Privacy Act, so this paper will start with setting out some terms.

- An "agency" is the primary actor with obligations under the Privacy Act – it is what might be called the "controller" in offshore regulations. In this document it will be referred to as "the principal agency". The principal agency is the body making the decisions on what personal information needs to be collected, from whom, how and why. The principal agency is accountable for compliance with the Privacy Act.
- Section 11 of the Privacy Act introduces the concept of the agency's "agent". In this paper it will be called the "s11(2) agent". A s11(2) agent is an interim party or agency that is directed to hold information for custody or processing by and for the principal agency. This role might be called "processor" in other jurisdictions. For the purposes of the Privacy Act, the holding of the information by a s11(3) agent is to be treated as being held by the principal agency regardless of whether that s11(3) agent is outside New Zealand.[2] This position stands unless the s11(2) agent uses or discloses it for their own purposes.
- Where one agency collects information about an individual independent of the principal agency that ultimately receives the information, this paper refers to that agency as a "third party agency". That third party agency might be an second individual, or an entity, for example a company that employs the individual. Where the information is within scope of the Privacy Act, the third party agency has obligations under the Privacy Act and the provision of information to and from it would be considered a "disclosure" and "transfer" of information.
- Where an agency collects information from other independent agencies and not from the individual, this paper refers to it as a "fourth party agency". Where the information is within scope of the Privacy Act, the fourth party agency holds its own obligations, but must come within an exception to IPP 2 to ensure it is not required to collect information directly from the individual.

[2] Privacy Act 2020, s 11.

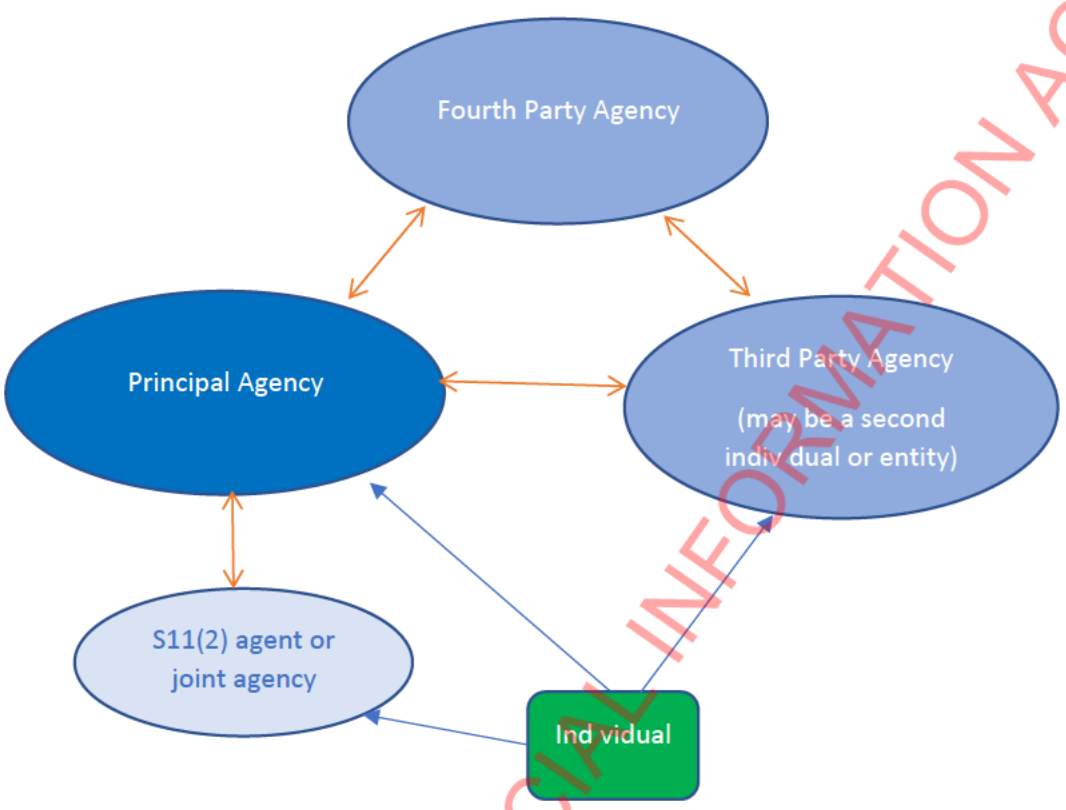


Figure 1: All parties

"Direct" collection in this paper is understood to be collection of personal information about the individual from the individual themselves. This might be through active collection methods, such as an individual completing a form, or passive collection methods, such as trackers on websites or in emails that the individual triggers by simply using the tool (this distinction may also be called overt/covert methods).

By way of contrast, "indirect" collection is understood to be collection of personal information about the individual from someone other than the individual such as another individual, or from another entity holding that information. The individual themselves is not directly involved in the collection arrangements, despite the information being about them. Indirect collection is more likely to be intentionally provided and received between the agencies, sometimes in exchange for money or services, and can involve many "hops" of transactions away from the individual.

In the diagram above, the blue arrow show direct collection from an individual, whereas the orange arrows indicate indirect collection (or provision). In this diagram, at some point the source of the personal information is directly connected from the individual themselves.

Responses to questions

1 What factors do you think are most important when considering changes to indirect collection of personal information?

When considering indirect collection the main factors to consider are:

a) how do the circumstances of the original collection define the obligations of the agency receiving it; and
b) what is the best way to empower the individual to understand and control the disclosures of their personal information.

The response to this question looks at three scenarios - intentional indirect collection by a principal agency by way of other organisations, indirect collection by an organisation due to a principal agency providing it for a use, and finally indirect collection by an agency that has no connection to the individual.

Intentional Indirect Collection by a Principal Agency via Interim Party

A principal agency may request that an interim agency collect personal information from an individual on the principal agency's behalf. This might be explicitly agreed between the parties, for example if a charity engages a temping agency to provide street collectors that signing up potential donors for the charity it is clear the donors' information collected by those individuals belongs to the

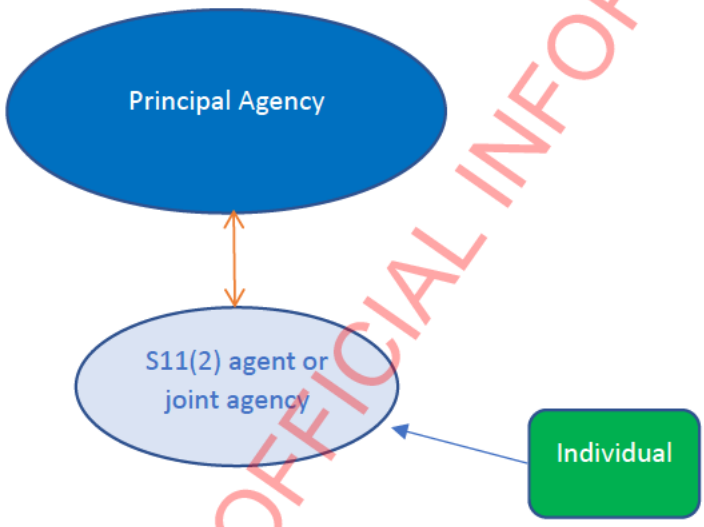


Figure 2: Indirect Collection by Principal Agency via Interim Party

charity and not to the temping agency. In other situations, the principal agency may play a less active and more permissive role in facilitating the interim party's collection. An example might be where a principal agency website code enables the interim party to drop a digital tracker on the individual's browser which provides the interim party with information about the individual's likes and dislikes which the principal agency can benefit from by using the third party to advertise to the individual.

In both these cases, the personal information is collected directly from the individual by a third party, but the relationship between the party and the principal agency means the principal agency continues to hold (at least partly) the IPP 3 obligation to provide a notice to the individual.

Explanation: Interim party collection techniques direct from an individual – pixels and cookies on the web and in mobile app.

When a data subject loads a website, their browser performs a "server call" during which the coding of a website prompts the loading of the visible and invisible content. A pixel,[3] invisible to the data subject, prompts the dropping of small strings of code called "cookies" onto the browser of the data

[3] A pixel is literally a 1x1 image which is added to web pages, typically the footer, that runs a piece of JavaScript code. The server call loads the pixel code which creates the cookie.

subject. Some of these cookies are essential to the running of the website and may remain until the end of the visit, but others may be dropped by third parties for the purposes of analytics or tracking of the user across the internet. Behavioural information is collected on a data subject's movement through the internet, enabling the collection of a cumulative picture of their likes, interests, habits and behaviours.[4] A 2016 study of the top one million websites observed that Google was able to use cookies to track an individual across the majority of those websites.[5]

Mobile devices have been described by the New Zealand Supreme Court as raising "special privacy concerns, because of the nature and extent of information they hold."[6] Mobile devices are full of sensors that collect contextual information about the user and the device, like the time of day, location, weather, motion and activity. In mobile applications (apps) this contextual information from the device is accessible to app developers (the principal agency) through the app code or to an interim party through the principal agency building that interim party's Software Data Kits (SDK) into the app. SDK have been likened to lego for app developers; organisations like Google and Facebook have SDK libraries that enable an app to integrate seamlessly with other functions – sales, analytics, social media etc.[7] In the context of this consultation, the SDK are collecting information directly from the individual for the SDK interim party, who may provide it to the principal agency or use it for the principal agency's benefit.

A s11(2) agent or joint agency relationship

This paper submits that the principal agency still holds a responsibility (albeit maybe a joint one) to make a disclosure to the individual that satisfies IPP3 regarding all collection it requests and facilitates via an interim party. This includes collection via the principal agency's digital platforms including in-app.

This is a consistent position with EU law, where a website owner (principal agency) is generally considered a joint controller with those third parties that collect personal information through its site. This joint-controller status applies even where the website owner does not have access to the original data and only receives de-personalised information from the third party.[8] The European decision also noted that the website owner choices had given the third party (Facebook) the opportunity to collect information on data subjects who it would not otherwise have had access to (as they did not have their own Facebook account).[9] In the EU joint responsibility requires

---

[4] This can collect face-value data points like interests, but some tracking tools can measure elements like movement within websites and time spent viewing particular aspects of the website.

[5] Steven Englehardt and Arvind Narayanan, "Online Tracking: A 1-million-site Measurement and Analysis," (paper presented to ACM SIGSAC Conference on Computer and Communications Security, 2016).

[6] *Dotcom v Attorney General* [2014] NZSC 199, [2015] 1 NZLR 745 at [1191] referring to both computers and mobile devices.

[7] MightySignal is an organization that tracks mobile apps, including tracking the most used SDKs in free ioS and Android apps. Organisations like Google and Facebook have SDK libraries and their SDK are commonly used by app developers. Google Analytics, for example, is in 49% of the top 200 ioS apps as reported on MightySignal <www.mightysignal.com>.

[8] The Court took a purposive approach and found that Wirtschaftsakademie must be regarded as taking part in the determination of purposes and means of processing the personal information collected for analytics, so must be categorized as controller responsible for processing jointly with Facebook, Case C-210/16, *Wirtschaftsakademie Schleswig-Holstein GmbH* ECLI:EU:C:2018:388 at [34]–[39]; It is irrelevant whether the party had access to the processed data for controllership to arise, Case C-25/17 *Jehovan todistajat* ECLI:EU:C:2018:551 at [65]–[75]; A joint controller relationship arise because the website owner had a decisive influence on the purposes of processing by permitting the collection and transmission of the data, and because both parties attained a mutual benefit from the activity, Case C-40/17 *Fashion ID* ECLI:EU:C:2019:629 at [80].

[9] *Wirtschaftsakademie* above at n 107, [40] to [41]; *Fashion ID* above at n 107, at [78].

demonstration of a shared responsibility for that information collection, including a IPP3 equivalent disclosure, and an ability for data subjects to enforce their rights against both parties.[10] In New Zealand, the Privacy Act implies that a joint-agency status might exist (see s11(3)), but there no further guidance on the point. MOJ may wish to look at this further.

How to empower the individual with knowledge of and control over passive collection techniques by interim parties

The application of the GDPR and the European Directive 2002/58/EC[11] has resulted in the proliferation of "cookie-banners" in Europe and those websites targeting the European market. These banners interrupt the data subject's journey to give them information about the essential and non-essential cookies the website uses, and provide the user with opt-in consent to the non-essential use.[12] These cookie banners have garnered criticism as they create disclosure fatigue – they interrupt the user experience and require attention and consent on every website. There is no current New Zealand guidance regarding the application of the Privacy Act IPPs to cookies and the information they collect. The MOJ ought to engage with EU experts to understand whether there is a better method of disclosure in place of cookie banners.

In mobile apps, the privacy disclosures are being defined by private sector players like Apple requiring that a principal agency comply with the App Tracking Transparency standards to be able to be listed in the Apple Appstore. Apple defines "tracking" as the act of linking user or device data collected from a principal agency's app with user or device data collected from other companies' apps, websites, or offline properties for targeted advertising or advertising measurement purposes. Tracking also refers to the principal agency sharing user or device data with data brokers. [13] If the principal agency is proposing to allow interim or third parties to track the individual or access their device's advertising identifier, the app must present the user with a standardised privacy disclosure that explain data collection, and a pop-up opt in consent. Unless consent is given by the user, tracking must not be recorded.

---

[10] GDPR, art 26.

[11] For example the Privacy and Electronic Communications Regulations 2003 (UK) ["PECR"]. The EU directive is being developed into a standardised EU-wide regulation.

[12] The case C-673/17 *Planet 49* ECLI:EU:C:2019:801 clarified that consent to cookies cannot be pre-checked for a user. Strictly necessary or essential cookies enable the smooth running of the website. Marketing cookies which track online a tivity to help advertisers deliver more relevant advertising, are considered non-essential. Marketing cookies are persistent and almost always come from third parties rather than the website owner. GDPR.eu "Cookies, the GDPR and the ePrivacy Directive" www.gdpr.eu.

[13] Examples of tracking include displaying targeted advertisements in the app based on user data collected from apps and websites owned by other companies; sharing device location data or email lists with a data broker; sharing a list of emails, advertising IDs, or other IDs with a third party advertising network that uses that informat on to retarget those users in other developers' apps or to find similar users; and placing a third party SDK in your app that combines user data from your app with user data from other developers apps to target advertising or measure advertising efficiency, even if you don't use the SDK for these purposes – using an analytics SDK that repurposes the data it collects from your app to enable targeted advertising in other developers' apps. It doesn't include linking to third party data solely on the user's device and is not sent off-device in a way that can identify the user or device; or when the data broker uses data solely for fraud detection, fraud prevention, or security purposes, and solely on your behalf. Apple "Asking Permission to Track" <www.developer.apple.com>

Indirect collection by a Third Party Agency due to a Principal Agency providing it

The example in the blue box in the consultation paper fits under this heading. In that example the principal agency website terms and conditions (which satisfy IPP3 for the principal agency) provide that the individual authorise the sharing of their information with an advertising agency to provide the individual with advertising about the principal agency.

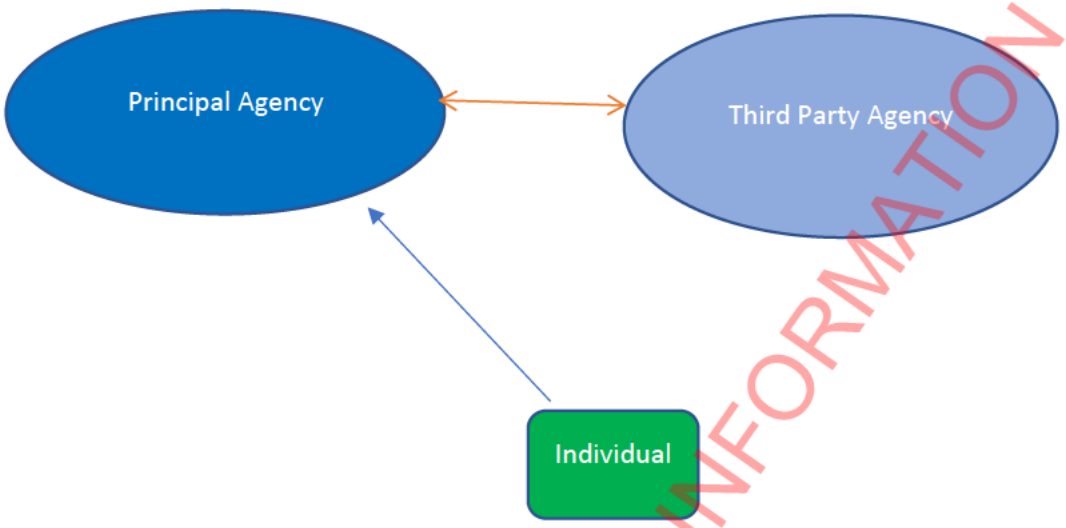


Figure 3: Indirect collection by Third Party Agency via Principal Agency

Similar situations might be the provision of personal information to a mail house to ensure the principal agency's documents are sent to customers, provision of personal information to an organisation to provide customers with a survey on behalf of the principal agency, or provisions of address data to an organisation to be "cleaned" to the correct format for the principal agency's use.

The key point to note in these circumstances is the information is originally collected and held by the principal agency for its lawful purpose, and the personal information is provided to the third party agency for a particular service or use pursuant to a relationship between the parties (which is usually contractual). This creates a s11(2) relationship with the third party, who is usually restricted from using the information for their own purposes and is required to destroy the information after a reasonable period of time. That s11(2) party must keep to the uses in accordance with the principal agent's IPP 3 disclosure.

Indirect collection by a Principal Agency from a Third Party Agency

In this situation a Principal Agency is provided information from a Third Party Agency under contract, agreement, or as an a alternative source to the individual themselves.

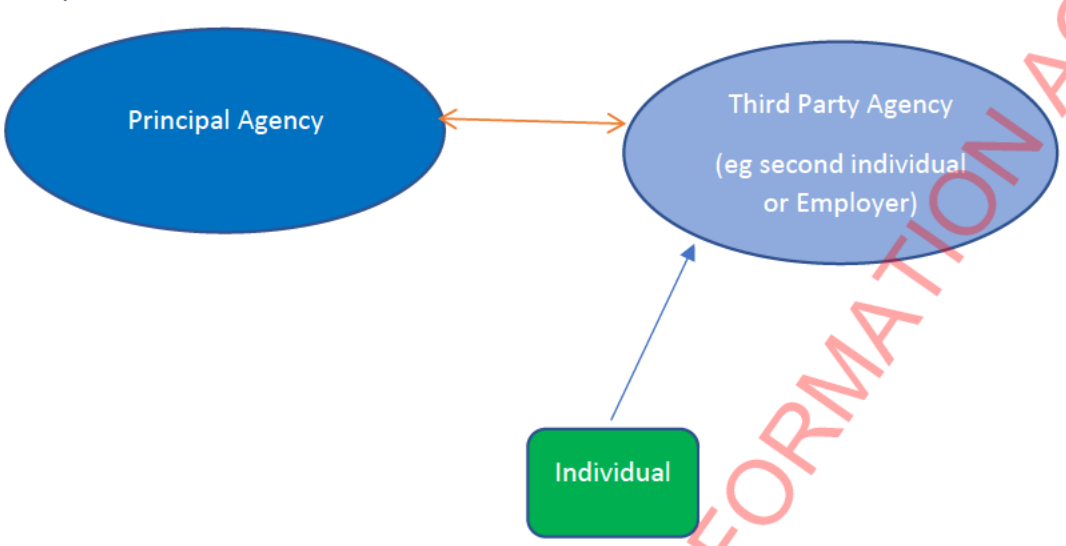


Figure 4: Indirect collection by Principal Agency via Third Party Agency

In many cases, the individual would have given the Third Party express or implied consent to provide this information to the Principal Agency. For example, an employer might provide contact details to a Principal Agency so the individual can participate in an employment benefit scheme. The Third Party Agency holds the IPP 3 responsibility to make it clear what information is being collected and that provision to the Principal Agency is or might be part of the purposes for which the information is collected.

It would be helpful to understand from MOJ whether there are specific scenarios in this structure that give rise to concerns, to best comment on whether an additional disclosure by the principal agency to the individual is a necessary step.

Indirect collection by a Fourth Party completely disconnected from the individual

This is probably one of the key concerns of indirect collection – where information is collected by a fourth party agency for their own purposes without any interaction with the individual.

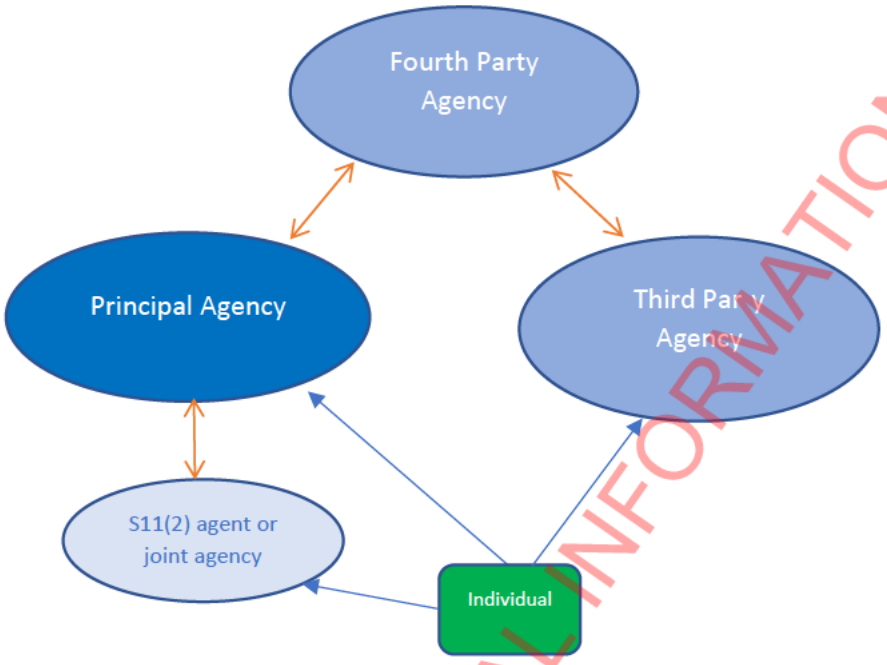


Figure 5: Indirect Fourth Party Collection

In theory any provision of personal information to a third party in this way must align with the purposes expressed in an initial disclosure to the individual by the Principal Agency or Third Party Agency. A challenge here is a) where that information is sourced overseas it is not clear an original disclosure was provided; b) there is usually nformational asymmetry between the collecting party and the individuals understanding of the original disclosure including who that information is provided to (this is especially present in complex layerings of digital terms and conditions from multiple parties); and c) whether there are any meaningful options for the individual to stop the indirect collection of this data.

As discussed above, while a principal agency has some responsibility for the data collected by a s11(2) agent or joint agency on their digital platforms, these sources of personal information are often the source of databases personal information offshore. A high risk example is of mobile phone location data. These can be created through GPS pings collected by SDK in apps, collected through GPS enabled cars, or even IP address recording (this gives a broad location). These regular pings can create a large t ove of location data.[14] Private companies may buy and sell this data which can have uses from advertising to surveillance, and even be mined to establish more sensitive personal information like religious affiliation or sexual orientation. As many of the technology companies are US based the data moves out of reach of the exercise of New Zealand data rights.

Another high privacy risk space are data broker holdings off behavioural and preference profiles on individuals. Behavioural profiles can be used in Real Time Bidding, in which in the time it takes for

[14] A6 claims that there are 30 to 60 GPS location pings per device per day and 2.5 trillion location data points annually worldwide. Sam Biddle and Jack Poulson "Anomaly Six Demo'd Surveillance Powers by Spying on CIA" *The Intercept* (online ed, 22 April 2022).

an advertising space to load on a browser the ability to put an ad in front of that particular viewer has been sold with regard to data points in their profile and whether the data shows them to be a target customer for that ad. For example Digital Out-Of-Home programmatic advertising uses data to heat map "audience affinity" showing the likelihood of a target audience to be in a particular place at any point in time. This is created from the target audience's GPS location data that shows how the audience moves throughout the day overlaid with third-party data about the individual's behaviours, interests or habits to enhance the target audiences.[15]

As a note, Credit Reporters are a fourth party who receive information from principal agencies and has no direct link to the individual, but credit reporting agencies are also subject to a Privacy Code. MOJ may wish to review the code to confirm it is happy that the indirect collection by credit reporters does not require an amendment to that Code.

2. What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?

The benefits in clarifying and strengthening the notification requirements would in theory give individuals an opportunity to be more proactive in whether to accept privacy terms and in theory be able to enhance their privacy protections. However, it is worth noting that while the privacy framework relies entirely on the Disclosure Model there will be challenges with individual understanding and a lack of meaningful choices. In *R v Alsford*[16] the Court was cautious about consent given to express information-sharing provisions in terms and conditions as they were broad and often in contracts of adhesion.[17] In her 2018 Sir Bruce Slane lecture, Winkelmann J said:[18]

> *There is good reason for proceeding with caution when weighing the significance to be given to consent when assessing whether the individual expected privacy or had waived it. These are standard contracts people must agree to if they are to access services, sometimes essential services. Most do not read the full content of any such contract. That is especially so with online service providers. Although the privacy policy must be agreed to before services can be accessed, acceptance is easy – simply click on the accept button.*
>
> *Often the consequential authorized collection of data will occur in the course of a very low to no value transaction. Few would spend time reading a privacy policy before using a search engine or purchasing food to go. And yet by clicking accept, we are agreeing to all of the terms and conditions, if expressed in suitably plain English, contained in the privacy policy of the service provider. Even if we do read the privacy policy, it is doubtful we will have a full understanding of the implications of what we have agreed to. There is a very substantial asymmetry in technical understanding between the customer and most who operate business in an online world.*

In blog post guidance the Privacy Commissioner suggested that Privacy Act principles of transparency and fairness would not likely be satisfied by a vague up-front statement and a legalese-

---

[15] Intended audiences could be created based on TV watching behaviours (including viewership patterns across live and on-demand viewing) interests and intentions based on mobile apps they have, or demographic, lifestyle, behavioural, transactional and occupational data attributes. Vistar Media "Programmatic Ad Buying Example Audiences and Targeting Strategies for DOOH" www.vistarmedia.com at 19.

[16] *R v Alsford* [2017] NZSC 42.

[17] *R v Gomboc* 2010 SCC 55, [2010] 3 SCR 211 at [33] cited at *R v Alsford* [2017] NZSC 42 at [68].

[18] Hon Justice Helen Winkelmann, (then) Judge of the Court of Appeal of New Zealand "Sir Bruce Slane Memorial Lecture" (Wellington, November 2018).

dense privacy policy.[19] The information asymmetry mentioned by the Chief Justice and Privacy Commissioner is exacerbated by power asymmetry between the parties with the data subject having no real choice or alternative but to accept data collection. One of the challenges posed by the Covid-19 pandemic was an accelerated shift of activity online as people were forced to interact online for work, socialising and shopping for essentials. Under the current regime there is very little opportunity for someone to object to personal information collection or on-disclosure and still be able to use a service, which meant the amount of collectable data about an individual online would have dramatically increased. MOJ may wish to consider whether this "all-or-nothing" approach to information collection is consistent with the fairness concept in IPP 4[20] and may wish to consult with the Commerce Commission about the convergence point between privacy law and consumer protection laws.[21]

The benefits for organisations of the suggestions in this paper are around clarity of responsibility and role, and further alignment with international counterparts.

3. What form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate.

The three options provided in the consultation paper are:

1. An amendment to IPP 3 to introduce a notification requirement when an agency collects personal information indirectly from other sources.
2. An amendment to one of the other IPPs, for example to IPP 2 to narrow the exception for indirect collection or to IPP 11 to require a disclosing agency to notify that the information has been disclosed to a third party.
3. Introducing a new separate privacy principle dealing with notification of indirect collection.

This paper proposes a 3 step amendment to address indirect collection.

Clarify existing roles under the Privacy Act

Organisations need to understand when they hold full responsibility for disclosures, where that responsibility is held on behalf of another, or jointly with another agency. This would be improved by MOJ enhancing the clarity of the roles and responsibilities in the existing Privacy Act, including clarifying what a principal agency needs to understand regarding the s11(2) agent to satisfy their own Privacy Act obligations, and how joint-responsibility is entered into and responsibilities discharged.

Strengthen existing disclosures

Name the third parties receiving disclosures

Amendments could require the third parties receiving personal information from the principal agency to be named in the principal agency's IPP3 disclosure. That disclosure could explain what

---

[19] John Edwards "Click to consent? Not good enough anymore" (2 September 2019) Office of the Privacy Commissione <www.privacy.org.nz>

[20] This was exacerbated by the Covid-19 pandemic of 2020; as people were undergoing lock-downs the digital services became lifelines, requiring them to agree to terms and conditions with no objection rights to information collection.

[21] *Australian Competition and Consumer Commission (ACCC) v Google LLC* (No.2) [2021] FCA 367 has linked consumer protection laws and privacy disclosures, as have conversations in Australia regarding facial recognition technologies and its use in retail stores. Consumer protection laws also contain provisions that prohibit unfair contract clauses in contracts where there are power imbalances.

data rights and individual has regarding that third party. In some circumstances it might be appropriate to request consent from the individual to the disclosure, or allow the individual to object to the sharing

Establish uniformity and increase clarity.

The Privacy Commissioner has also questioned whether lengthy and complex privacy disclosures would be compliant with the transparency and fairness principles in the Privacy Act.[22] In addition, complex privacy notifications could potentially be misleading under consumer protection legislation. A recent case in Australia has said that the disclosures and settings of data collection need to be understood by a "reasonable user who was concerned enough to click through to settings but not enough to read the granular detail"[23] to be consistent with the Australian version of the Fair Trading Act.

To address this consumer bandwidth issue, researchers from Carnegie Mellon University have come up with a prototype security and privacy "nutrition" style label for IoT devices. The intention is to standardize labelling so a consumer can compare a device's security posture, how it manages user data, and what privacy controls it has. The prototype of the label has a simple version for device packaging that contains a URL or QR code for privacy-conscious individuals to access further detailed information.[24] Some countries are developing their own national IoT label programs that focus on elements like the security features of IoT devices.[25] Clear, consistent and easily understandable privacy nutrition labels could be developed to simplify IPP 3 disclosures and ensure that they are clear, particularly with regard to children or young people.[26]

Create a targeted regulation for fourth party agencies with multiple sources of indirect collection and no connection with the individual.

As set out in the first question, the key considerations are the circumstances of the original collection and the empowerment of the individual regarding their data subject rights. It may be worth brainstorming specific scenarios where the privacy risks in this fourth party indirect collection are heightened to ensure that a notification to individuals would address that issue.

Assuming a notification would address the issue of keeping a fourth party accountable to any original purpose of collection is a challenge, as is maintaining any consents given due to the lack of contact, which also impairs the individual from exercising their access rights, this paper proposes a targeted regulation. It could be in the form of an additional privacy principle, but MOJ may wish to explore the connection between this indirect collection and marketing, data broking, profiling and 360 view services, and do some research to refine organisations of this type that would benefit from more regulation. It could include, for example, a threshold of information held about an individual at which point an organisation is required to provide an individual with a direct disclosure explaining the source(s) of the information, purpose and data subject access rights.

---

[22] John Edwards "Click to consent? Not good enough anymore" (2 September 2019) Office of the Privacy Commissione <www.privacy.org.nz>

[23] The ACCC alleges that from Jan 2017 to late 2018 it was misleading for Google to not properly disclose to consumers that both settings had to be switched off if someone did not want Google to collect, keep and use their lo ation data.

[24] Lily Hay Newman "IoT Security is a Mess. Privacy "Nutrition" Labels Could Help" *Wired* (online ed, 9 June 2020).

[25] Jay Ashar "Regulatory proposal on mandatory IoT security label" *GovTech Leaders* (7 May 2019).

[26] Privacy Act, s 22, IPPs 3 and 4.

4. If you are a New Zealand business, are there any practical implementation issues you can identify in complying with the proposed changes?

This paper is not written on behalf of a business, but there are two main implementation challenges that arise from these proposed changes.

Rewrite of existing notifications

Whether an organisation doesn't have an IPP3 notice and it should, or whether it has one that could be strengthened through the use of a uniform "nutrition" label there is likely to be some implementation issues in updating collateral. Guidance and templates provided by OPC could assist with this.

Data Governance requirements

A bigger challenge for a business might be Data Governance 101 – understanding what is being collected by your organisation or on your behalf, why, who it is disclosed to and used by and for, and when it is destroyed. These seem like simple points but the mapping of the data lifecycle and sources of information may be a space that organisations will need to work on to be able to implement the strengthened IPP 3 requirements.

5. Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?

There are few areas that MOJ might like to consider:

- The application of this regime to the data of children and young people. It may be that MOJ consider that there is no good reason that a child or young person's data ought to be being indirectly collected especially for market ng purposes. MOJ may like to consider a specific code regarding data and children and young people, and there are some international examples that could be used as a base line.
- Data collection through mobile devices. As indicated in an earlier question, the collection through the myriad of sensors and SDK in apps can lead to many companies receiving information without an individual's conscious provision of data. Requiring notification from all of these companies is going to drown an individual, so that must be kept in mind. Many of these companies are offshore, so MOJ may wish to consider whether the collection in New Zealand in apps available in our appstores is "carrying on business" such that the companies come within scope of the NZ Privacy Act.
- The effect of data collection on the ability of an individual to be anonymous and the impact of all the data collection on the autonomy of an individual. The question for MOJ is should more regulation around the function and activity data can be collected for remove privacy risks to anonymity and autonomy of decision making.

6. Should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?

There are two reasons to stay away from the creation of a two-step process (different requirements individuals overseas and for New Zealanders).

First, arguably, the indirect notification is designed to improve the privacy protections for the recipient - ensuring the recipient understands which organisation holds their personal information, giving them an opportunity to exercise their rights. With that established, is seems strange to suggest only overseas individuals are worthy of enhanced protections.

Second, a two-step system would create additional compliance costs to embed and administer. An organisation would have to establish which data point an organisation uses as an indicator that an individual is in fact overseas and be flexible enough to account for a mobile population coming in and out of the country. A single standard is strongly recommended.

7. Is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback.

In these deliberations, the Ministry of Justice may also want to consider some other aspects of Privacy Law reform as they link into whether disclosures are sufficient or accurate in add essing indirect collection and use of personal information.

Whether IPP 13, IPP 1 and IPP 4 are being applied correctly

Considering indirect collection is an opportunity for MOJ to consider the circumstances under which agencies are able to broadly collect information and pass to another agency or match or enrich it with information from a fourth party. That is, MOJ may wish to explore the interaction between IPP 1, IPP 4 and IPP 13 of the Privacy Act.

IPP 1 requires a principal agency to know its "function and activities" and ensure that collection of personal information is "necessary" and "connected to" that function and activities. Aside from government departments, which have establishment legislation, it is open for an organisation to define its functions and activities as broadly as it likes. This leaves it ambiguous whether, in a data driven economy, any collecting principal agency is including some level of advertising and/or data broking as part of its functions and activities. This is important, because where this line falls defines whether information can be passed along to an advertising agency freely (as that information is necessary for the advertising function of the store) or requires an extra level of transparency and perhaps consent.

The author suggests that IPP 1 functions and activities should be read narrowly due to IPP 4, that as any collection has an ethics assessment inherent in it including whether it is unreasonably intrusive in personal affairs. As a result, activity ike data collection for sale, brokerage, or advertising would be outside core functions of the large majority of organisations.

Finally, this narrow reading of function or activity due to IPP 4 would also have implications for IPP 13. IPP13 does not allow one agency to "reassign" an individual's unique identifier to that individual for their own purposes. The reassignment of a unique identifier carries the risk that it would facilitate illegitimate profiling and data matching of individuals.[27] The digital world, however, is full of identifying codes includ ng a mobile device's operating systems provide unique IDs for that device: AdID (Android) and Identifier For Advertising (IDFA) for Apple. Digital identifiers like this are designed to connect pieces of information about individuals from multiple sources.

IPP13(3), which fulfils a recommendation by the Law Commission, provides that an agency does not "assign" a unique identifier to an individual by simply recording the other agency's unique identifier for the individual for the sole purpose of communicating with that agency about the individual.

The distinction between "assign" and "record" is not explicit in the Act. In 1995 Blair Stewart, then Manager of Codes and Legislation in the Office of the Privacy Commissioner, commented that "assignment" would involve the act of bringing the identifier into use in the second agency to identify the individual. In 1998 the Privacy Commissioner echoed this: assignment is where "the

[27] Office of the Privacy Commissioner, *Necessary and Desirable: Privacy Act 1993 Review* (1998) at [2.14.5] summarizing Dr Paul Roth in *Privacy Law and Practice* (Butterworths, Wellington 1995-1998).

identifiers need to be brought into effect in an agency for the purposes of uniquely identifying particular individuals", though noted this was yet to be tested in the Tribunal.[28] These two statements, along with a narrow reading of function and activity in IPP 1 and a strong application of the ethics and reasonable test in IPP 4 suggest that when a mobile identifier is collected and used by multiple organisations through apps and SDKs the identifiers are being "re-assigned" rather than "recorded." Communication between the parties using the identifier as a connection for that individual is not solely to "locate its records" (as contemplated in the explanatory note to the Privacy Bill), but rather with the specific purpose to build a composite profile of an individual, precisely the concern IPP 13 was supposed to address.

This author suggests this indirect collection, in so far as profile building, should be further explored by MOJ clarified in an enforceable Adtech Privacy Code under the Privacy Act 2020.

[28] At [2.14.11].

CENTRIX

30 September 2022

Electoral and Constitutional
Ministry of Justice
PO Box 180
Wellington
By email: privacyfeedback@justice.govt.nz

Possible changes to notification rules under the Privacy Act 2020
Centrix Group Limited (Centrix) Submission

1. Thank you for the opportunity to provide feedback on broadening notification requirements of indirect collection of personal information.

2. Centrix operates as a credit reporter, was founded in 2009 by industry experts, and specialises in the provision of credit reporting services and solutions. Centrix Management has extensive experience in credit bureau development, data management, analytics and debt recovery solutions in New Zealand, Australia and Asia.

3. As you will be aware, Centrix while carrying out its credit reporting function is governed by the Credit Reporting Privacy Code 2020 (CRPC).

Submissions

4. Centrix supports transparency regarding the collection, use and disclosure of personal information, however, considers no further regulation on notification for indirect collection of credit information by credit reporters is required.

5. Credit providers are already required to inform individuals that their information will be disclosed to a credit reporter and the purposes for which the credit reporting is collecting the information and how it will be used and disclosed.

6. The right of access and correction of a consumer's credit reporting file is well known, and Centrix is involved in a number of initiatives to increase the awareness of this, including:

    - Promotion of the 'My Credit Report' via our public website along with guides in multiple languages; and

- Access agreements with agencies such as FinCap and Good Shepherd to assist individuals experiencing credit hardship.

7. Requiring notification of indirect collection is likely to lead to notification fatigue, information overload and significantly increased costs to agencies.

8. Any changes to the notification rules for indirect collection of personal information should not apply to credit reporters, as the CRPC already requires notification via the credit providers. If it is considered changes are required in the credit-reporting context, this should be subject to a discrete consultation process on proposed changes to the CRPC. This is to ensure appropriate consideration is given to whether there are any additional benefits to consumers and whether these benefits outweigh the negative outcomes of a proposal – such as notification fatigue and increased operations costs for credit reporters, which will ultimately be passed onto consumers.

9. We request the Ministry looks to the areas/industries of concern where individuals may be surprised that their information has been shared (which may include advertising and marketing) and not use a "broad brush" approach to this issue.

10. If there is to be a change to the Privacy Act, this should be by way of an amendment to IPP3, however there should be a number of exceptions and notification should not be required where:
    a. the original agency collecting the personal information has given notice of all the matters required on behalf of the entities that they disclose the information to (who is indirectly collecting the personal information).
    b. the individual is already aware of the matters that would be notified.
    c. the information is obtained from a publicly available source.
    d. notification is not possible or would involve a disproportionate effort.

Collection of personal information by credit reporters

11. Credit reporters can only collect credit information for use in its credit reporting business. Credit information is prescribed in the CRPC, and credit reporters cannot collect any other personal information to use in its credit reporting business. Essentially all information collected by credit reporters for use in their credit reporting business is collected indirectly, and not from the individual concerned.[1]

[1] One exception is when an individual requests access to their credit file, and the individual provides Centrix with identification information and the individual consents to that information being used to update the Centrix credit reporting database.

12. Generally, credit reporters collect information from:
    a. Credit providers (an agency that provides credit to an individual) – such as banks, finance companies, and utilities and agencies that provide goods or services before payments.
    b. Landlords and property mangers.
    c. Employers and recruitment agencies.
    d. Debt collectors (an agency that carries on the business of collecting debt).
    e. Public register (Company, Insolvency, Limited Partnership, PPSR).

13. The CRPC already has in place notification requirements that covers the majority of the credit information it collects. Credit reporters are required to have a subscriber agreement in place with all subscribers who they disclose credit information to. The subscriber agreement must have the following provision:[2]

Where the subscriber collects credit information directly or indirectly from the individual concerned for disclosure to the credit reporter, the subscriber must inform the individual of the purposes for which the credit reporter is collecting the information and the purposes for which the information will be used and disclosed.

14. Centrix collects in excess of 12.5 million updates monthly from its subscribers. To notify every individual each time information is uploaded would be impossible, particularly repayment history information, which would require notifications to mostly the same individuals each month.

15. Credit reporting is already heavily regulated by the CRPC and any proposed change to the Privacy Act on indirect collection should not automatically be applied to the credit-reporting context.

16. Thank you for the opportunity to provide submissions and we would welcome further discussions with the Ministry on this matter.

s9(2)(a)

Keith McLaughlin
Managing Director
Centrix Group Limited

[2] Note however this does not include debt collectors as debt collectors who disclose information to a credit reporter does not collect debt information directly from the individual concerned.

18 September 2022
Ministry of Justice

Submission on possible changes to notification rules under the Privacy Act 2020
Dr Andrew Chen

1. Thank you for the opportunity to provide feedback on these possible changes. I am a Research Fellow with Koi Tū: The Centre for Informed Futures at The University of Auckland, based in Wellington. My research area is in digital technologies and their impacts on society, particularly in terms of public sector use and privacy. The views in this submission are my own and may not reflect those of my employers.

Key Factors

2. Upholding the principle that individuals should have *control* over their personal information, where it is, who has it, and how it is used, would logically conclude that when personal information is *transferred* between agencies hat they should be notified so that they can make informed and appropriate choices about their personal information. Therefore, I generally support the intent of the possible changes.

3. This is particularly important as the type of personal information being commonly collected becomes increasingly invasive (for example, analysis or insights derived about a person that speak to intangible aspects like personality rather than purely tangible characteristics like street addresses or phone numbers) and increasingly immutable (for example, biometrics that are unique and cannot be changed). In these cases, the negative impacts of personal information misuse or privacy breaches are greater than in the past, and there may be more reason for individuals to oppose their information or specific types of information ending up in someone else's ownership or control without their knowledge.

4. The level of privacy harm that has accrued as a result of a lack of requirement for notification of indirect collection thus far is very difficult to quantify, because for the most part we simply do not know how much personal information has been indirectly collected. What we do know is that many modern business models (e.g. large tech companies generating personalised advertising) rely on transferring personal information between agencies for monetary value. Similarly, government agencies are increasingly transferring information about individuals in order to make better decisions and provide better services to individuals (e.g. through the IDI, or through digital identity systems), although there are more protections in place in the public sector. Notifying individuals each time their information is being transferred (with an opportunity to opt-out) may reduce the scale of those transfers, which is not necessarily a bad thing.

5. That our broader society has seemingly accepted business models and processes that rely on the transfer of personal information without notification of individuals is not a sufficient reason to oppose the need for such notification – the harm is still present and therefore it is appropriate to explore mechanisms to mitigate against that harm. An approach that introduces new compliance costs to mitigate that harm should be evaluated by balancing those costs against the harm that is mitigated, rather than accepting an argument that any compliance costs are unacceptable.

6. Our traditional conception of privacy focuses at the individual level, which can make it challenging to assess the level of harm from indirect collection of personal information. It is difficult to identify that a tech company selling someone's personal information to an advertising company produces significant monetary or emotional harm to justify taking regulatory or enforcement action. However, in developing this policy, the government should consider the level of harm at a collective level – that transferring the personal information of many people between agencies can allow those agencies to make decisions with broader harm. A strong example is the Cambridge Analytica scandal – the individual users, whose information was shared with a political consulting firm when they thought it was only being used for academic purposes, did not suffer much harm at the individual level, but the way that the data was then used to influence over 200 elections in 68 countries is significantly more harmful to those democratic societies.

7. A notification approach is effectively an opt-out approach, where a notified individual has to then take action to stop the transfer of personal information or to request that information be deleted, rather than agencies needing to actively seek permission from the individual to opt-in and agree to the information transfer. This is already a compromise against best practice privacy principles but a necessary one for practical reasons, particularly where significant amounts of information are being transferred. This approach should not be compromised further in any proposed changes.

8. On notification fatigue, while this is a fair concern and a real user experience challenge, it is a weak argument to reject the possible changes. Firstly, in jurisdictions that already have notifications for indirect collection of personal information, I have not been able to find any reports or literature on notification fatigue being an issue based on empirical data, only theoretical arguments. Secondly, that the notifications will be coming from different agencies helps mitigate against notification fatigue, which is much more common when the notifications are from the same source and similar in style and content. With sufficient variation between agencies, this may help reduce the potential risk of notification fatigue. An argument against the possible changes on the grounds of notification fatigue should be based on an analysis of the quantity and frequency of notifications that individuals are likely to receive if such changes were implemented.

9. Maintaining adequacy, particularly with the European Union, is a critical competitive advantage for New Zealand. Adequacy is the status of being deemed to have an adequate level of data protection relative to another jurisdiction's regulations and expectations, and allows data to flow between the jurisdictions more easily. Particularly where notification of indirect collection of personal information has already been implemented under the EU's GDPR, and we can see that it is effective and working, it is important for New Zealand to keep up with international best practice. This should also be considered in the discussion around compliance costs, as the cost to New Zealand of not meeting international best practice may be greater than the cost of compliance to agencies.

10. I believe that overall it would be likely beneficial to give individuals stronger agency over their personal information through the notification of indirect collection.

Additional Considerations

11. Practically, we should consider the scenario where agencies may transfer personal information to each other without either agency having contact details for the individual. The legislation should consider this situation and whether or not an exception is required. Taking “reasonable steps” may be sufficient in the legislation to allow for scenarios where it is simply not possible to notify the individual.

12. However, we should not overly rely on a “reasonable steps” standard in other situations. Over-reliance on a “reasonable steps” standard makes it difficult for both businesses and individuals to know whether the standard has been met. It creates a period of uncertainty where we will have to wait for relevant cases to be brought to the Office of the Privacy Commissioner or the courts before precedent for “reasonable steps” can be established. Such an approach should be used sparingly and for relatively specific parts of the legislation.

13. Policymakers should also consider the scenario where an agency collects information about a person from public sources. Just because personal information is publicly available does not mean that information is no longer personal, and should not mean that the individual has relinquished their rights to privacy – for example, an agency may collect phone numbers from phone books, or harvest information about people from social media networks. Where the personal information will fall under the ownership of a new agency that the individual may not have known about, then they should still be notified about that (acknowledging the exceptions in IPP2/IPP3). For example, the personal information may be combined with other sources already held by the agency, or the personal information may be collected in a public space (e.g. a photo of a person’s face) which becomes a biometric identifier for the individual – the individual should have a right to know how the personal information will be used.

14. The framing of the consultation places emphasis on the collecting agency, which is understandable given the structure of the Privacy Act and the earlier Information Privacy Principles. In terms of the obligations on the disclosing agency, as currently described in IPP11, policymakers should consider whether or not to add an obligation that the disclosing agency must be satisfied that the collecting agency has sufficient processes and controls to be able to uphold the Privacy Act. This could be similar to the provisions of IPP12 in that agencies cannot make disclosures overseas unless the agency believe on reasonable grounds that the exceptions apply. This would reduce the likelihood of information being indirectly collected by poor actors if they cannot demonstrate to the disclosing agency that they are responsible stewards of personal information.

15. It would be important to ensure that, in their interactions with individuals, disclosing agencies cannot contract out of notification requirements ahead of time, and that providing blanket statements would be insufficient. Essentially, agencies should not be able to just put in the Terms and Conditions that the agency may disclose the information to other unspecified agencies without notifying the individual. Firstly, the general approach of satisfying IPP3 through a Privacy Policy or Terms and Conditions on an agency website is weak for ensuring that individuals actually understand what is happening to their personal information. Secondly, individuals’ perceptions of the value of their personal information, and the risks that may be associated with sharing it, change over time and individuals should be given the

opportunity to exert control over their personal information at the time that it is being disclosed.

Preferred form of proposed changes

16. My preferred mechanism for enacting these changes would be through amending IPP 11, such that a disclosing agency has to notify the individual concerned that their information has been disclosed to a third party. It would be preferable to strengthen the amendment such that, where possible, notification is provided before the information is disclosed with a minimum notice period, so that the individual has the opportunity to exercise a right to opt-out or request that information not be disclosed.

17. Other mechanisms that place the obligation on the collecting agency run the risk of the collecting agency being a poor actor and notification not being given, and it can be very difficult to ensure that information is deleted once they already have it. If there are no obligations on the disclosing agency, and the collecting agency is either unaware of their obligations or a poor actor, then we may remain with the status quo where no one other than those two agencies know that the information transfer has taken place. Furthermore, the disclosing agency may receive some form of monetary value in exchange for disclosing the information (e.g. selling information to an advertising agency), and therefore they may be more incentivised to ensure that they are meeting their regulatory requirements in order to not compromise their ongoing business model. It may also be easier for a disclosing agency to build the infrastructure to serve notifications if they are providing data to multiple agencies, rather than each of those collecting agencies having to build their own systems.

18. If it is decided that the proposed changes are through IPP3 or otherwise place the onus on the collecting agency to provide notification, then it may still be helpful to specify in IPP11 that for particular types of sensitive personal information (e.g. biometrics) that the disclosing agency has an obligation to also notify the individual of indirect collection. The development of a sensitivity classification may be useful for other sections of the Privacy Act too, and is discussed further in para 22-23.

19. Separately, it would be beneficial to add to IPP2 that where personal information is collected from public sources, the collecting agency must make reasonable efforts to notify the individual that their personal information has been collected and what that information may be used for.

20. Additionally, there may need to be some consideration for how any possible changes to the Privacy Act 2020 may interact with s11, particularly where agencies argue that a discloser collector relationship falls under this section. The threshold for use needs to be carefully considered in this context.

Applicability to individuals overseas vs domestically

21. While it is understandable that policymakers may want to limit the impact of changes by only requiring notification of indirect collection of information for individuals overseas, that would stop individuals in New Zealand from benefitting from the stronger protections. If we accept that notification of indirect collection is a good thing, then ethically it should be made available to all individuals under the jurisdiction of the Act. Harm can still accrue from the indirect collection of information within our domestic borders (perhaps most significantly when transferred between

government agencies), and so these protections should apply to agencies operating exclusively domestically too.

22. If some form of reduction in scope is considered necessary to mitigate the risks of introducing the possible changes, then it may be better to base that on the sensitivity of the personal information through a risk-based approach rather than on jurisdiction. For example, the UK Information Commissioner's Office maintains a list of "Examples of processing likely to result in high risk" based on both the type of information and the applications. A similar approach was taken in the European Union s development of AI regulation, which separated use cases into unacceptable risk, high-risk, and limited or minimal risk categories.

23. As the harms are more serious where the personal information being disclosed is more sensitive (e.g. biometrics), it would be appropriate to still require notification/action in these circumstances. This approach could even allow for banning unconsented and unnotified transfer of personal information for particular very high-risk applications (e.g. real-time biometric identification systems or social scoring), requiring agencies to collect the information from individuals directly. While this approach may require more maintenance than a purely principle-based approach (and therefore should be maintained by the Office of the Privacy Commissioner rather than through legislation), it would also offer more flexibility to allow lower risk indirect collection to occur without notification.

Thank you for considering this submission. I would be happy to engage in further dialogue about these issues in the future if that would be helpful to officials.

Possible changes to notification rules under the Privacy Act 2020

Chorus feedback to the Ministry of Justice

CHORUS

Summary of Chorus feedback

The proposed notification rules will not meaningfully improve transparency and may require a disproportionate administrative burden. The proposed notification changes will not provide individuals with a meaningful improvement to transparency and their privacy rights. There may be a disproportionate administrative burden to comply if the changes are implemented in a "one size fits all" approach, requiring granular notification requirements. Although it might be beneficial to align the Privacy Act 2020 with other key jurisdictions, the Ministry's engagement paper does not identify specific examples of harms arising from the current notification gap. We would encourage further work on identifying the harms, in order to better assess the trade-offs that will come with adding new requirements to the Act. If changes are to be made, we recommend that the onus to notify should be on the original collecting agency, and any changes use the existing 'principles-based' approach in the Privacy Act rather than mandating granular notification. We support the exceptions proposed and provide some suggestions, but we don't see merit in the changes only applying to overseas individuals.

If changes are to be made, we recommend:

- The onus to notify should be on the original collecting agency as they are better placed to notify. The original collecting agency who discloses information to a third party will likely in most cases be better placed to give any required notifications or disclosures. As such, we would support a change to IPP 11 over a change to IPP 2, IPP 3 or a new IPP. Chorus is a wholesaler of telecommunication services, and retail service providers have the primary relationship with end users of our services. These retail service providers disclose to us end users' details, and importantly we are subject to legal restrictions on the extent of our contact with end users. As a result, we often have incomplete or out of date contact details of end users so it will be difficult to notify end users. This may be the case with other wholesalers, or where a supplier/service provider has no relationship with, or is constrained from contacting, end customers.

- Not mandating granular notification requirements as they would be onerous and disproportionate. We see significant downsides in mandating notification at a granular level (e.g., notifying individuals directly, or notifying individual instances of indirect collection). This would have the adverse effect of forcing agencies to build systems that track individuals more closely, so that particular collections or notifications can be associated with their profiles. It may also force agencies to be more aggressive in collecting contact information that is not otherwise required. If the aim is to put individuals in a better position to understand who holds their information, then the least intrusive way to achieve this is to require agencies to take reasonable steps to disclose details of the agencies (or, if this is not practicable, the kinds of agencies) to whom they disclose personal information. For example, if a business publishes a list of third parties to whom they disclose customer information, then any interested customer can look up the list and start contacting those third parties in order to exercise their privacy rights (e.g., access and correction under the Act).

- The exception where the individual already has the information. This would support practical compliance, as the agency indirectly collecting the information could get assurances from the disclosing agency that this has occurred. In addition, as a way to limit the circumstances to notify, we suggest that the agency indirectly collecting is required to notify only if it is not "reasonably practicable" for the original collecting agency to do so. This builds on established concepts in the Privacy Act around practical compliance and reflects its principles-based approach.

- Not having the notification rules only apply to overseas individuals as this will be difficult to implement. Whilst we appreciate approaches to reduce the compliance burden, reducing the scope of notification to overseas individuals only will be hard to implement in practice. This is because it is often difficult to categorise overseas individuals in a data set (particularly with information that doesn't lend itself to determine this, such as IP addresses).

Chorus feedback in more detail

Chorus is New Zealand's largest telecommunications infrastructure company. We are a regulated wholesaler of telecommunications services, and provide our services to retail services companies (RSPs). Under this split, we have limited access to communicate with end-users of our services. As is set out below, this brings challenges should there be additional requirements to notify end-users of our services.

We agree that the indirect collection of information is increasing, and we see this being driven by technology changes and agencies wanting to share their information to offer better products and services to consumers. Transparency is an important element to empower people to exercise their privacy rights, but we believe that that at a practical level the existing notification requirements in the Privacy Act provide this.

We have provided feedback on your questions below.

1. What factors do you think are most important when considering changes to indirect collection of personal information?

A key factor to consider for any changes are the compliance impact on agencies, including clarity on what's required on agencies to comply, and the effort and associated cost to comply. Others factors to consider are assessing whether the change will actually provide a meaningful improvement in individuals' privacy rights, and any adverse consequences from agencies' compliance activities.

2. What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?

For individuals, a new notification requirement may provide incremental transparency of where people's information has been collected from. However, this needs to be considered against existing protections in the Privacy Act, and agency's existing privacy practices.

If the aim is to make it easier for individuals to find out who they should contact to exercise their privacy rights (and to make informed privacy decisions), we would suggest that any reforms should aim for the 'lightest touch' measures that achieve that aim.

Agencies can comply with existing notification requirements under their privacy policies. Chorus, like other agencies with comprehensive privacy policies, already cover where information may be collected indirectly.

Therefore, we are not convinced the proposed change will actually be effective in providing greater transparency to improve people's privacy rights.

3. What form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate.

Rather than amending the Privacy Act, we recommend that a more effective and practical initiative would be for the Privacy Commissioner to provide further training and tools for agencies to better understand the sources that they collect and share information. These sorts of data flow resources will have the benefit of supporting agencies to comply with IPP 2, IPP 3 and IPP 11 generally.

If necessary, focus on IPP 11 –the onus being on the disclosing agency to notify
However, if after this consultation the Ministry determines that amendments are necessary, our recommendation is to amend IPP 11 – and not IPP 2, IPP3, or introduce a new IPP. Amending IPP11 would more appropriately put the notification onus on the agency that discloses (or will disclose) the information it collected to a third party. This is preferable as a disclosing agency is likely to have a relationship with the individual who it collected the information from, that the agency who indirectly collects the information does not.

Chorus has limitations around contacting end users, and may not have up-to-date end user details (as the RSP has the primary relationship with end users). As a result, it will be difficult for Chorus to notify end users. Other wholesalers or suppliers / service providers may similarly not have a relationship with, or are constrained from contacting, end customers. Therefore, amending IPP 11 would cater for these indirect relationships with end customers / users.

Amending IP 11 would also make more sense from the individual's perspective. If the agency who is indirectly collecting the information is to notify the individual of the collection (as would be the effect under the proposed amendments to IPP 2 or 3), the individual may be confused as to why they are getting notified and may get notified multiple times for the same set of information. For example, if Chorus uses a platform provider to support our order process (and for the purposes of section 11 of the Act assume the platform uses some information sent to it for its own purpose). If the platform was required to notify an end user each time their details were added to that platform's database, end users might get very confused given that it is a back office tool that would normally send communications branded with the organisation implementing the order.

As a related point, section 11 of the Act provides that transferring information to another agency for that agency to hold or process solely on the transferring agency's behalf (i.e., as an agent) is not a disclosure under IPP 11. It is not clear how this section aligns with the aim of new notification requirements. If section 11 applies there would not be a "disclosure" requiring notification and therefore an individual would not know that their information was disclosed to another agency, which cuts across the aim of the new notification requirements.

Preserve principles-based approach

If the requirements for indirect collection are amended as currently proposed, we would strongly support structuring the changes in a manner that respects the existing principles-based approach embedded in the Act, anchored around concepts of reasonableness, practicality, and proportionality.

We see significant downsides in a 'one-size fits all' approach such as requiring notifications be sent directly to individuals, or requiring notification of individual instances of collection, since this would require agencies to build systems that can track when a particular individual's information is indirectly collected and whether that person has been notified. The compliance costs and implementation challenges of such an approach would be significant, and for many organisations, prohibitive. Based on the engagement paper, it also appears disproportionate given the lack of evidence for existing consumer harm.

Consistent with the existing 'principles-based' approach embedded in the Act - a more flexible and proportionate approach would require only reasonable steps to ensure that an individual can ascertain to whom their personal information has been disclosed. It would also include exceptions where (for example) an agency believes on reasonable grounds that compliance would prejudice the purposes of collection. This would provide disclosing agencies with greater flexibility in how to meet the requirement. For example, disclosing details to individuals on request, or publishing general information (e.g., in a privacy policy) identifying the third parties to whom it has disclosed various categories of personal information. In turn, that should be sufficient to allow interested individuals to find out who has indirectly collected their personal information (and to exercise their rights under IPPs 6 and 7 if desired).

Other considerations if the onus is on the agency indirectly collecting

If the onus is instead placed on the collecting agency to make disclosures about indirect collection, then:

- *Publish general notification information not individual notifications.* It would be desirable to structure the requirements so that in most cases the agency can comply by publishing general information (e.g., in its privacy policy) about the types of information it collects and who it collects the information from, rather than requiring notification to individuals for every instance of indirect collection. As we state above, any legal requirement to protect individual privacy should be mindful of the potential for public apathy due to notification fatigue, and the compliance costs of building systems to track and manage individual collections and notifications.

- *List kinds of entities that collect information from.* It would be desirable to ensure that, consistent with 5.11 of the OAIC guidelines on APP 5 (the Australian equivalent privacy principle for notification), if it is not practicable to notify the name of each entity from whom information is collected from (for example, because the collecting agency collects information from a variety of sources and it would not be practicable to give a separate notice in relation to each entity), the collecting agency can comply with notification requirements by instead indicating the kinds of entities from which it collects that information.

4. If you are a New Zealand business, are there any practical implementation issues you can identify in complying with the proposed changes?

As above, there would be practical difficulties to individually notify people given an agency indirectly collecting information may not have any, or correct, contact details of individuals that the information relates to. This is particularly in the case of IP addresses or device information that may be collected and shared with third parties where this information is associated with unique identifiers, rather than a person's contact details. For example, someone visits a website, and that individual's IP and device information, along with their interactions on the webpage, is collected to build a profile of that individual's preferences. If this is disclosed to another agency, then it is going to be difficult, and probably impossible for the agency that has indirectly collected the information to notify the individual given they do not have contact details. The broad definition of "personal information" means that agencies may be dealing with personal information without any way to actually contact the relevant individual without the assistance of the collecting agency.

As outlined above, we foresee significant practical issues and costs with a 'one-size fits all' approach such as requiring notifications directly to individuals, or requiring notification of individual instances of collection, since this would require agencies to build systems that can track when a particular individual's information is indirectly collected and whether that person has been notified.

5. Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?

If there was mandated notification at a granular level, there is an additional risk of unintended consequences given agencies may commit a privacy breach if they hold incomplete or incorrect contact information and contact the wrong individuals.

We support the exception to the indirect notification requirement when an individual has already been provided the information as required under IPP 3. This would support practical compliance, as the agency indirectly collecting the information could get assurances from the disclosing agency that this has occurred. This often occurs in practice, including by checking the disclosing agency's privacy policy that individuals have adequate notification at the point of the original collection that disclosure to another party is possible.

Although we prefer the exception above, we comment below on the other ways listed to mitigate risk:

- *Limiting circumstances when notification to be provided.* Whilst we appreciate the flexibility with the suggested language "any steps that are in the circumstances, reasonable" it may be a practical challenge for the agency indirectly collecting the information to determine what is reasonable. We suggest it would be better if the agency indirectly collecting the information has an obligation to notify only if it's "not reasonably practicable" for the original collecting agency to do so.

  This uses the existing approach in IPPs 2[1] and 3[2], where there is an exception to comply when "…compliance is not reasonably practicable in the circumstances of the particular case". Whilst there would be a level of uncertainty as to what is "reasonable", this is tied to the concept of what is "practical" and importantly uses the foundation of established concepts in the Privacy Act.

- *Notification to overseas individuals*. Whilst we acknowledge the intention to reduce the compliance burden by reducing the scope of who needs to be notified, we suggest that limiting notification requirements to overseas individuals would introduce complexity for agencies to comply with. This

[1] IPP 2 (2)(f).
[2] IPP 3 (4)(d).

is because there will be practical challenges to implement processes to determine overseas individuals in an agency's data set and then ensuring additional notification requirements target that group. Practically, agencies may just decide to apply the additional notification to both overseas and New Zealand based individuals.

Again, this becomes even more challenging when collecting IP addresses, device information, or other information that does not lend itself to being able to easily contact the individual. This is because it would be difficult, and in some cases unrealistic, to establish whether that person is in outside of New Zealand.

6. Should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?

As above, limiting additional notification requirements to information collected from overseas individuals may be difficult implement in practice. It would be unusual to have a regime that in theory provides greater protection to overseas individual's data compared to individuals in the jurisdiction itself.

So, if the notification requirements would not apply to New Zealanders, then unless there is a clear international consequence of not changing the notification requirements (please see below), it is difficult to see why it should instead only apply to overseas based individuals.

7. Is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback

We appreciate the aim of improving transparency, but based on the engagement document it is unclear what is driving these changes. Importantly, it is unclear what degree of harm the proposals are intended to address – besides an attempt to better align ourselves with overseas approaches. As a result, the current proposals appear disproportionate where the likely cost of implementation (and potential adverse side-effects) will outweigh benefits to consumers.

There is mention of New Zealand being out of step with the notification requirements in other jurisdictions. But there is no insight of the potential consequences of this (such as the risk of New Zealand losing its adequacy status under the GDPR), or whether this gap has had an adverse impact on people's privacy.

30th September 2022

Electoral and Constitutional Team
Ministry of Justice

By email only: privacyfeedback@justice.govt.nz

Tenā kotou,

PROPOSED CHANGES TO NOTIFICATION RULES UNDER THE PRIVACY ACT 2020
Submission in support of REINZ submission

1. Crockers Realty Limited is a member of the Real Estate Institute of New Zealand (REINZ), a membership organisation supporting the real estate profession across New Zealand. Our sales practice is focused primarily on the sale of residential and commercial properties.
2. REINZ has lodged a submission in respect of the above consultation currently underway.
3. As outlined by REINZ in their submission, we are dependent on the availability of data on recent home sales to discharge our legal obligations to clients under the Real Estate Agents Act.
4. As the sales market can move quickly, the availability of the REINZ data series is crucial to our ability to provide clients with an accurate assessment of the value of their home – as is our legal obligation as real estate agents.
5. Changes that delayed or made this data unavailable would have ramifications for the quality of the service we are able to provide to consumers.
6. We wholeheartedly support REINZ's submission and note that we are able and willing to participate in direct member feedback sessions as suggested by REINZ, if this would be of use to MOJ.

Please do not hesitate to contact the writer should you have any queries in respect of this submission.

Naku noa, nā

s9(2)(a)

Helen O'Sullivan
Chief Executive Officer, Crockers Realty Limited

E property@crockers.co.nz
T +64 9 630 8890
F 0800 CROCKERS (2762 5377)

CROCKERS PROPERTY GROUP
525 Manukau Road, Epsom, Auckland 1023, New Zealand
PO Box 74054, Greenlane, Auckland 1546, New Zealand

MANAGEMENT
REALTY
BODY CORP

EST. 1971
crockers.co.nz

Crockers Property Management Ltd | Crockers Body Corporate Management Ltd | Crockers Realty Ltd *Licensed (REAA 2008)*

NEW ZEALAND
CUSTOMS SERVICE
TE MANA ĀRAI O AOTEAROA

PROTECTING NEW ZEALAND'S BORDER

The Customhouse, 1 Hinemoa Street, Wellington
PO Box 2218, Wellington 6140
Phone: +64 4 901 4500

29 September 2022

Electoral and Constitutional
Ministry of Justice
PO Box 180
Wellington 6140

Broadening the Privacy Act's notification rules

Thank you for the opportunity to provide feedback on potentia changes to notification requirements for indirect collection of personal information under the Privacy Act 2020.

Personal information is critical for the fulfilment of Te Mana Ārai o Aotearoa / New Zealand Customs Service's (Customs) statutory functions. Customs manages the flow of goods, people, and craft across the New Zealand border, and these domains are rich in personal information. Personal information collected from third parties (rather than directly from the individual) is an essential aspect of these functions.

Examples of collection of indirect personal information from FY 2021/2022
(provisional figures)

- Customs staff processed 25.5 million import and export transactions (20.3m and 5.2m respectively), each of which contained information collected about the importer and exporter – including personal information where that party is an individual rather than a company.
- Customs collected $17.5 billion in revenue on behalf of the Crown.
- Customs prevented $3.7 billion of potential social and economic harm by seizing drugs at our border and offshore. This involved working with Customs' counterparts for other countries, as well as collecting 3rd party information from numerous sources.

It is of utmost importance to Customs that we collect, store, use and disclose personal information in ways that maintain public trust and confidence. It is also essential that the right balance is struck between transparency and operational effectiveness and efficiency across Customs' areas of responsibility. Any changes to notifications requirements under the Privacy Act 2020 will significantly impact our ability to fulfil our statutory functions. As such Customs has considerable interest in this proposal.

1. What factors do you think are most important when considering changes to indirect collection of personal information?

There are numerous factors to consider relating to scope and how any new requirements would be applied in practice. Generally, ensuring sure that -

- changes are technically and logistically feasible to implement and maintain

- if IPP3 is amended (per question 3), it is made explicit that notification to individuals does not need to be direct and can take any form appropriate in the circumstance, consistent with current configuration of IPP 3(1), 3(2), 3(3) and 3(4). This is philosophically consistent with both the policy objective and the configuration and intent of the principles-based approach of the Privacy Act. It is essential that agencies can use their judgement, rather than be bound by a prescriptive format
- changes are designed with careful consideration as to the timeline of changes, (providing sufficient opportunity for agencies to make necessary adjustments), and accompanied by adequate guidance that includes clear expectations from both the Ministry of Justice and the Privacy Commissioner
- benefits obtained clearly outweigh the potential costs and risks, including the risk of notification fatigue and the risk of creating tension in commercial relationships
- any new requirements are appropriately aligned with agencies' existing obligations under empowering legislation (such as the Customs and Excise Act, or GST Act etc) regarding information that is required to be collected from 3rd parties (rather than the individual).

Further, it is essential that changes do not inhibit Customs' ability to carry out designated statutory functions, particularly with respect to law enforcement and national security.

2. What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?

Advantages / Benefits

We anticipate the potential benefits would primarily be realised by the individual rather than by Customs, through greater awareness and potentially greater control of their personal information.

Customs may benefit through enhanced public trust and confidence stemming from greater transparency and awareness - but notes the possibility of an undermining effect on trust and confidence stemming from notification burden and confusion due to the additional volume of information being provided to the public.

Disadvantages

Law enforcement and national security

This proposal, depending on its ultimate design, has significant implications for Customs' ability to conduct investigative and law enforcement activities.

It's not clear how far reaching this provision would extend – for example, would it include information obtained from covert human sources? What about information that is available to the public consistent with IPP 2(d)? Would existing exceptions present in the Act be implemented for this new issue?

Too broad a provision could cover, for example, all the requests for information we make of other agencies in relation to investigative targets or whenever another agency provides us with intelligence reporting which contains personal information. It could cover personal information provided to us by Corrections and IRD for the purpose of identifying people with bail conditions attempting to travel or student loan debtors. This would be highly problematic from our perspective.

There is a risk that third parties from whom we seek information for intelligence purposes might notify an individual that a law enforcement agency is seeking information about them.

This applies to companies that operate in New Zealand and offshore, and where the information on the individual may have been collected offshore (e.g., airlines). This may happen unintentionally, for example, where one agency lacks the contextual knowledge to appreciate the significance of certain information to another agency. Again, this scenario is highly problematic from our perspective.

Customs' preferred approach involves a clear exemption with respect to data used for law enforcement / national security purposes. We consider other exemptions may be needed, for example, for the purpose of managing communicable disease outbreaks.

These exemptions are broadly consistent with the existing regime which has carve outs for compliance prejudicing the purpose of collection, or publicly available information, or where non-compliance is necessary to avoid prejudicing government functions (law enforcement, revenue, judicial proceedings).

Practical application and anticipated compliance burden on part of agencies

Depending on final design (and the notification mechanisms permitted or required), enhanced notification requirements could significantly impact operations and have substantial resource implications for Customs.

This reflects the volume of personal information we collect (see below tables) and that the majority of that information is collected indirectly via domestic and international third party providers. With respect to intelligence activities specifically, even if there is a broad exemption, agencies will still encounter a compliance burden as they work to ensure their activities fit into that exemption (e.g. legal advice).

To give an idea of the scale of information involved for Customs -

Passengers - In the last full year pre Covid-19 (01 Jan 2019 – 31 Dec 2019), passenger number entering and exiting NZ via the air pathway were -

Passenger direction	***Total number of passengers***
Arrival	*7,031,090*
Departure	*6,999,166*
Total	***14,030,256***

This information was collected via a third party for each of these individual passenger movements and submitted to Custom for processing and risk assessment purposes.

Cargo - These numbers represent the previous five calendar months (April – August 2022) of import and export movements (ICR and Entry transactions (Inward)) -

Cargo Reports	*8,924,805*
Entries	*1,413,562*
Total	***10,338,367***

Each individual number represents an importation or exportation by an individual person or business. This information is provided by the individual or business to a Customs Broker who in turn submit that information in the prescribed format to Customs (and other Border Agencies) for risk assessment / revenue collection purposes.

There are also implicit quality issues in notification, particularly around whether appropriate identity information has been provided by a third party. For example, the majority of the cargo reports are low value goods on an electronic manifest, with supporting data that may be insufficient for contact to be made with the individual importer or exporter. Nor will it

enable us to state confidently that the notification is going to the right place – this could proliferate breaches.

The complexity of the proposed notification system is a critical consideration.

- Who would have the responsibility to provide notification? This is especially relevant where transactions are 'daisy chained' – e.g., foreign domestic post disclosing to foreign customs disclosing to global shipping company disclosing to sub contractor disclosing to a ship (noting that this cycle could occur a number of times for some goods) before goods and import information arrive in New Zealand.
- Can the third party do it? They are already responsible for providing clear guidance on their disclosures under IPP 3(1)(c) – one mechanism to ensure commercial systems are sufficiently transparent is through ensuring one party is providing information for *each transmission.* This would prevent two notifications for each transfer of information.
- Would a blanket notification be acceptable (e.g., on Customs' website)?
- Can a notification be covered within a terms of sale notice in the standard transaction? This is going to be of particular relevance for companies not domiciled in New Zealand who sell goods into New Zealand. Would Customs be compensating for companies who don't provide detail about their information to customers, thereby shifting the cost onto the New Zealand public?
- From a data science perspective, how would notifications function if we ingested bulk datasets containing open source details (e.g., Companies office data containing director and shareholder details)?
- Would it cover large datasets (e.g., advanced passenger notification (PNR) data received from airlines)?

These questions are of relevance to the successful implementation of any notification regime and apply more broadly than Customs.

Broader impact on operations

Customs identifies, assesses and mitigates risks for international passengers and exports / imports in advance. This advanced processing, part of what enables us to provide efficient arrival processes that benefit the public, is almost entirely dependent on 3rd party collection.

Excessive notification burden or additional restrictions in information stemming from new notification requirements will inhibit the flow of legitimate passengers and goods entering / exiting the country. This is not operationally viable for Customs.

Noting the volume of information Customs currently collects in this way, (and that this volume is scheduled to substantially increase by the end of 2023 due to the additional data that will soon accompany all postal items), the possibility of a privacy breach would also increase (e.g. due to incorrect data collection at source or inadequacies in contact information provided).

Notification fatigue

Depending on design (and as noted in your consultation document), there is a risk that people will receive such a volume of notifications that they disengage, ultimately leading to less and not greater transparency and awareness. It may be challenging for the recipient to interpret the information provided.

3. What form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate.

Form

Amending IPP 3 seems to be the simplest mechanism to ensuring the policy objective (broadly summarised as improving transparency). Theoretically, a small amendment to the language of IPP3 could achieve this goal. This would enable the following existing exceptions to carry over –

- the concept of IPP 3(1) 'reasonable in the circumstances'
- the sequencing under IPP 3(2)
- the repetition issue under IPP 3(3)
- the existing exceptions under IPP 3(4).

These existing facets of IPP3 will be critical to an appropriate extension to notification and are philosophically consistent with other principles (critically, IPP 1, which applies regardless of the directness or indirectness of collection of personal information).

The other options appear to be more challenging to implement and would duplicate much of the IPP 3 content – which is already consistent with the other principles. There is also a risk that if a new IPP ("IPP X") were created there could be a gap between the application of IPP 3 and IPP X.

Use case guidance

Ideally, guidance should be issued around specific use cases where disclosure to the individual is required (where indirect collection has occurred). For example, a key driver appears to be the commercialisation of personal information so should the provision be designed around imposing the obligation in those circumstances?

Form of disclosure guidance

Guidance should also be issued regarding the appropriateness of selected mechanisms for communication.

5. Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?

Additional risks include -

- creating relationship tensions between agencies who share information, and potential ambiguity for individuals due to inconsistent messaging around the disclosure and the collection
- socialising costs onto Government agencies (and thereby the taxpayer)
- broadly, the creation of new risks through efforts to manage the existing risk – for example, Customs is aware that phishing scams can be conducted via privacy notifications to individuals (eg, via privacy notification emails requiring people to click an online link to opt out of future notifications).

Mitigations include -

- clarification that existing exceptions in the Privacy Act (or in IPP 3) apply
- issuing guidance around the form of disclosure (including using public notices), and guidance around use cases

- adding a section 30(1)(e) enabling OPC to authorise collection otherwise inconsistent with IPP 3
- careful consideration of allowable notification mechanisms.

6. Should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?

To answer this question completely, Customs would need to understand the policy desires underpinning each option.

Applying a *direct notification* (rather than public notices, or another mechanism of notification) to people residing overseas would require Customs to collect more information to be able to identify residency. This would be very complex - potentially unworkable – and likely error prone.

7. Is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback.

Te Mana Ārai o Aotearoa/Customs has nothing further to add at this stage. We look forward to further information and consultation on the proposal as it progresses and are happy to provide further feedback, including greater detail on individual issues, if that is useful. In the first instance, please contact Rachel Winthrop - rachel.winthrop@customs.govt.nz.

Carter, Adam

From: Neil Bryant s9(2)(a)
Sent: Thursday, 29 September 2022 8:43 pm
To: Privacy Feedback
Subject: Feedback on changes to Privacy Act 2020

Hi,

My email is in response to the request for feedback regarding the proposed changes to the Privacy Act 2020, as detailed here:
https://www.justice.govt.nz/justice-sector-policy/key-initiatives/broadening-the-privacy-acts-notification-rules/

I am writing this on behalf of Data Insight, which is one of the many analytics consultancy organisations that operate within NZ. We work with a number of different organisations across all sectors, with a focus on finance, government, telco, utilities, and the retail sector.

1. **What factors do you think are most important when considering changes to indirect collection of personal information?**

   I believe the most important factor is the benefit it provides the public who are affected by the changes, as well as what the flow on effects of any change could be. Another would be the cost associated to the change, and how this balances with the benefit that it provides. I can understand the desire to strengthen the current privacy laws, and make sure that data being collected is being used in a responsible manner. This brings to one of the largest factors involved, which is how the data that is being collected is being used, as this has the largest influence on the impact to the New Zealand public.

2. **What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?**

   Advantages – providing New Zealande s with confidence that their data is secure, adhering to international / EU standards, and clear communication should their data personal identifiable information (PII) be used in a way that doesn't benefit them by a party they didn't agree to sharing that information with.

   Disadvantages – depending on how it is implemented, it potentially creates a significant cost and barrier to using 3rd parties, particularly at a time when there is already a shortage of analytical support in the industry. If they have to notify customers every time they use a 3rd party, many may simply see it as being too difficult and stop using data partners all together. This will also mean they won't be able to deliver on their business initiatives, and customers will end up with a worse result because of a lack of analytical power. The cost of notifying is also significant, but even more than that is the perceived damage to reputation by nature of customers getting notified that their data is being used by a 3rd party. The customer does not understand the data world well enough to know what is best practice and what isn't, which means any notification at all about data being used by another company will likely damage their view of the agency the customer has a relationship with.

3. **What form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate.**

   We believe that amending one of the current IPP sections would be the best approach. Regarding how this is amended is the biggest factor in determining the impact that it has on agencies and individuals. The manner in which a 3rd party uses a customer's data varies significantly, and should be reflected in any changes to the Privacy Act. Should a company hire a consultant to help with building a churn model, would the company need to notify all 1 million customers they have about it (since the consultant would have

access to PII)? Likely not necessary, nor any benefit to the individual for doing so. However, if a 3rd party were to purchase PII from a company for the purpose of marketing to them, then it would make more sense for the individuals affected to be notified about this.

4. **If you are a New Zealand business, are there any practical implementation issues you can identify in complying with the proposed changes?**

   Below are the main practical issues:
   - Duplication of communication - most businesses already inform customers about how their data will be used in the T&C's. Would they need to notify their customers every time a 3rd party gains access to PII data? Once per year per 3rd party? These details would need to be clear in any ammendment
   - Many New Zealand business don't manage or hold their own data, and use agencies that are specialized on this. This could potentially punish such companies more, since they would then have to essentially notify every customer they have about their data storage solutions
   - What is the definition of 'collects'? Does this specifically mean that they are hosting the data themselves, rather than simply accessing it? It also draws back to my point raised in section 3, that the intended use of the data is the more critical element in deciding whether or not notifying the individual is necessary.

5. **Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?**

   One part I couldn't see addressed was the frequency or volume of notifications that would be deemed necessary. If the data is refreshed on a daily or weekly basis, would the individual need to be notified every single time that their data has been collected by a 3rd party? Another mitigation that we weren't sure about was the circumstances that would mean an agency can instead take "any steps that are, in the circumstances, reasonable to notify individuals about the collection of information". Does this imply that it would be up to the agency to decide whether or not it is reasonable to contact individuals, compared to simply putting it in the T&C's (which also notifies the individual)?

   I would also raise again the idea of reputation damage that I don't believe has been considered yet. Any notification that a 3rd party is accessing your data is likely to be met with poor reception, particularly since the individuals wont necessarily understand enough of the data world to know whether it is 'right' or 'wrong' use of their data. This is highly likely to become a barrier to operate for any companies affected.

6. **Should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?**

   I was a bit unsure about what this question means sorry – would this mean that a consideration is whether or not the changes should apply to individuals based only overseas vs individuals in New Zealand? Assuming this is the right interpretation, I would think that any changes made would be made to both individuals overseas and in New Zealand.

7. **Is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback.**

   That is all from me, thank you very much for asking for feedback on this. My only other recommendation would be for further discussion with the agencies affected by the change (i.e. those who would be 3rd parties collecting PII) to help ensure a smooth transition for any potential changes to the current act.

Thanks
Neil Bryant

Neil Bryant
Head of Analytics

m: s9(2)(a) **w:** datainsight.co.nz

7 St Benedicts Street, Eden Terrace, Auckland, New Zealand

Carter, Adam

From: Paul Davies <paul.davies@pdlaw.co.nz>
Sent: Wednesday, 31 August 2022 10:32 am
To: Privacy Feedback
Subject: Feedback

Important Factors
In my view these are:

1. The practicality of any new obligation;
2. Clarity of any new obligation so that compliance is clear;
3. The content of the notice, ie how this person uses, stores, and protects and how that might be different from the collector's policies;
4. A range of consequences for breaches from minor to significant, and repeated breaches.

Some privacy policies contain wide authorisation to share all personal information collected, particularly in large organisations where data sharing is common across groups of companies and with business partners.

In that regard, not all personal information is equal. For example, sharing a name and contact details across a group of companies and business partners relying on a general policy may be reasonable but sharing personal financial information may require explicit consent.

Defining collection in these circumstances can be difficult. For example, if a person provides access to personal information it holds, is that the same as a third party collecting that data? Should it be?

Perhaps an inadvertent impact of the prosed change is how one-off data sharing is dealt with. Rightly or wrongly, it is not uncommon for two organisations to share personal information about a common customer, particularly where there are problems and mostly without specific authorisation. While the person sharing that data may breach the Act without thinking, a new notice obligation is likely going to impact these one-off situations significantly and especially if the recipient (collector) and discloser both have notice obligations and consequences.

Advantages and Disadvantages
The clear advantage to individuals of this proposal is that it will make consent real, ie the knowledge of where and how personal information is shared, and what controls exist will not stop with the original collectors' generic and wide privacy policy.

The clear disadvantages include:

1. the cost to implement the regime for those who do share personal information;
2. that non-complying organisations have an advantage over compliant organisations unless there is enforcement.

Form of Change
If the proposal proceeds, my view is that it must be a binding obligation with consequences for breach. That's because compliance is going to cost some organisations a lot of money in terms of implementation and maintenance. It wouldn't be equitable if the good corporate citizens complied, and the bad actors were let off because of soft rules.

Practical Implementation Issues
Most have been highlighted: Is access collection or do you need the ability to modify, change, or delete? In my view, sharing is the same as a collection even if the recipient doesn't become a data owner. Who gives the notice? In what timeframes? What should it contain? A scale of enforcement responses, small to large fines, repeat offenders, etc.

An implementation period would be critically important perhaps with extra time for existing c/f new sharing arrangements.

Scope of Change

I cannot see any basis to limit this change to information collected from overseas persons.

Other

It is disappointing when personal information is shared, especially when it is unexpected and the sharing is discovered in error. The proposed changes sound fantastic, and in an ideal world, I would support them. However, I do not think the proposed changes should be implemented. The reason for my view is that the harm caused by sharing, or third-party collection, does not justify the widespread compliance and enforcement costs that will flow from the proposed changes.

Regards

Paul Davies
paul.davies@pdlaw.co.nz
Direct +64 9 357 0676
Mobile s9(2)(a)

PaulDavies|Law
Paul Davies Law Limited
Level 10, 55 Shortland Street, Auckland
P O Box 767, Shortland Street, Auckland
Facsimile +64 9 357 0678

http://www.pdlaw.co.nz

Carter, Adam

From: Judd de la Roche s9(2)(a)
Sent: Thursday, 29 September 2022 8:22 am
To: Privacy Feedback
Subject: Feedback submission regarding third party authorization

Proper Broker

To whomever it may concern,

I have answered the questions you have asked to be addressed below and from a real estate perspective whereby sale prices and addresses are collected by salespeople and passed on to REINZ for national statistics on New Zealand's real estate market.

1.What factors do you think are most important when considering changes to indirect collection of personal information?
I believe the question needs to be asked: If changes are needed, why are they needed? Does someone in the DoJ feel it is a good idea or is there pressure from an overseas body?, Has there been a breach of information and if so, how many and what is the scale of the issue? Is this proposed change and the cost and effort involved warranted? Will the proposed changes actually protect data better or could it be sourced by someone to use in a nefarious way anyway? How would someone actually use this data in a nefarious way?

2. What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?
I cannot think of one advantage unless nefarious use of this data is occurring at this time. The disadvantages are numerous:

It is important to appreciate the gravity of the decisions made with the REINZ sales data collected by the salespeople at the coalface. This data is used by the Reserve Bank to analyse the health of the housing market which is a barometer of the overall health of the economy. This data is fresh, being available monthly and even in real time as the month progresses. The official cash rate (OCR) is determined by such information which then has a flow on to the interest rates set by the banks and a direct effect on how much money home owners need to find to service their mortgages. This information is available to trading banks and valuers also. It would

be fair to say, this data is of critical national importance and the flow of which MUST be timely and unfettered. This cannot be stated strongly enough.

3. What form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate.

I believe no change is warranted for the sake of change.
The privacy situation and the collection of information of both parties to a transaction (buyer and seller of property) is clearly noted in clause 19.0 in the Agreement for Sale and Purchase Of Real Estate (produced by ADLS and REINZ) and this is reproduced below:

19.0 Collection of Sales Information
19.1 Once this agreement has become unconditional in all respects, the agent may provide certain information relating to the sale to the
Real Estate Institute of New Zealand Incorporated (REINZ).
19.2 This information will be stored on a secure password protected network under REINZ's control and may include (amongst other
things) the sale price and the address of the property, but will not include the parties' names or other personal information under
the Privacy Act 2020.
19.3 This information is collected, used and published for statistical, property appraisal and market analysis purposes, by REINZ, REINZ
member agents and others.
19.4 Despite the above, if REINZ does come to hold any of the vendor's or purchaser's personal information, that party has a right to
access and correct that personal information by contacting REINZ at info@reinz.co.nz or by post or telephone.

In 27 years of real estate, I have clearly stated to buyers and sellers that data surrounding the sale / purchase of their property will be passed on to REINZ and never has anyone refused or been concerned in any way about this.

4. If you are a New Zealand business, are there any practical implementation issues you can identify in complying with the proposed changes?
The proposed change requiring a third party to affirm the use of the sellers details of their sale is troublesome as it requires the recording of contact details of those individuals. Currently, the contact details of the seller and the buyer (This is the buyer's information also remember) are not recorded by REINZ (see 19.2 above). For a third party to gain clearance to use data, the contact details will then be needed to be passed to these third parties. This is more opportunity for nefarious entities to source this information which previously did not exist in REINZ databases. This is a bigger issue than the one trying to be solved here is it not?

Also, what is the definition of a third party? So far we have defined REINZ as the third party, but when REINZ passes the sales statistics to the Reserve Bank every month, will the Reserve Bank need to contact every agent for clearance to use the data that is legally theirs at that point, because the agent is then the third down the chain of that information? Or would the Reserve Bank need to go to the seller and the buyer or indeed all three? Clearly, this is impractical and opens a vast number of doors for sensitive information that is currently not captured, to be harvested by some computer hacker. This is a very real scenario. I can see yet another layer of legislation coming after this layer to try and stop any leakage of information. Blocking a sieve is somewhat difficult. The current practice works perfectly well and if there is an issue that the MoJ observes currently, the business community should be informed of this with real numbers and incidences, not hypothesis that a problem may exist. Fair enough?

In practice, when the legislators have no way of practically outlawing and stopping an event, historically they tend to introduce a penalty by way of fines upon those who have failed to perform their duty (i.e a data leak). The risk to parties involves would be huge if names and contact details are available in the data and businesses would be at risk of fines.

What if the buyer or seller or both are deceased? Who does the third party contact? This data is all historical and people tend to die, so how would authority to use the data work in this instance? Does the third party contact the lawyer, the trustees, the descendants or a medium? Can you begin to imagine the issues?

5. Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?

Carrying on from number 4 above, the facts are very clear that the path for a third party to gain authority to use this sales data, is tortuous and in many cases would end in exhaustion due to inability to complete or too higher cost. There for we have GAPS in the data and an incomplete data set. REINZ have been compiling sales statistics since 1992 and this data is invaluable and any law change that would threaten the integrity of this data would be a crime in itself.

6. Should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?

Many sellers and buyers of New Zealand property do indeed live overseas and have every right to buy property or sell property in New Zealand. Their information regarding their sale or purchase is required for national statistics, like those who reside in New Zealand. Both those who reside overseas and are resident in New

Zealand, bind themselves to this requirement upon signing of an agency and/or upon signing of a sale and purchase agreement.

7. Is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback.

Everyone appreciates that privacy must be respected. Also, everyone would agree that the biggest issues with protecting privacy should be addressed in order of importance. The greatest threat to the public's privacy is definitely not third party authorization, but rather AML data. Anti Money laundering data collection modus operandi is a complete disaster waiting to happen. The fact that a hacker has not broken into one of the hundreds of servers (physical or cloud) which contains pictures of passports, credit cards, addresses, full names, reasons for selling etc etc, is either a complete miracle or it has not been reported. I would strongly suggest the elephant in the room is not third party authorization of data use, but rather an immediate and urgent overhaul of the AML data protection by way of one central, secure database. Moj and DIA need to get on to that huge issue and not be worried about the trivia of third party authorization. As the Jedi knight says "…There is nothing to see here".

Thank you for the opportunity to put in this submission.

Judd de la Roche
Residential Sales Consultant
Mosgiel
s9(2)(a) | s9(2)(a)

Property Brokers
125 Gordon Road Mosgiel, Dunedin 9024
pb.co.nz

大成 DENTONS KENSINGTON SWAN

Dentons Kensington Swan
89 The Terrace
PO Box 10246
Wellington 6140
New Zealand

dentons.co.nz

Electoral and Constitutional
Ministry of Justice
PO Box 180
Wellington 6150

By email:
privacyfeedback@justice.govt.nz

30 September 2022

Feedback – Possible changes to the notification rules under the Privacy Act 2020

1 About Dentons Kensington Swan

1.1 This submission sets out feedback from Dentons Kensington Swan on the possible changes to the notification rules under the Privacy Act 2020 ('**Privacy Act**'). This submission is made by the firm and not on behalf of any client of the firm.

1.2 We have extensive experience advising a range of agencies in various industries who collect, hold, and process personal information. We act for consumer-facing organisations, social media platforms, government departments, software developers, users of cloud technology, and a wide variety of other agencies who use personal information in the course of their business.

1.3 We assist clients in New Zealand and overseas with their regulatory compliance obligations, and initiatives aimed at proactively addressing risk to our clients, and their customers and employees in respect of the treatment of personal information.

1.4 Our lawyers have also advised clients, in New Zealand and overseas, in relation to their compliance obligations under the European Union's General Data Protection Regulation ('**GDPR**'); its United Kingdom equivalent; and the California Consumer Privacy Act.

2 General comment

2.1 We do not believe that any changes to the Privacy Act to address indirect collection of personal information are warranted. In our view, the existing regime contemplated by the IPPs (and in particular, IPPs 2, 3 and 11) is sufficient.

2.2 We do not understand there to be an identified policy problem that requires the indirection collection of personal information to be specifically addressed any more so than it is currently, and we are concerned that the imposition of additional notification requirements are likely to result in, as the Ministry has identified, both 'notification fatigue' and increased compliance costs (without a corresponding tangible benefit for consumers).

2.3 While we do generally support changes to New Zealand privacy law that will result in a harmonisation of practices in Aotearoa with practices in other key jurisdictions, such as the EU, the UK and Australia, we think that any proposed changes:

a must be assessed in the context of the 'principles'-based approach of the Privacy Act, which is much less prescriptive than the approach followed by other more formal data protection regimes such as the GDPR; and

b must also recognise that the imposition of similar indirect notification requirements under the laws of other jurisdictions are likely to have led to a realisation of the concerns identified by the Ministry – that is, 'notification fatigue' and increased compliance costs – and accordingly should only be implemented with a view to securing tangible benefits for consumers (and not just 'for the sake' of harmonisation).

2.4 That said, we are always supportive of changes to the Privacy Act which will result in New Zealand maintaining its status of adequacy under the EU and UK GDPRs. Our view is that the benefits that New Zealand's 'white list' status bring are significant, and most likely underappreciated by New Zealand agencies. Our experience dealing with cross-border transfers involving jurisdictions other than 'white list' jurisdictions has given us a solid insight into the significant challenges faced by businesses looking to sell into the EU or the UK who aren't able to benefit in the same way as New Zealand businesses can. If the proposed changes to the Privacy Act are a 'necessary evil' – that is, a condition of New Zealand maintaining its adequacy status – then we think such changes are ultimately a price worth paying.

3 Feedback on the Ministry's questions

(1) What factors do you think are most important when considering changes to indirect collection of personal information? / (2) What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?

3.1 The factors that we think are most important, and the likely advantages and disadvantages of broadening the notification requirements, are as follows:

Whether the proposed changes will bring a tangible benefit to consumers, who will end up 'better informed' about the use of thei personal information.	We think that is unlikely. Agencies who collect personal information directly from individuals (in this feedback, 'collecting agencies') are already under an obligation under IPP 3 to make appropriate disclosures regarding the purposes for which their information is to be collected, and the intended recipients of that information. If collecting agencies are not making appropriate disclosures in their privacy statements or otherwise informing individuals at, or as soon as practicable after, the time of collection, then those agencies are not fulfilling their obligations under IPP 3. Collecting agencies – who form the initial relationship with the individuals from whom the information is collected – are the best-placed to make the disclosures and provide the information that an individual needs to understand the likely journey of their personal information.

	Retaining the onus on collecting agencies to include appropria e disclosures in their privacy statements also helps ensure that individuals are able to retain some control about how their personal information is to be used in the future, since the individuals are informed at the time of their collection who might receive the information, and the purposes for which it may be used. In our view, that is the appropriate time: in particular, in circumstances where the proposed future use of their information may be a relevant consideration as to whether the individual wishes to proceed to engage with the collecting agency, taking into account the collecting agency's privacy practices. This further emphasises that the onus must fall on the collecting agency to properly describe the intended recipients of, and purposes for using, the individual's personal information. We also share the Ministry's concerns regarding 'notification fatigue'. Our view is that requiring additional disclosures, from agencies who receive personal information from a collecting agency (in this feedback, 'recipient agencies') – all relating to effectively the 'same collection – is likely to result in consumers 'switching off' to 'yet another email or tick box exercise'. Our preference would be to see more guidance, and more enforcement, in relation to IPP 3, encouraging a more transparent and engaging 'user journey' regarding the disclosures that a collecting agency is required to make at the time of initial collection from the individual.
The likely compliance costs for agencies required to comply	Our expectation is that many agencies operating in New Zealand rely on the indirect collection of personal information in their day-to-day operations. They do so, in theory, in reliance on their ability to collect that personal information from another agency under IPP 2. In theory, agencies who initially collect the personal information from the individuals concerned and make that information available to the other agency do so on the basis of disclosures which comply with IPP 3 and in accordance with IPP 11 respectively. That framework already provides a solid basis on which a recipient agency may collect personal information from a collecting agency, in circumstances which – provided that IPP 3 and IPP 11 have been complied with – should result in personal information being collected and disclosed in the manner anticipated by individuals. The introduction of a new privacy principle or changes to existing privacy principles will require a significant review of public-facing privacy disclosures, only a short time after most agencies have reviewed theirs in light of the new Privacy Act coming into force in late 2020. In the absence of any tangible enforcement action being taken against agencies that do not make appropriate

	disclosures (including the many agencies which have failed to update their privacy statements to take into account the changes in 2020), New Zealand agencies may suffer from 'compliance fatigue' and may refuse to, or may delay, making any changes necessary. This is particularly likely to be the case where the Ministry is unable to clearly explain the rationale for imposing an additional compliance obligation on New Zealand agencies, where there is no obvious or well-articulated tangible benefit to consumers.
Retention of New Zealand's status of adequacy	We think that the benefits that New Zealand's 'white list' status bring are significant, and most likely underappreciated by New Zealand agencies. If changes to New Zealand privacy law are necessary in order to ensure that we maintain this status, then ultimately we think such changes are likely to be worthwhile (despite the other drawbacks of the changes identified in this feedback).

(3) What form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate. / (4) If you are a New Zealand business, are there any practical implementation issues you can identify in complying with the proposed changes? / (5) Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?

3.2 As noted above, we think that changes are unnecessary on the basis that the existing regime contemplated by the IPPs (and in particular, IPPs 2, 3 and 11) is sufficient.

3.3 However, if changes are necessary, we would support a change which continues to place the onus on (or, indeed, emphasises the existing obligation on) the collecting agency to make sufficient disclosures to individuals about where their personal information will end up.

3.4 This is because it is the collecting agency which forms the 'relationship' with the individual concerned, at the time of collection of the personal information. Collecting agencies are best-placed to provide the information about the likely 'journey' of the personal information, including details of the other agencies likely to receive that information, and the purposes for which they might be disclosed that information. Where practicable, that agency can also provide contact details for the recipient agencies to facilitate individuals exercising their access and correction rights.

3.5 In our view, this approach is the most practical to implement, in that:

a it will result in only a single notification to consumers, at the time of collection of their personal information (or shortly afterwards) – that is, when consumers are more likely to be engaged – thereby being less likely to lead to notification fatigue;

b in theory, a collecting agency's existing disclosure that complies with IPP 3 should contain most, if not all, of the information that would be made available to consumers.

3.6 We expect that implementing this approach would require, at most, a few 'tweaks' to IPP 3 (or, perhaps only some guidelines), which could contemplate that the collecting agency must include in its IPP 3-compliant disclosure to individuals:

a contact details about each recipient agency to whom the collecting agency is likely to disclose personal information (and in this regard, the collecting agency may need to be under an express obligation to keep the details of the likely recipient agencies up-to-date on its website);

b more specifics about the purposes for which disclosures may be made to the likely recipient agencies.

3.7 We think changes of this nature are likely to result in the least administrative burden – in particular for agencies that already follow best practice when it comes to the transparency and clarity of their privacy statements – yet are still likely to deliver the same (if not more) benefits that the other proposals, due to the likely mitigation of 'notification fatigue' through the single notification approach.

3.8 With respect to the proposed changes contemplated by the consultation paper:

a We think that any extension of IPP 3 which would require a privacy statement to be disclosed to individuals at the time the recipient agency collects personal information from a collecting agency:

i is more likely to lead to 'notification fatigue' and confusion, especially since the individual may have forgotten the initial contact with the collecting agency which has led to the further disclosure;

ii may be difficult to implement in practice, especially if the recipient agency has not received contact details for the individual concerned (or, it could lead to an additional disclosure of personal information, and a corresponding risk to individuals, if the collecting agency is required to disclose contact details to the recipient agency to enable the recipient agency to fulfil its notification obligation).

b We think that an amendment to IPP 11 to require a collecting agency to make a further privacy disclosure at the time of disclosing personal information to a recipient agency is more likely to lead to 'notification fatigue' and confusion. Such a disclosure would not be built into the initial 'user journey' at the time of collection, but would instead have to be integrated into a further engagement between the collecting agency and the individual concerned, which may be seen as intrusive or overwhelming for the individual.

c We do not think that an amendment to IPP 2 that would narrow the exceptions that allow indirect collection of personal information is warranted. Those exceptions are, in our view, reasonable, and so far as we are aware, there is no obvious policy reason to restrict the ability of agencies to indirectly collection personal information.

(6) Should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?

3.9 We see no reason to distinguish between individuals overseas and individuals in New Zealand (unless to do so is the bare minimum required for New Zealand to maintain adequacy status).

4 Further information

4.1 We are happy to discuss any aspects of our feedback on the possible changes to the notification rules under the Privacy Act.

4.2 Thank you for the opportunity to provide feedback.

Yours faithfully

s9(2)(a)

Hayden Wilson
Chair & Partner
Dentons Kensington Swan

D +64 4 915 0782
hayden.wilson@dentons.com

s9(2)(a)

Campbell Featherstone
Partner
Dentons Kensington Swan

D +64 4 498 0832
campbell.featherstone@dentons.com

s9(2)(a)

Partner
Dentons Kensington Swan

D +64 9 915 3366
hayley.miller@dentons.com

Carter, Adam

From: Fiona Staples <Fiona.Staples@dia.govt.nz>
Sent: Monday, 3 October 2022 9:40 am
To: Privacy Feedback
Subject: Feedback - possible changes to notification rules under Privacy Act 2020
Attachments: FW: Privacy Act 2020 - possible changes to notification rules [CALL FOR FEEDBACK BY 28 SEPT 2022]

Kia ora

My apologies for the slight delay in providing our feedback. I hope it is still able to be considered. I have received the following feedback from our Service Delivery and Operations branch:

Personal information is core to Kāwai ki te Iwi's identity-related products and services. We collect personal information to enable us to process and register over 20 products, services, and life events. Our key products and services relate to registering births, deaths, marriages and civil unions, issuing passports and other travel documents, and processing applications for citizenship and verified RealMe accounts.

To ensure those who receive our products and services, or who register life events, do so legitimately, we must have the ability to investigate possible false applications.

The Department takes our obligations under the Privacy Act seriously, and the decision to collect personal information from someone other than the individual concerned is not taken lightly. Information is collected this way either to ensure its accurate and to make an application easier for an applicant (with their knowledge) or to investigate suspected instances of fraudulent applications or registrations.

1. What factors do you think are most important when considering changes to indirect collection of personal information?

In our context there are a number of factors when considering requiring agencies to notify individuals when their personal information is collected from a third party. The Department ~~is the~~ shares personal information widely under Approved Information Sharing Agreements (for example, birth and death information is shared with the Ministry of Social Development). We also collect information on behalf of other agencies, where the individual chooses to provide it. (e.g. people can apply for benefit changes or an IR number as part of registering a birth). In processing applications for citizenship we receive travel and visa information from Immigration New Zealand and character information from the NZ Police and the NZSIS. When processing an individual's first passport application we receive citizenship and identity information from either the citizenship or birth registers.

Collecting or enabling other agencies to collect personal information indirectly ensures that the information is accurate, and that it is easier for applicants to apply for a service. It's unclear from the paper if an individual's consent to these indirect collections at the point of application would meet the requirement of notification.

In our view, the following are important consideration:

- whether the indirect collection is necessary for the service applied for, (e.g. it's necessary to collect travel and visa information from INZ as part of a citizenship application)
- whether the individual consents to that collection at the point of application (e.g. provides an identity witness as part of a passport application process, consenting to the Department contacting that witness)

- whether the individual explicitly provided the information to be shared with another agency (e.g. asked that birth registration information be shared with IR or MSD).

I note that any requirement to notify may also be logistically difficult to implement for the following reasons:

- much of our collection and sharing is automated, so would need possibly tricky and resource-intensive system changes
- the contact details provided with the application may not be up to date or fit for purpose
- it's unclear how the requirement would be monitored and the consequences of non-compliance
- it's unclear if requiring notification in all instances would achieve the outcome of increasing transparency, or would instead result in 'notification fatigue'.

2. What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?

We can see that there are some advantages in broadening the notification requirements. A requirement would enable individuals to better see how their information is used and reused across data systems. It may also provide them with the opportunity to ensure that their information is fit for the purpose for which it's shared. It could also increase public trust in the use and reuse of information across government.

Some possible disadvantages are that:

- individuals may be notified of sharing where they've already consented
- notifying could undermine the purpose for not collecting the information directly from the individual, e.g. where an agency is investigating possible fraud
- it could be unclear who to notify. In our context we sometimes have two people claiming one identity
- Resource-intensive for agencies. This would either be expensive to automate, or require extra staff to implement. As our services are provided on a cost recovery basis, it could increase the cost of those services for consumers
- Contact details may not be available or may be out of date, or more information than necessary is collected to enable notification

3. What form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate.

From the information in the consultation document I think an amendment to IPP2 to narrow the exceptions that allow agencies not to collect information directly from the individual concerned would be our preferred option. This would be likely to ensure the appropriate balance between enabling information to be shared where necessary (e.g. to investigate a crime or prevent harm) and ensuring people are aware of the use and reuse of their personal information. This could also enable an individual to authorise the disclosure of their personal information to other agencies. For example, customers regularly ask the Department to share their name change information across Government. We are currently unable to do so (because we don't have the system functionality), but are considering developing a service enabling people to share their information with other agencies. This could also manage concerns (below) about sharing that is authorised under an information-matching programme or AISA.

From a DIA perspective there are some possible fishhooks in the notification proposal. From time to time people apply for products or services, or register events, on behalf of others (for example, funeral directors register deaths on behalf of next of kin). The Department would be concerned if the changes were to require the Department to notify individuals when someone applies for a product or service, or registers a life event, on behalf. Should this proposal proceed, we're keen to work with you to ensure that the notification provisions both meet the purposes of notification and are able to be implemented.

I note that there are already requirements to notify people where an adverse action may result from information-sharing (e.g. where information about a death means that a pension will stop). While this doesn't increase transparency across the board, it does ensure that individuals are not adversely impacted by mistakes when sharing personal information. In our view duplicative requirements to notify (as would happen in these use cases) should be avoided.

I'd suggest that information sharing that is already regulated by an information-matching programme or an AISA should be out of scope of the notification requirements. Reporting and notification requirements are already built into these programmes by agencies, Cabinet and the Commissioner as part of their development.

4. If you are a New Zealand business, are there any practical implementation issues you can identify in complying with the proposed changes?

N/A

5. Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?

As set out above, the Department would be concerned if notification requirements undermined the purpose of disclosure or collection, e.g. investigating fraud or other unlawful activities. Introducing these requirements ~~may also result in businesses or agencies~~ would almost certainly lead to agencies such as ours needing to collect and hold more personal information for individuals than they otherwise would need to e.g. additional contact information to notify individuals. We see this as a major negative unintended consequence of the proposal.

6. Should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?

The Department does not have a view on this question. The Department collects limited personal information indirectly on individuals based outside of New Zealand. These are usually New Zealand citizens, or applicants for New Zealand citizenship by descent. As part of the citizenship registration process or passport application process the Department may contact the identity witness provided with the application. This is part of our processes to ensure that the applicant is who they say they are, and are entitled to the product for which they've applied.

In these cases the identity witness is provided by the individual concerned (or their parent / guardian). Depending on the way in which a requirement to notify is drafted, it's likely we would consider that the individual concerned s already aware that the Department will collect information from the witness.

7. Is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback.

There should be considerations made to the collection of information pertaining to a child. Would agencies be required to notify one or both parents where a child's information is collected indirectly?

As noted above, the Department's preference is that this would exclude all information matching programmes where there are information matching provisions specified under schedule 5 of the Privacy Act 2020 as they are already covered by the notification requirements under schedule 6. In particular, section 1(2) of Schedule 6 states "Nothing in subclause (1) requires an agency to notify any individual about an authorised information matching programme if to do so would be likely to frustrate the objective of the programme."

In our view, information-sharing under Part 7 of the Act should also be included, including that set out in Schedules 3 (Identity Information) and 4 (Law Enforcement Information).

I've also received feedback from another staff member in Service Delivery and Operations – please see attached.

If you have any questions please get in touch and I can connect you with the right people.

Ngā mihi
Fiona

Fiona Staples (she/her)
Manager Information Management and Privacy

Workplace Services Group
He Pou Aronui | Organisational Capability and Services Branch
Te Tari Taiwhenua | Department of Internal Affairs
Mobile: s9(2)(a) | Fiona.staples@dia.govt.nz
Level 3 | 45 Pipitea St | PO Box 805, Wellington 6140
www.dia.govt.nz

MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA

Ministry of Education submission to the Ministry of Justice on the proposed changes to notification rules under the Privacy Act 2020

Key Feedback Messages

- We support making changes to notification rules under the Privacy Act 2020 to include notifications of indirect collection of personal information through an amendment to IPP 3.
- It is conceptually consistent with the right to privacy, whether understood as a right to control use and access to one's information or as a right to be let alone from interference, that personal data collected from third parties are subject to the Privacy Act.
- Broadening the notification rules strengthens the framework for privacy provided by the Privacy Act, particularly for children and young people who merit protection as they may be less aware of the risks, consequences, and their rights in relation to their personal data.
- We support making changes to our legislation to ensure NZ keeps up to date with best practice in overseas jurisdictions and to retain adequacy under EU law, with particular regard to General Data Protection Regulation (GDPR) Article 14 (Ar. 14).
- Alongside Ar.14, it is important the complimentary and supporting articles, rights, and exemptions to Ar.14 are also considered in terms of potential amendments to the Privacy Act. The articles and exemptions which enable Ar.14 to be operationalised in the EU will be necessary in NZ to enable an amendment based on Ar. 14 to be successfully operationalised. Lessons from EU experience on what not to do are also important.
- The operational implications of broadening notification rules on the Ministry and the education sector are likely to be large. It will take time to implement and embed the necessary changes.

Our response to the Ministry of Justice seven questions:

1. What factors do you think are most important when considering changes to indirect collection of personal information?

- **Timeline for changes**

  The Ministry will need time to implement changes to our processes and support the sector with changes to their processes (especially early learning services and schools). We would like to know the timeframes for the amendments, and whether there will be a grace period for compliance following royal assent. We would prefer the amendment to come into force in 2024 to provide sufficient time to operationalise the changes across the education sector.

- **What data is included?**

Personal information which moves to a receiving third party from the collecting party may also include information about the individual which has been created by the collecting party. The information about a person that is collected indirectly may not just be the personal data originally collected at source from the individual.

Clarity on how the Privacy Act amendment would treat information relating to a person that has been created by an agency would be useful to ensure that there is no ambiguity around what information is captured by an amendment to the notification requirements (see also our comments on pseudonymous or anonymous data under question 5). Additionally, clarity on how the amendment will apply to all parties downstream from the collecting party which may receive data would also be useful.

- **Application to current disclosures vs new disclosures**

  If the proposed amendment is intended to apply retrospectively to existing and ongoing information sharing arrangements, this could create operationally difficulties from two sets of rules on disclosures operating in the same agency. For example, a 5-year-old starting school after the amendment is enacted, vs an 8-year-old child already in a school with data moving under existing authorities to share.

  We will also need to consider whether changes to existing Information Sharing Agreements (ISAs) or Approved Information Sharing Agreements (AISAs) under the Privacy Act will be required. Many ISAs support the sharing of personal information between government agencies or third parties for purposes enabled by the Privacy Act (e.g., research and statistics) and involved indirect collection of personal information.

  Some of these agreements support on-going shares where notification was not required but maybe required because of the proposed amendment to notification rules. Expanding this thinking, we will also need to consider the impact of the proposed changes to existing privacy impact assessments that have been completed to support existing data collections and projects that use personal information.

- **Exemptions**

  Effective exemptions to the amendment will be critical, however, these exemptions should not be driven by administrative burdens government agencies may face in implementing the changes to the notification requirements under the Act.

  Insofar as amendment is enacted through revision of IPP3 (which we support), careful consideration should be given to the existing exemptions under IPP3 and the extent to which these should also apply to third-party collection.

  Insofar as amendment is aligned with the GDPR, careful consideration should be given to exemptions existing within that legislation (for example exemptions if data is required to be

shared under existing legislation or if data is already shared with the third party for an existing purpose).

Exemptions relating to the maintenance of law and order and health and safety, as in IPP 11, should also be considered (for example exemptions on notification when seeking to prevent potential risks to children).

- **Notifications**

Notification processes should achieve the intended purposes of the proposed amendments. A regime of notification to every learner (or parent/caregiver) for all indirect collections that form part of an agencies normal business operations (e.g., attendance data collections, school roll return collections for MOE) would be administratively impracticable and costly. Repeated notifications for these on-going regular indirect collections may also result in notification fatigue thus undermining the intended purposes of proposed changes. This potential impact could be exacerbated for individuals through notifications being received from multiple agencies.

2. What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?

The advantage is that it is conceptually consistent with and a strengthening to the right to privacy that that personal information indirectly collected from third parties are subject to the Privacy Act.

The disadvantages will come from how the amendment is operationalised. If notification is a burden on the individual receiving it, and overly costly for the agency implementing it, parties will seek to find work arounds which will undermine the integrity of our privacy framework. The potential for 'notification fatigue' is significant and could render the changes pointless if they are ignored by individuals, or not delivered in a plain language or age-appropriate manner. Also, it will be a disadvantage if the amendment is confusing and unclear, so that the requirements, obligations, and outcomes are unpredictable for entities operating under it.

3. What form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate.

- We agree with the Privacy Commissioner's submission for a revision to IPP 3.
- We agree with the Commissioner's comment: "*I expect that some agencies may express reservations from a compliance costs standpoint. Agencies collecting personal information could well incur at least some extra costs from updating their systems. However, as the Ministry identifies in the discussion paper, there is scope to design IPP 3 in a way that ensures the obligation both effects the policy objectives but is also practical, and not unduly burdensome for agencies. My Office will be pleased to assist the Ministry in these matters*."

- We welcome the offer of support by the Commissioner to the Ministry of Justice to ensure the changes are practical and not unduly burdensome.

4. If you are a New Zealand business, are there any practical implementation issues you can identify in complying with the proposed changes?

- N/A

5. Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?

How will the amendment apply to pseudonymous or anonymous data? There is much debate within the EU on the ability to re-identify purportedly anonymous data with other data sets, to form aggregated data which is then capable of identifying an individual.

The GDPR includes identified and identifiable natural persons and is clear that pseudonymous data, which the receiving party can attribute to an individual, is included. Anonymous information is not if it is: 'personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable'.

6. Should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?

There is no obvious rationale for offering under New Zealand law greater protection to privacy for New Zealanders or non-New Zealanders who reside in the jurisdiction of another State, and less protection to those residing within New Zealand. Residing in New Zealand should not come with a penalty to one's rights to privacy.

We note you mention that Japan and South Korea have recently introduced additional safeguards surrounding the notification rules for organisations indirectly collecting personal information of EU individuals. It would be impractical for NZ-based organisations to segregate information about EU citizens/residents from non-EU citizens/residents, and in any case how would this apply for joint NZ-EU citizens?

7. Is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback.

We have noted the confusion in the EU on the application of Art. 14 and the exemptions to it, and what counts as adequate notification. We stress the need for the definitions in the amendment to be very clear and the requirements for notification to not be ambiguous.

NZ can avoid the issues which have arisen for the EU with the GDPR through careful drafting of our amendment. For example, notice from the receiver being passed through and provided at point of collection by the collector, on the receiver's behalf, alongside the collector's own notification. This

would possibly not be compliant under the GDPR but would be an extremely simple way for all to manage notification.

EQUIFAX®

29 September 2022

Notification Rules Submission
Electoral and Constitutional
Ministry of Justice
PO Box 180
Wellington 6140

By email to: privacyfeedback@justice.govt.nz

Dear Madam/Sir

RE: Possible changes to notification rules under the Privacy Act 2020

1. We write in response to the Ministry of Justice's Consultation paper into 'Possible changes to notification rules under the Privacy Act 2020'. We are grateful for the opportunity to provide a submission on this issue.

2. Equifax is a credit reporting agency which is regulated under the Credit Reporting Privacy Code 2020 (Code). Equifax is also a member of the Marketing Association (MA). Equifax has had the opportunity to read the MA submission on this consultation and supports the contents of that submission.

3. Equifax makes this submission as it is a business that holds substantial information about individuals, and most of this is collected through indirect, but legally compliant, means. Equifax has two primary businesses, its credit reporting business, which is governed by the Code, and its marketing services business, which is governed by the Privacy Act (Act). Both businesses obtain most of their information indirectly, as discussed below.

4. The credit reporting business is based on sharing personal information, primarily among credit providers, to create a central repository of credit risk data relating to individuals. Lenders are required under the Code to obtain consent from individuals before undertaking a credit check. Once lenders have this consent, they share the individual's information with Equifax, and we return information on that individual. The information provided by the lender is added to the pool of information on that individual, and subsequently shared with other lenders.

5. The marketing services business contains a separate database of information on individuals. This is not part of the credit reporting business, and therefore is not governed by the Code. The marketing services database is comprised of some legacy publicly available data, but mostly through purchased, legally compliant, datasets. These datasets have been compiled by third parties, who often use prize competitions or incentivised surveys as consideration for a person providing their contact details for marketing purposes. Individuals expressly consent to their data being shared with third parties for marketing purposes, without necessarily knowing who these third parties will be.

6. In the event a consumer is not happy that their data has been shared, our customers direct complaints back to us, where we maintain robust opt-out processes and apply industry suppression

files including Do Not Call, Do Not Mail and Deceased suppressions to ensure we honour consumer preferences with regard to receiving marketing offers from third parties.

7. Turning to the Ministry's consultation document, we would be very concerned with the viability of either of our businesses if Equifax had to subsequently notify individuals that we hold their data, despite the fact the initial recipient, for example a lender or a data acquirer, had already complied with the obligations in IPP3 under the Act.

8. We cannot see any benefit to be obtained by making IPP3 apply to indirect recipients of personal information when the obligations will have already been carried out by the direct recipient. There is no 'gap' in the Act as such. If the direct recipient did not provide appropriate notice to the individuals concerned as to the collection, use and disclosure of their personal information, then that is a breach of the Act as it stands.

9. As well as offering no benefit, we consider that the proposed change to IPP3 could make the collection of personal information unworkable, if agencies must repeat steps already undertaken. This is especially so in relation to the credit reporting business, which is premised on the need to have rights to retain and share an individual's credit information. Further, credit reporting is already heavily regulated under the Code, which provides sufficient protections to individuals regarding their personal information.

10. As noted in the MA submission, many businesses use public information to supplement their own information. It would also be unworkable to require agencies to notify individuals every time their information is collected from a publicly available source. If there is a concern with privacy in relation to public sources, then it is these public sources that should be reviewed, not the agencies use of these.

11. As well as disagreeing with the suggested change to IPP3 to include indirect recipients, we also do not see any need to change IPP2 regarding the exceptions to collecting personal information from sources other than the individual, and IPP11 regarding disclosure. In both examples we give in relation to our credit reporting and marketing services businesses, it is not possible for us to collect this information directly from the individual. However, there is no detriment to individuals by this, as their protections under the Act regarding collection, use and disclosure of their personal information are sufficiently met by the direct recipient.

12. As noted above, we are grateful for the opportunity to submit on this consultation and welcome any questions you may have for us.

Yours faithfully

Deborah Malaghan
Head of Legal

Equifax New Zealand Information Services and Solutions Limited
NZBN 9429039517487
equifax.co.nz
+0800 692 733

Level 10, 48 Shortland Street,
Auckland 1010, New Zealand

FINANCIAL SERVICES FEDERATION

30 September 2022

Electoral and Constitutional
Ministry of Justice
PO Box 180
Wellington 6140

By email to: privacyfeedback@justice.govt.nz

Dear Madam/Sir,

Re: Broadening the notification requirements under the Privacy Act 2020

The Financial Services Federation ('FSF') is sincerely grateful for the opportunity to consult and provide feedback on the engagement document ("the paper") on broadening the notification requirements under the Privacy Act 2020.

By way of background, the FSF is the industry body representing responsible non-bank lenders, fleet and asset leasing providers and credit-related insurance providers. We have 89 members and affiliates providing these products to more than 1.7 million New Zealand consumers and business. Our affiliate members include internationally recognised legal and consulting partners. A list of our members is attached as Appendix A. Data relating to the extent to which FSF members (excluding Affiliate members) contribute to New Zealand consumers, society and business is attached as Appendix B.

Many of our members are entities which are dealing with personal information, including gathering information necessary for customer onboarding processes including processes that involve the use of authorised and disclosed outsourced partners and third parties. Thereby warranting FSF's submission today. The FSF is only able to comment from the perspective and usage of the financing sector.

Prior to answering the questions ahead, the FSF has some introductory comments to make.

The FSF found the interpretation of the engagement document to be problematic, and thus we have written our submission on the probability for either interpretation. The FSF encourages the OPC to clearly define third parties and consult on this definition prior to any finalisation of the amended expansion. This would ensure that the interpretation is correct and accurate and addresses the objective of the engagement document reasonably.

In particular, the FSF has issues with the interpretation of what the OPC considers a third party. Although FSF members require outsourced partners and third parties to finalise processes such as credit checks, this disclosure is made compliantly, and the individual has knowledge as to whom their personal information is being passed and for what purpose.

These third parties are not therefore collecting personal information indirectly and without good faith and purpose. To include these third parties in the scope of this expansion makes no sense, and therefore warrants clarification from the OPC as to the issues surrounding this transfer.

Question 1: What factors do you think are most important when considering changes to indirect collection of personal information?
As mentioned in our introductory comments, the FSF has concerns as to whether information that has already been obtained via a notification and then passed on to a service provider, whether this service provider would then need to provide notification of use of this personal information; considering the original party has already notified the consumer of the use of personal information for processes. This situation, which can be interpreted in the consultation document, would be unnecessary and practically impossible. It is obvious that the individual would have no doubt consented to that information being passed onto another agency for outsourced purposes.

The FSF suggests that their regulation only impacts those agencies who collect personal information indirectly for other purposes, and not through authorised access via a collector of the information.

Question 2: What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?
The FSF entirely supports consumers being aware of their personal information and where this is distributed and our members are highly concerned with the personal information they hold on behalf of consumers, and ensuring all information is collected, stored and disposed of in good faith and in a compliant and reasonable manner.

However, the FSF outlines some concerns about whether this regulation would require too much notification to the consumer which would then add to the notification fatigue already existent; perhaps an issue as a result of the interpretational issues that the engagement document holds.

If the amended expansion proposed further notification and therefore two sets of notifications, one from the party collecting the information, and another from the party who is processing on the behalf of the collector, then this creates issues. This would be beyond the reasonable expectations of notification and would then require two sets of notifications for the purpose of one process.

For example, the consumer provides personal information to a lender who then passes this information on to their credit check provider (or an outsourced partner/third party) who is processing on behalf of the lender (scenario A). The consumer does not need two sets of notifications from the lender and the credit check provider to state that they both have their information. This provides incredible disadvantages, adds to the notification fatigue of the consumer, and is a practically impossible requirement to meet as the credit check provider will already have the personal data as a necessity through a commercial partnership.

If in the instance that the notification requirements are broadened such that only where a third party acquires information indirectly and outside the purposes specified to the lender (scenario B), as stated in the example in the engagement document, then because FSF members do not engage in this behaviour, we would have no issue with this going ahead.

Question 3: What form do you think the proposed changes to notification rules under the Privacy Act should take?
The proposed changes should consider that business models typically require niche and consistent checks for processes such as lending criteria checks, and these are typically done by outsourced partners. Requiring this from outsourced partners who process checks on behalf of collectors would be a practically impossible and onerous burden to place on all parties to the transfer of personal information, thus not necessary.

If the OPC feels the need to extend this to all outsourced parties who receive information from business partners directly as part of user and service agreements, then the FSF requests that no more stringent a position be adopted than that of the Australian position. Many service providers in New Zealand also operate in Australia, and consistency in the legislation in this sphere will be critical. More burdensome legislation in New Zealand then affects the market and the ability to provide services in the market, stifling competition and efficiency.

Further, the FSF sees the proposed change to IPP 11, for scenarios such as scenario B outlined in our answer to question 2, would be most appropriate if the information is collected indirectly and not for the purpose that the consumer initially thought (such as credit checks). No further amendment would be necessary outside of this, except for enforcement where information indirectly collected is used not in compliance with the current Act.

Question 4: If you are a New Zealand business or agency, are there any practical implementation issues you can identify in complying with the proposed changes?
The practical implementation issues in scenarios such as scenario A, outlined in our answer to question 2, would be immense. They would frustrate already efficient and compliant processes where lenders collect information for agencies to process on their behalf. Then requiring that agency to contact the consumer again and disclose is impractical and would stifle and stall the transfer of information effectively for the consumer's benefit.

This scenario would also increase costs, as with any compliance, and also frustrate the timeframe in which processors on behalf of lenders have to complete therefore causing worse consumer outcomes. Lenders already disclose to consumers that their information will need to be passed on to authorised partners which process the information on their behalf and therefore expansion to require this would be a complete frustration of the process. FSF members do not allow for their consumer information to be passed on to indirect agencies which will then use this information for purposes outside the original collection and who did not have original authority in the first instance.

Question 5: Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?

The FSF does not have any other risks or mitigations to add that have not already been mentioned in the document and throughout our submission.

Question 6: Should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?
Members interpreted the engagement document as targeting New Zealand consumers, considering the law is domestic law and the consultation process has targeted entities operating domestically.

However, the FSF understands the larger risks associated with individuals overseas, and thus the need to consider overseas usage more so. This consideration, and the higher level of regulation required for overseas entities and individuals to mitigate global associated risks, should not impact the level of regulation on domestic users and entities. Changes should only obviously enhance protections to consumers, and they should be limited so they do not create unnecessary hurdles for business and consumer access to personal information.

International regulation should also be considered in this query, as General Data Protection Regulation ('GDPR') is a comprehensive international standard to which all entities who operate internationally abide. Thereby, further regulation on just an international front need to be considered in light of the existing regulations beyond the scope of the OPC.

Question 7: Is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback.
The FSF members note that any obligations which go above what the current Australian position requires for those entities using third party information will be met with difficulty and seen as unnecessarily burdensome, thereby frustrating an already well-efficient system.

Lastly, the FSF would like to strongly emphasise that only mischief where an entity acquires personal information indirectly, and where it would be unclear and not within the reasonable expectation of the individual for their information to be processed by that unknown agency (i.e., unknown marketing agency) that this mischief is targeted as opposed to the lenders and credit reporters who work in processes known to the individual and consented by the individual. Anything outside of this scenario would cause detriment to all three parties involved in the process.

Please do not hesitate to contact us if you wish for us to speak further to our points raised in this submission.

Yours sincerely

s9(2)(a)

Diana Yeritsyan
Legal and Policy Manager

Appendix A - FSF Membership List as at 1 August 2022

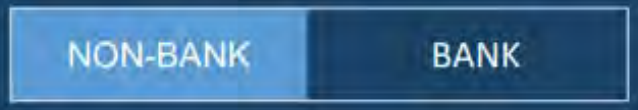
Non-Bank Deposit Takers, Insurance Premium Funders	Vehicle Lenders	Finance Companies/ Diversified Lenders	Finance Companies/ Diversified Lenders, Leasing Providers	Affiliate Members	Affiliate Members cont'd and Credit-related Insurance Providers
XCEDA (B)	AA Finance Limited	Avanti Finance ➢ Branded Financial	Nectar NZ Limited	Buddle Findlay	Credit Reporting, Debt Collection Agencies, Insurance Providers
Finance Direct Limited ➢ Lending Crowd	Auto Finance Direct Limited	Basalt Group	NZ Finance Ltd	Chapman Tripp	Baycorp (NZ) ➢ Credit Corp
Gold Band Finance ➢ Loan Co	BMW Financial Services ➢ Mini ➢ Alphera Financial Services	Basecorp Finance Ltd	Pepper NZ Limited	Credisense Ltd	Centrix
Mutual Credit Finance	Community Financial Services	Blackbird Finance	Personal Loan Corporation	Credit Sense Pty ltd	Collection House
Credit Unions/Building Societies	European Financial Services	Caterpillar Financial Services NZ Ltd	Pioneer Finance	Experian	Debt Managers
First Credit Union	Go Car Finance Ltd	Centracorp Finance 2000	Prospa NZ Ltd	Experieco Limited	Debtworks (NZ) Limited
Nelson Building Society	Honda Financial Services	Finance Now ➢ The Warehouse Financial Services ➢ SBS Insurance	Resimac NZ Limited	EY	Equifax (prev Veda)
Police and Families Credit Union	Kubota New Zealand Ltd	Future Finance	Smith's City Finance Ltd	FinTech NZ	Illion (prev Dun & Bradstreet (NZ) Limited
Steelsands Credit Union Inc	Mercedes-Benz Financial	Geneva Finance	Speirs Finance Group ➢ Speirs Finance ➢ Speirs Corporate & Leasing ➢ Yoogo Fleet	Finzsoft	Quadrant Group (NZ) Limited
Westforce Credit Union	Motor Trade Finance	Harmoney	Turners Automotive Group ➢ Autosure ➢ East Coast Credit ➢ Oxford Finance	Happy Prime Consultancy Limited	Credit-related Insurance Providers
Insurance Premium Funders	Nissan Financial Services NZ Ltd ➢ Mitsubishi Motors Financial Services ➢ Skyline Car Finance	Humm Group	UDC Finance Limited	Lendscape Ltd	Protecta Insurance
Elantis Premium Funding NZ Ltd	Onyx Finance Limited	Instant Finance ➢ Fair City ➢ My Finance	Leasing Providers	KPMG	Provident Insurance Corporation Ltd
Financial Synergy Limited	Scania Finance NZ Limited	John Deere Financial	Custom Fleet	LexisNexis	
Hunter Premium Funding	Toyota Finance NZ ➢ Mazda Finance	Latitude Financial	Fleet Partners NZ Ltd	Motor Trade Association	
IQumulate Premium Funding	Yamaha Motor Finance	Lifestyle Money NZ Ltd	ORIX New Zealand	PWC	
Rothbury Instalment Services		Limelight Group	SG Fleet	Simpson Western	
		Mainland Finance Limited		Verifier Australia	
		Metro Finance			Total 89 members

Appendix B – Key Facts from FSF Member Data Survey

FINANCIAL SERVICES FEDERATION (FSF)

THE NON-BANK FINANCE INDUSTRY SECTOR - 2022

48%



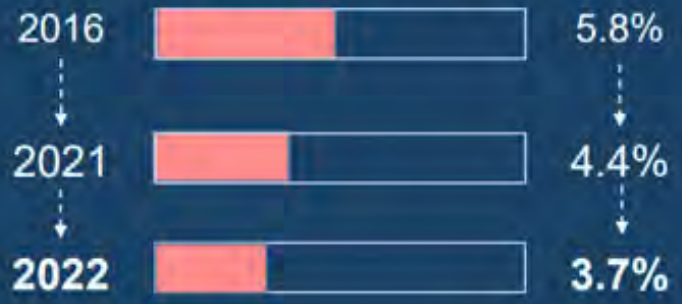
of personal consumer loans are financed by the **non-bank sector** represented by FSF members.

Setting industry standards for responsible lending, promoting compliance and consumer awareness.

Percent of Loan Requests Approved

46%

Percent of Loan Book in Arrears



Harcourts Group Limited
Licensed REAA 2008
Auckland Regional Office
PO Box 99 549, Newmarket
Auckland 1149
DX CX10299 Newmarket

P: +64 9 520 5569
F: +64 9 524 1481

30 September 2022

Electoral and Constitutional Team,
Ministry of Justice

By email only: privacyfeedback@justice.govt.nz

SUBMISSION ON CHANGES TO NOTIFICATION RULES UNDER THE PRIVACY ACT 2020

Introduction

1. This is a submission by Harcourts Group Limited (**"Harcourts", "We"**) in response to the Ministry of Justice's (**"MOJ"**) engagement document (**"Engagement Document"**) released in August 2022 on the possible changes to the privacy principles under the Privacy Act 2020 (**"Privacy Act"**) with respect to notification requirements.

2. Harcourts Group Limited ("**Harcourts**", "**Our**", "**We**") is the franchisor of New Zealand's largest real estate group. Now 134 years old and boasting 203 offices and 2,641 Sales Consultants as of 31 August 2022, Harcourts is a dominant presence in the New Zealand real estate market. We are committed to ensuring excellence at all levels of our business.

3. Our Sales Consultants collect personal information concerning the sale of properties when they enter into a listing agreement with the Vendor. As soon as a property sale becomes unconditional, we provide the property address, sale price and date of agreement to specific data collection agencies named in the listing agreement for the purposes of research and compiling sales statistics. Our Sales Consultants are also legally obliged to provide Purchasers and Vendors a true and accurate price range of a property.

4. We are a member of the Real Estate Institute of New Zealand (**"REINZ"**). We depend on recent property sales data provided by REINZ to provide an accurate price range of a property. This submission supplements the submission made by REINZ to the MOJ in respect of notification requirements under the Act.

Executive Summary

5. In our view, the status quo should prevail. There are no material gaps in the existing Privacy Act and Information Privacy Principles (**"IPPs"**) as it relates to the notification requirements for indirect collection of personal information.

6. However, to the extent that MOJ requires changes to the existing notification requirements:

   (a) We support REINZ's submission that it should only be limited to Option 1 proposed by MOJ in the Engagement Document.

   (b) However, we submit that the changes described in Option 1 should only apply to agencies indirectly collecting personal information of individuals based overseas.

Change of Notification Rules not Required

7. In our view, the status quo should prevail with respect to the collection of personal information of individuals in New Zealand, for the following reasons:

(a) The Information Privacy Principle 3 ("**IPP 3**") requires the agency to inform the individual intended recipients of the personal information collected. It is important to note that the IPP requires the name and address of the recipient agency that is collecting the information, as opposed to a category of recipients. In practice, to satisfy IPP 3, prior to collecting personal information, an agency would firstly obtain signed authority from the individual through a contractually binding agreement. For example, the listing agreement between our Sales Consultant and a property vendor would include an agreement that the personal information of the vendor would only be provided to certain third party agencies specifically named in the agreement. An additional requirement to notify the individual, who is already made aware, and have authorised access of their information adds no material value;

(b) Similarly, amending the exception to Information Privacy Principle 2 (**"IPP 2"**) concerning collection of information indirectly would add no material value. As mentioned in paragraph 7(a) above, the individual would have authorised the third party agency to collect the individual's information;

(c) IPP 3 also requires agencies to inform the individual of the intended purpose for which the information is being collected. This would form part of the authority obtained from the individual described in paragraph 7(a) above. A disclosing agency which indirectly collects information and discloses the information for a purpose to a third party not authorised by the individual would breach Information Privacy Principle ("**IPP 11**"). Accordingly, it creates unnecessary administrative cost and burden to require a disclosing agency to notify each individual their information (which they have authorised) have been shared. It is also neither necessary nor reasonably practicable to require notification for information which is publicly searchable; and

(d) Both the Information Privacy Principle 1 (**"IPP 1"**) and the Information Privacy Principle 12 (**"IPP 12"**) provide additional safeguards by preventing New Zealand agencies from:

i. collecting personal information that is not necessary for the function of the agency; and

ii. sending personal information to overseas agencies that may not provide comparable privacy safeguards, unless authorised by the individual.

If a change must be made

8. If a change is to be made to the notification requirements for indirect collection, we support REINZ's submission that it should only be limited to Option 1 but provided that similar exceptions under Australia's Privacy Principle are also available to New Zealand.

9. However, we submit that Option 1 should only apply to agencies indirectly collecting personal information of individuals based overseas. Overseas agencies may not be subject to privacy safeguards comparable to the New Zealand Privacy Act and thus, overseas individuals may not be sufficiently informed how their information is being collected and shared to a third party agency. In that regard, it is reasonable to require the agency to notify the individual concerned that their information has been collected indirectly and whether it has been disclosed.

Australia's Privacy Act 1988 and Privacy Principle 5

10. We acknowledge that Australia's Privacy Act 1988 and Privacy Principle 5 provides generally for notification, regardless of the manner of collection. However, as mentioned in REINZ's submissions, clause 5.6 of Australia's Privacy Principle 5 provides that notification can be satisfied by ensuring that the original agency collecting the personal information has given notice on behalf of the agency indirectly collecting the information, such as through an enforceable contractual agreement.

11. This is similar to the IPP 3, where the individual is required to be notified of the name and address of the agency that will be collecting and holding the information. Harcourts satisfies this requirement by entering into a listing agreement with a property vendor which includes the type of information being shared and the details of the

third party agencies the information is being shared. Accordingly, the original collecting agency would have notified the individual on behalf of the intended recipients or third party agencies.

United Kingdom Data Protection Act 2018

12. The Engagement Document referred to general notification obligations under the United Kingdom Data Protection Act 2018, including indirect collection under section 44(3). Section 44(3) provides that further information may be necessary if personal information is being collected without the knowledge of the individual.

13. We submit that further information is unnecessary under the requirements of the New Zealand Privacy Act and IPP 3, since the individual would have been informed that the individual's information is being collected by a third party agency at the time the individual gives authority to the original collecting agency.

General Data Protection Regulation ("GDPR"), the key privacy law of the European Union ("EU")

14. Although the GDPR requires an individual to be informed that their personal information is being collected, whether directly or indirectly, clause 5(a) of the Article 14 provides an exception if the individual is already informed of the collection.

15. We submit that the Privacy Act and IPP 3 requires the individual to be informed of third party agencies that are collecting their information indirectly. Therefore, under the GDPR additional notification is not required since the individual is already informed of the collection by the original collecting agency.

Feedback on the Seven Questions in the Engagement Document

16. We refer to MOJ's request for feedback on seven questions in the Engagement Document. Adopting the numbering in the Engagement Document, we comment as follows:

    (a) Question one - We believe it is important that the individual is sufficiently informed that their personal information is being collected, the purpose for the collection and the intended recipients of the information. The IPPs in the current form achieve this.

    (b) Question two - As mentioned above, there are no material benefits to broadening notification requirements for agencies indirectly collecting personal information domestically. The disadvantages are creating unnecessary compliance costs, practical difficulties in notifying individuals who do not have a direct relationship with the agency and notification fatigue, as individuals are notified (albeit unnecessary) when their information is collected and when information is disclosed.

    (c) Question three - There may be advantages for broader notification requirements to apply to agencies indirectly collecting personal information of individuals based overseas, since the original collecting agency may not have comparable privacy laws. However, we believe that broadening notification requirements for agencies collecting personal information of individuals in New Zealand is not necessary as the existing IPPs allow domestic individuals to be sufficiently notified.

    (d) Question four – Harcourts does not provide identifiable personal information of the individual to a third party agency. The proposed changes would create practical difficulties for the third party notifying the individual when collecting information.

    (e) Question five – A blanket requirement that a disclosing agency notify the individual concerned that their information has been disclosed to a third party (regardless of whether or not the disclosure itself is allowed) is unnecessary, especially considering the individual has been notified of the information collection by the third party agency or if the information is publicly searchable.

    (f) Question six – For the reasons mentioned above, the proposed changes, if required, should only be made in accordance to Option 1 and to apply only to personal information collected indirectly from individuals overseas.

(g) Question seven – We support REINZ's submission that introducing a new privacy principle requires further clarification by MOJ.

Further information

17. Harcourts is grateful for the opportunity to submit to the MOJ on the proposed changes to the IPPs. If the Electoral and Constitutional Team have any questions regarding any aspect of our feedback, please direct them to s9(2)(a)

Yours sincerely,

s9(2)(a)

Kelvin Wong
Legal Counsel
Harcourts Group Limited
Licensed Agent REAA 2008

ICNZ Insurance Council of New Zealand
Te Kāhui Inihua o Aotearoa

Insurance Council of New Zealand
Level 2 Asteron House, 139 The Terrace,
Wellington 6011
Tel 64 4 472 5230
Email icnz@icnz.org.nz
Fax 64 4 473 3011
www.icnz.org.nz

30 September 2022

By email: privacyfeedback@justice.govt.nz

Electoral and Constitutional
Ministry of Justice – Te Tāhū o te Ture

Dear Madam/Sir,

Submission on Broadening the Privacy Act's notification rules

Thank you for the opportunity to submit on the Ministry of Justice s – Te Tāhū o te Ture (**MOJ**'s) 'Possible changes to notification rules under the Privacy Act 2020' Engagement Document (**Engagement Document**).

By way of background, the Insurance Council of New Zealand - Te Kāhui Inihua o Aotearoa (**ICNZ**'s) members are general insurers and reinsurers that insure about 95 percent of the Aotearoa New Zealand general insurance market, including about a trillion dollars' worth of Aotearoa New Zealand assets and liabilities. ICNZ members provide insurance products ranging from those usually purchased by individuals (such as home and contents, travel and motor vehicle insurance) to those purchased by small businesses and larger organisations (such as Product and Public Liability, Business Interruption, Professional Indemnity, Commercial Property and Directors' and Officers' insurance).

Please contact Jane Brown s9(2)(a) if you have any questions about our submission or require further information

This submission has two parts:

- overarching comments, and
- responses to the questions in the Engagement Document.

Overarching comments

ICNZ understands from speaking with MOJ that this consultation has arisen in response to the EU Commission s review of Aotearoa New Zealand's adequacy status. We are supportive of Aotearoa retaining its adequacy status and recognise that this is a valuable tool for those entities doing business in the European Union. We also appreciate that while there is an apparent gap in the legislation at present where personal information is collected indirectly, in the majority of these situations the individual will have provided a general waiver for the agency to collect their information from third parties, which will include how their information will be used and shared.

In considering changes to the Privacy Act, which we understand is Parliament's intention, it is imperative that any future notification obligations do not become unduly onerous for the notifying agency, or so overwhelming for an individual as to lose their effectiveness, with the result that the individual is no better informed of their privacy rights or suffers from notification fatigue. This may require finding an appropriate balance, for example by only implementing this expectation for instances in which the customer does not already have the information.

The MOJ must also appreciate the potential administrative burden in complying with any proposed change to the law, and that implementing the necessary changes will likely be costly a cost that would inevitability end up being passed onto consumers. Insurers collect informat on from many sources when taking out cover, deciding whether or not to accept a risk and on what terms, as well as at claim time where many parties can be involved. This includes collection from other individuals, third party databases such as the NZTA's Motor Vehicle Register and the Insurance Claims Register, from repairers and suppliers, government agencies such as the New Zealand Police, and from other insurers. The impact of the proposed changes is therefore potentially significant for the general insurance sector.

Given this and recognising the high level at which the options have been framed in the consultation, ICNZ seeks further engagement from MOJ during its development of a preferred option (in advance of any legislation being introduced to Parliament), so as to ensure that whichever option is progressed is workable for the general insurance sector and its many customers.

Responses to the questions in the Engagement Document

The following section sets out ICNZ's responses to the questions set out in the Engagement Document.

Question 1.
What factors do you think are most important when considering changes to indirect collection of personal information?

Broadly, we believe that any changes need to specifically address circumstances where harm to individuals from the gap in the current notification regime could occur, and not introduce wide sweeping changes. Introducing wide sweeping changes has a high risk of creating unintended consequences or significantly increased compliance costs for businesses where there is nil to low levels of harm to the individual arising from a lack of notification of indirect collection.

Other important factor that must be considered include:

- Considering whether "blanket/general" notification to customers via existing privacy statements (and in the case of insurers, policy wordings) will suffice, or whether there will need to be specific notification each time a third party provides an individual's personal information, and if so, how that notification would need to be made.
- To ensure only instances of high risk or potential harm are captured, consideration should be given to ensuring the existing manner in which IPPs 2, 3 and 11 operate remains unaffected (aside from the amendment to address indirect collection notification) and New Zealand agencies are able to continue collecting personal information in largely the same manner as they do currently, without creating excessively onerous and costly compliance obligations.

- Avoiding notification fatigue for individuals which would dilute, if not erase, any benefit associated with the notification.
- Noting that for some agencies, such as insurers, who regularly collect from and share information with third parties, there is a risk that increased compliance costs will be passed onto consumers.
- Ensuring there is clarity in the definition of "indirect collection" so that agencies can appropriately scope the extent of their notification obligations. If necessary, distinguishing between indirect collection from a third party explicitly authorised by the individual (such as collection via an insurance adviser), and indirect collection through other means (such as an advertiser collecting information, as in the example used in the consultation document). It may also be appropriate for the indirect collection notification requirement to be targeted to circumstances where the indirect collection was not contemplated when the information was originally obtained.
- Considering where the onus for notification should lie (i.e., with the collecting agency or the disclosing agency), MOJ should consider:
  - Whether it is more appropriate for the collecting agency to provide notification to the individual given that they will be in a better position to explain how the information is intended to be used and how long it will be stored, how to access or correct the information, etc., however, noting this will occur after the disclosure has been made.
  - Whether the disclosing agency should have the obligation to notify the individual as they are likely to have an existing relationship with the individual and the notification could occur before the disclosure is made.
  - In either case, practicalities, avoiding duplicate notification in relation to the same use and notification fatigue, and compliance costs should be carefully considered.
- Whether, in broadening the notification requirement, there should also be notification exceptions introduced for agencies around indirect information that is collected for a lawful purpose connected with the agency's functions or activities, and the information is necessary for that purpose. In many cases collection of personal information is clearly envisaged and expected by the individual in the context of the transaction they are conducting and therefore any changes to the legislation which affect these scenarios are unlikely to benefit either individuals or agencies. For example, in the case of a consumer purchasing an insurance policy, it is made clear during that process that information will be collected by an insurer as necessary to issue and manage the policy, and to process claims.
- Consideration of what should happen if the personal information is sourced indirectly from a commercial or government source which is not a publicly available source. For example, use of credit agency or ownership verification information. It will be important to consider in advance how this can be practically managed by agencies and in a manner that does not jeopardise the other IPP in the Privacy Act.
- Ensuring that any changes allow for a complex and diverse range of business models.
- Allowing an appropriate timeframe for entities to implement changes, and avoiding legislative changes having any retrospective impacts.

Question 2.
What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?
ICNZ sees the following potential advantages for individuals and agencies in broadening the notifications:

- Broadening the notification requirements in the way identified by MOJ, could be beneficial for individuals in circumstances where their information has been collected when they would not have expected or previously consented to this occurring.
- Consumers would also be better empowered to be proactive custodians of their own data and have greater transparency around use of personal information.
- There would be an obvious benefit for New Zealand businesses if changing the law means retaining our adequacy status in the EU.

There are also serious disadvantages to be considered before any law change. These include:

- Notification fatigue: depending on how the changes are worded, they could result in individuals becoming overloaded with notifications about the disclosure of their personal information.
- Further notification fatigue would occur if both parties had to notify an individual and on every occasion of indirect collection (as opposed to one general notification about collection, as is used by insurers at present). We would not be supportive of a law change which requires notification by both the collecting and disclosing agencies.
- Notification fatigue would be exacerbated given the number of entities insurers interact with on a daily basis to process insurance policies and claims.
- Significantly updating the existing principles could cause confusion, when at present, we believe they work well. We also note, there are existing mandatory breach notification requirements where individuals must be informed of certain issues relating to breaches of the Privacy Act irrespective of whether they had been informed of collection or disclosure at the time it is occurring.
- Compliance with the law change could potentially slow down agencies' processes – if agencies need to dedicate a larger portion of time to notifying individuals about indirect information collection, they may not then be able to service their needs in other ways. There would also be an education component to the change – consumers would need to be educated about the change and what it means before they would understand why agencies were requiring additional consents or other actions from them. For example, failure to inform consumers of any changes could lead to frustrations about additional time delays when processing customer requests.
- In an insurance setting, changing the law could lead to increased compliance costs with little benefit to insureds (i.e. they will be told what they already know, that the broker has disclosed their personal information to insurers for the purposes of placing their insurance or processing a claim or an insurer has provided their information to a supplier),[1] costly change to business practices, subsequent increased costs for consumers, and difficulties of notifying individuals with whom an agency does not have direct contact.
- Broadening the notification requirement may give individuals greater awareness of their privacy rights without any real way to exercise those rights (i.e., correction, deletion, or supply of information) or to fully understand what information is being collected/disclosed via indirect means.
- Compliance with this law may risk infringing on that under the Unsolicited Electronic Messages Act 2007 if it is the collecting agency that is responsible for notification. It is

[1] There are a number of commonly used distribution channels used by insurers in Aotearoa New Zealand, including direct channels (where a consumer purchases a policy directly from an insurer) and intermediated channels (where a consumer uses a broker or other intermediary to place their insurance). When a broker is used, they act as the agent for the insured and will pass information onto the insurer for underwriting purposes.

possible that, depending on the type of information, they do not have an existing relationship with the individual and the individual has therefore not consented to receiving communication from the collecting agency.

- Agencies would likely have to work through the detail of numerous different "indirectly sourced" scenarios to determine whether notification is required, and how and when it should take place. This process, along with the necessary system changes already noted above, will likely be time consuming and resource intensive. A long lead time for implementation will be required.

Question 3.
What form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate.
It is not possible to provide detailed comments on proposed changes, or identify a preferred option, without further detail of how any proposed changes would be designed. However, we set out some initial comments on each of the proposals in the table below.

Option 1 (amendment to IPP 3)	• IPP 3 feels like a natural fit around notification of collection of personal information from individuals. • Agencies should easily be able to incorporate any notification requirements within existing privacy statements/notices/processes, if a blanket approach is deemed acceptable and the indirect collection notification requirement applies only where the indirect collection was not contemplated when the information was originally obtained (although related to the purposes of the initial collection). • Broadening the existing IPP 3 would considerably reduce the cost associated with updating artefacts for businesses and thus make compliance more viable.
Option 2 (amendment to IPP 2 or IPP 11)	• Amending IPP 11 to require notification of disclosure would be a plausible option for change. However, the cost and effort of practically applying this for agencies would be larger and more disruptive than the other options, unless a blanket notification approach is permitted to cover the fact disclosures occur (indirectly to third parties) and customers consent to this as a whole. • It seems practical for the central obligation to notify if data is collected indirectly to sit with the disclosing agency. The disclosing agency should already have mechanisms in place to notify an individual if required, such as for a breach, and they have the immediate control and accountability regarding whether the indirect provision of the information should even take place. • It is otherwise not possible to comment on proposed amendments to IPP 2 without more detail as to how the exception will be narrowed.
Option 3 (new IPP)	• While all options would necessitate change, option 3 in particular would necessitate the most internal change and resource to reflect an entirely new principle (i.e., communications, training, updating documentation and privacy compliance processes, etc.). • However, this option could also be specifically written to cater for requirements on collecting information from external sources, by increasing requirements to declare upfront to a customer on what the details will be used for or by enhancing the current privacy statements on companies' websites.

In our view, whichever proposal is advanced, it must ensure that the existing collection and disclosure principles remain intact so far as possible. Specifically, the exceptions (such as those listed in IPP 2(2)(a)-(g) and IPP 3(2)-(4) which enable collection or disclosure to occur must continue to be available for agencies to rely on. There is no clear benefit for individuals that would be achieved by removing many of these exceptions which are regularly relied on by agencies to operate. For example, under IPP 3(4)(a), if there is no prejudice to the interests of an individual, then arguably, there would be no benefit in notifying them of collection of the information.

Question 4.
If you are a New Zealand business, are there any practical implementation issues you can identify in complying with the proposed changes?
ICNZ has identified a number of issues that would arise in having to comply with the proposed changes. Firstly, a change to ensure all individuals are aware of exactly who their information is shared with comes with significant downsides for both the individual and insurer. Insurers regularly collect information from other parties (such as where a policy is in joint names) and regularly collect information at claim time from other parties (such as from other drivers in motor vehicle claims, and from suppliers, repairs, etc). We believe that the compliance and time involved to comply with the requirements would outweigh any benefits and negatively impact the overall customer experience if the proposed changes are poorly designed.

With regards to intermediated and brokered insurance business, in most cases the insurer will not have direct contact with many of their customers, and in fact can be contractually restricted from making contact with their customers, with all contact instead going through the broker, distributor, or other intermediaries. Based on this, it is unclear how any of the proposed changes would operate other than a provision for the intermediated or broker party to notify the individual that their personal information will be provided to the insurer and why.

Implementing changes to the legislation will require changes to computer systems, websites and claim forms, and training material, etc. This would come at a cost, and note that this has already been done recently, following the passage of the Privacy Act 2020. Additionally, due to some processes and operations being automated/system generated, implementation would likely require significant time and effort. Insurers would also have to install processes to identify, manage and track third party sources of indirect collection to ensure a clear picture is provided and then use that information to determine how and when notification would be carried out (if that level of detail is not prescribed by legislation). We would therefore urge MOJ to carefully consider each option as well as the inclusion of a reasonable grace period to minimise impacts on business operations whilst implementing any new requirements, when finalising the proposals.

ICNZ has identified a number of implementation issues specifically arising in the insurance context, but which may also affect other agencies. Firstly, should it be necessary for insurers to contact non-customers/third parties individually to provide them notice (for example, in relation to information collected following a motor vehicle collision), then a range of practical challenges could arise. These include:

- An inability to issue notice to the person as their current contact details are not known. This then raises the question of how long the notice must be put on hold and what happens to the information that has been collected.
- What happens in those instances where a non-delivery notice is received.

- The content of the notices. For example, whether the notification itself should contain the information required under the law, or whether it is simply intended as an explanation of what it is.
- Whether it is intended that there will be a standard format or minimum standards for the notice.
- For tip-offs (for example, relating to fraud), whether notification risks identifying the informant, and if so, how notification should be provided to prevent identification of an information, which might dissuade further tip-offs being made in future.

Secondly, in terms of how notification is made, if notification were to be made via email, as an example, we foresee a number of issues, including:

- Notifications potentially being caught by spam email filters, particularly if notices are sent out in bulk lots.
- The potential that notification could create a privacy breach in some situations. For example, if notification is sent to a work email address that the individual's employer is entitled to access.
- Notifications with large file sizes, although rare, could be too large to send via the email system.
- Not everyone has access to email and some digitally vulnerable people or people with lower technological competency may seek assistance from other people, who may then receive the notification, rather than the individual it should be sent to, creating a breach.

The extent of implementation issues will also depend on the position the MOJ reaches on the use of general, as opposed to specific, notification to consumers. Insurers already include privacy statements that an insured must agree to, informing them that the insurer will collect information from other parties as part of their processes. If the use of statements such as these will satisfy changes to the legislation, then implementation would not be so onerous. However, if, despite the existence of these statements, insurers must also notify an insured each time they collect information from a different third party, this would significantly complicate implementation. From discussion with MOJ, we understand that there has not yet been a view reached on this point about use of general privacy statements. It will be important for MOJ to state their position on general privacy statements in order for submitters to provide the most informed feedback on the proposed changes to the law going forward. We note that for the purposes of GDPR privacy notices and privacy statements are essentially interchangeable and therefore, we would hope that MOJ would consider that transparency within a privacy statement would satisfy any notification requirements.

Finally, we question what MOJ's expectations would be in relation to personal information that has already been collected via a third party prior to any legislation change. We presume that there would not be any requirement to retrospectively communicate that that information had been collected (should Option 2 be the one that is advanced).

Question 5.
Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?
ICNZ has identified two further risks specific to the insurance industry that we raise for the MOJ's consideration. Firstly, introducing a new privacy principle to deal with indirect collection of personal information would create complexities for the insurance industry (and likely many others) where

information may be collected either directly or indirectly depending on how the individual chooses to interact with an agency. In practice this will create practical difficulties leading to excessive compliance/administrative obligations to manage two different sets of requirements.

Secondly, any change to the legislation would require significant changes to the dominant business model in the insurance industry, which will be costly. These costs would inevitably be pushed down to consumers by way of increased premiums at a time when there is already significant regulatory review underway that will mean the insurance industry must review policies and processes[2] (and, as noted in response to question four, very soon after the review that was required in response to the 2020 Privacy Act changes). Inflation and global economic pressures also mean that costs are rising across all areas of an insurer's business which is then reflected in the premiums being charged to consumers. We do not believe that the options in the Engagement Document propose positive changes for individuals or insurers.

Question 6.
Should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?
ICNZ believes that any proposed changes should apply to personal information from both individuals overseas and in Aotearoa New Zealand as this would minimise additional complexities and the potential creation of differing compliance approaches across a customer base. In practice it would be difficult for many agencies to identify which individuals it interacts with may be based overseas at a particular time, depending on how often they interact and how regularly they update their details (such as their residential address) with the agency. This is likely to create situations where agencies inadvertently become non-compliant, a situation that would be difficult for agencies to rectify until after a compliance breach has already occurred.

In relation to the potential cost of implementing any change, it should be noted that many insurers will already indirectly collect personal information relating to individuals both here and overseas, (for example, because an overseas resident insures a house they own in Aotearoa New Zealand with an insurer domiciled locally). Therefore, limiting the application of the proposed changes to personal information collected from individuals in Aotearoa New Zealand would not address the significant increase in compliance costs and impact on standard business practices and models in the insurance industry.

Question 7.
Is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback
We believe that if these proposals are advanced, in whichever form, the legislation should also be amended to provide an exception to an indirect notification requirement when the individual concerned already has the information that the agency is required to provide under the Privacy Act (i.e. the information required under IPP 3).

[2] For example, the Financial Markets (Conduct of Institutions) Amendment Act 2022, Natural Hazards Insurance Bill 2022 and yet-to-be-introduced Insurance Contracts Bill will require time consuming and costly reviews of products, systems and processes for insurers. ICNZ has previously advocated for the commencement periods of these pieces of legislation to either align, or be separated significantly in time so that the implementation periods do not overlap.

Finally, while ICNZ supports privacy transparency and providing individuals with clear and concise information about what agencies do with individuals' personal information, we again stress that any law change in this area must be afforded careful consideration to ensure that the privacy benefits it provides are not outweighed by the creation of costly and onerous compliance obligations.

Conclusion

Thank you again for the opportunity to submit on this matter. If you have any questions about our feedback, please contact our General Counsel by emailing s9(2)(a)

Yours sincerely,

s9(2)(a)

s9(2)(a)

Tim Grafton
Chief Executive

Jane Brown
General Counsel

Inland Revenue
Te Tari Taake

Inland Revenue submission in response to the Ministry of Justice **consultation on the broadening of the Privacy Act's notification** obligations

Inland Revenue understands the proposal to regulate indirect collection of personal information relates to New Zealand retaining its EU adequacy status that was granted in 2012.

Since that time the General Data Protection Regulations (GDPR) have come into force. To retain adequacy New Zealand must be able to meet European legal standards of data protection to continue facilitating the free flow of personal data from EU countries to New Zealand for processing. New Zealand law provides that individuals need to be informed when information is collected directly, but it does not refer to indirect collection when the individual does not know their information has been shared.

Article 14 of GDPR prescribes the information that is to be provided where personal data has not been obtained from the data subject. It is our understanding the proposal seeks to replicate this provision into New Zealand law.

General comment

Inland Revenue agrees that any processing of personal information should be lawful, fair, and transparent. We currently inform individuals on forms they complete and via our website what information we collect and why. We also include summaries of our information sharing agreements on our website so are transparent in what information is gathered and who it is shared with.

For the effective and efficient administration of the tax system, Inland Revenue collects information from third parties on a regular basis regarding taxpayers' income and tax deducted. For example, information is collected from employers, financial institutions, and Māori authorities. Notifying taxpayers each time information is collected will impose significant administration costs on Inland Revenue and compliance costs on individuals. The extent of these costs depends on the details of the notification proposal, which have not been outlined in the consultation document.

The broadening of notifications of data that is received and shared in principle is not problematic, if it is implemented generically through an understandable online declaration from the requesting agency. For example, new dataset arrives for property data. IR publishes on its website that it holds a dataset with data x y z, from which individuals can interpret for themselves that data about their property holdings will be amongst that data.

However, we do have concerns about how the proposal will work in practice if we are expected to notify every individual every time IR receives their data and the cost of complying. If this is the expectation, then IR proposes that there must be some exclusions to this general rule.

Our current data sharing administrative processes and authorising environments are already complex. This would add another layer to that and could adversely put more

obstacles in the way and reduce our collective ability to deliver improvements in services at pace and at scale.

1. What factors do you think are most important when considering changes to indirect collection of personal information?

IR is one of the largest data consumers and providers in the public sector. This means that operationally, depending on the extent of change, our compliance costs would increase through a large-scale change requiring us to notify individuals. On this basis, we consider these factors to be some of the most important:

a) *What is the information collection base on which the notification obligations are imposed?* Does it apply to all collections of information from third parties (legislated and non-legislated) or is it just non-legislated sharing or consented sharing? The example provided in the consultation document is about non-legislated/consented sharing, which can be distinguished from government agencies collection functions, which are generally authorised by legislation or legislatively.

   Inland Revenue's collection of information is authorised by legislation (eg the Tax Administration Act 1994) and is collected to undertake our government authorised functions and duties. Legislated collection is more transparent to individuals and may not be a problem to the same extent as non-legislated collection.

   Third party collection of information by government agencies is usually authorised by legislation, reducing the ability to change how information is collected in response to this proposal. Private sector agencies are more easily able to change the way information is collected if the costs of notification outweigh the benefits from third party collection.

b) *When is the collection triggered?* Is it when the information is first collected from a third party or each time the information is collected? Recording each collection occurrence for each taxpayer would be a significant cost for Inland Revenue and other agencies both to implement and operate on an ongoing basis.

   For example, Inland Revenue could receive information from third parties 34 times a year with regards to a taxpayer. Namely, 26 fortnightly pays, two interest payments from a bank, two dividend payments from two share registries, one KiwiSaver notice, and one information request from another agency (for example, border movement or contact detail change). This number increases if a taxpayer has more complex tax affairs, is in business, or is receiving social assistance including Working for Families tax credits, a student loan or child support.

c) *Obligations on receiving agencies* – IR receives information under international treaties and from the OECD on an 'in confidence' basis. There are restrictions on how we can use that information and who we can share it with. We currently could not inform an individual that we have received their information without breaching OECD confidentiality.

d) *Frequency of notification* - how often does an agency have to notify an individual? Each time a collection is made (34 times a year in the above example), or once a year that information was collected 34 times. The impact on

the proposal varies greatly depending on frequency of notification. Notification fatigue for individuals is also a very real thing as noted in the consultation paper.

e) *Scale and frequency of notifications may not align to customer's desired outcomes from cross-agency sharing*. Customers have told Inland Revenue in multiple research papers spanning many years that we need to minimise the burden of compliance, and the need to interact with multiple agencies. Adding personal notifications to agency's interactions, which ultimately seek to deliver improved public services, would be counter-productive to achieving this. The scale of products and services, customer base, and direct communications would increase complexity, and reduce the ability to operate at pace. This is specifically required for the introduction of new government policies (eg COVID payments).

f) *Method of notification* - to reduce administration and compliance costs of the proposal, the notification process would need to be electronic. But how do we inform those individuals who do not use online services (such as Inland Revenue's myIR secure online service), or people we do not have email or mobile contact details for?

g) *Time limits* - will there be a time limit to when notification must take place? The GDPR states within a reasonable period of having obtained the data and, at the latest, within one month.

h) *Ability to notify* – there will be circumstances where we do not hold accurate contact information or do not know how to contact the individuals directly. How will these circumstances be managed?

i) *Keep the intent and any operational management guidelines simple*. Online solutions for publishing the purpose and use of data, combined with generic declarations about privacy management activities, can more easily be incorporated for third party data collections and disclosures.

2. What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?

Advantages:

a) *Increased notification requirement will provide individuals improved access to, and visibility of how their data will be used so increases transparency*.

A review of qualitative and quantitative research on information sharing was conducted by Inland Revenue in 2018. It found taxpayers are already generally aware that Inland Revenue collects information from third parties for the effective administration of the tax system.

The end-of-year tax assessment process illustrates this collection and its use through the pre-population of taxpayer information on the taxpayer's annual tax return forms. Also, the Inland Revenue website outlines who we share information with, and legislation outlines our ability to collect information and who we collect information from (for example employers and banks who pay interest).

b) *Direct notification makes it easier for individuals to understand any adverse action, consequences, and compliance obligations.*

This enables informed choices about whether to comply or not. This is especially so with consented sharing where individuals may not be aware what their information is being used for.

c) *Agencies may note an increase in individual's compliance with their ta and social policy responsibilities.*

Research revealed there is a higher prospect of reduced compliance, as a result of misinformation about information sharing. People hearing about information sharing in an incomplete and unstructured way, creates misconceptions, and worry that information shared is not the kind that supports public good.

Disadvantages

a) *Direct notification could become a burden* for individuals who become fatigued by agencies seeking to meet requirements. This may end up creating apathy with people switching off about how their data is being used.

b) *Scale of collection* - the proposal does not address the scale of interactions that government has with individuals and how this is to be managed to reduce both administration and compliance costs.

The collection of information is at scale to enable the effective administration of the tax system.

For example, every time an employee commences employment or changes their tax code, their employer collects information from the employee and forwards it onto Inland Revenue. This information is used by the employer to calculate the amount of PAYE tax to deduct f om the employee's wages and for Inland Revenue to ensure that the taxpayer is paying the correct amount of tax. Under the proposal there could be an expectation that Inland Revenue would need to inform the employee that their employer has shared this information even though the individual is currently informed of this on the form they must complete. There seems no advantage to the individual being told twice.

c) *The extent of notification required* depending on the circumstances of the share. For example, publicly notifying that an organisation is sharing certain types of data for a particular purpose should be sufficient. So long as that notification is easy to access, understand, and is truly transparent.

Inland Revenue collects a lot of information to administer the tax system and social policy products. As it stands, the proposal would cover all of the information we collect from third parties including property data, government information shares, suspicious activity reports and when Inland Revenue uses its statutory information gathering power under the Tax Administration Act. This allows Inland Revenue to collect external datasets as well as information on specific taxpayers from banks or utility companies. If we were required to notify in each instance, it is likely Inland Revenue's compliance activity would be severely affected.

d) *Cost of complying with notification requirements*. Being able to operate at scale and pace would be affected through notification requirements. Notification may impact Inland Revenue's ability to carry out functions, and an increase in potential customer contacts resulting from individuals could impact frontline delivery services, which would impact current service levels to our customers.

3. What form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate.

An amendment to IPP 3 would be preferable. This is the IPP that relates to notification requirements so it would be logical to broaden its scope to apply when an agency collects personal information indirectly from other sources. It would also be simpler for agencies to implement.

Amending IPP 2 would not be functional as IPP2(2) may still be appropriate to the collection. For instance, compliance with IPP 2 may not be easonably practicable in the circumstances so indirect collection is acceptable. Adding notification requirements into IPP2 could cause confusion about the purpose of the principle.

The proposal is already covered under IPP 11 as that allows an agency to disclose information to any person if the agency believes, on reasonable grounds, that disclosure is to the individual concerned. This is not a requirement, but making notification a requirement in IPP 11 will be inconsistent with the discretionary nature of the principle.

4. If you are a New Zealand business, are there any practical implementation issues you can identify in complying with the proposed changes?

Addressed under question 2.

Although a general observation is the larger the business, the more difficult compliance becomes. From a service perspective, we know that New Zealand businesses sometimes struggle to comply with regulato y responsibilities eg tax, employment, health and safety, environmental, etc. This may become another cost for Small Medium Enterprise businesses to absorb.

5. Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?

Inland Revenue would strongly support providing exceptions to the indirect notification requirement to mitigate compliance costs and individuals being over-notified.

Inland Revenue also has obligations to protect the integrity of the tax system. Notifying individuals that we have collected information, let alone providing specific details, may create a risk to the integrity of the tax system through individuals having insight into compliance activities.

Like Article 14 of the GDPR, there must be circumstances in which the requirement to notify will not apply. For instance, where:

- the individual concerned already has the information; or
- it has been received under an information sharing agreement and information about that agreement is publicly available; or

- obtaining the information or disclosure of it is a legal obligation; or
- notifying would have a negative effect on law enforcement duties; or
- information is received solely for statistical or research purposes; or
- provision of the information would involve a disproportionate effort; or
- the personal data must remain confidential due to a statutory obligation of secrecy.

If New Zealand wants to align with the GDPR to retain adequacy, the proposal should also consider GDPR's Recital 31. It provides that public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of thei official mission (including tax authorities) don't need to comply with the GDPR when carrying out their legally-assigned tasks.

6. Should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?

Applying the notification obligations only to individuals overseas would keep ongoing costs to a minimum but there would still be development costs. The benefits from this would reduce the benefits from the notification proposal. However, having separate obligations, depending on an individuals' residency status, would require effort to identify those individuals affected.

Having the same notification requirements applying to all individuals would simplify the notification process.

7. Is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback.

a) The proposal does not take into account the vast amount of legitimate information sharing done by government agencies. This sharing is transparent as it is mostly permitted by law and government agencies inform people that information is shared.

   Overall, we think careful consideration is required, with limitations on the proposal as supporting the operational side would prove to be a large cost overhead with potentially nominal (in our view) additional benefit.

b) If the expectation is that individuals should be informed every time their personal information is shared, this may not be possible and will create huge administrative burdens on government agencies, not to mention the fatigue experienced by individuals. For instance, under the Customs/IR Student Loans Interest Match (an information share in force since 2007), Customs provides Inland Revenue with border movements for all student loan borrowers to assist in correctly assessing entitlement to an interest-free student loan. Last year this was more than 50,000 individuals. Under the proposal, Inland Revenue would need to inform those 50,000 that Customs had provided their information even though individuals can find notice of this on Inland Revenue's website and in myIR.

c) Inland Revenue receives a lot of information anonymously and may not act on that information. We cannot be expected to inform someone that an anonymous

allegation has been made about them unless we choose to take action. This must be excluded from the notification requirement to preserve the integrity of the tax system.

d) Inland Revenue also has confidentiality obligations. While the Tax Administration Act permits Inland Revenue to give information to the person from whom, or on behalf of whom, or in relation to whom such document or information is held or was obtained, this is subject to the Commissioner also being satisfied that such information is readily available in the department; and considers it reasonable and practicable to give that information.

   Any notification requirement in the Privacy Act will be subject to this obligation.

e) There is no comment as to how this notification proposal interacts with the digital identity trust framework and whether the framework could be used by agencies to fulfil the notification requirements under this proposal. Notifications from multiple businesses/agencies could be sent to a digital wallet for the individual to view, all in one place. Again, this would need to be done in such a way as not to over-communicate to the point that individuals cease to engage with the process.

f) We consider that the work towards digital identity may be helpful in solving the transparency question about what agencies know and share. This work feels like it has commonality with that but from a different lens.

28 September 2022

Carter, Adam

From: s9(2)(a)
Sent: Monday, 5 September 2022 10:05 am
To: Privacy Feedback
Subject: Feedback on your Privacy engagement document

That's for the opportunity to provide feedback on this issue. I work in IT, and have a strong personal focus on privacy.

1. What factors do you think are most important when considering changes to indirect collection of personal information?

I think that the international nature of data sharing, and the gargantuan scale of collection and processing requires an international approach. I see that there's little benefit in creating a set of rules that govern NZ, when data is collected from overseas websites, or passed/sold to overseas aggregators for whom our laws are immaterial. So creating a regulatory framework which is effective is more important than creating one which is principled. Alignment with (probably) the GDPR may be the most effective thing we can do

3. What form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate.

Pick a strong framework from a different administration and align with it. This will give a good chance that overseas entities will actually follow our regulations

regards

s9(2)(a)

Observations on the possible changes to notification rules under the Privacy Act 2020 (DRAFT)

These observations are made from a business standpoint and relate more specifically to the effect the proposed changes would have on the collection and management of personal information for marketing purposes

The document presented by the Justice department https://www.justice.govt.nz/justice-sector-policy/key-initiatives/broadening-the-privacy-acts-notification-rules/ asks for feedback on 7 questions:

Q1. What factors do you think are most important when considering changes to indirect collection of personal information

The most important factor must surely be the benefit derived by the individuals concerned. Where is the evidence that the New Zealand public are seeking such notifications? In the absence of any qualitative research, we could be drawn to the conclusion that the proposed changes are designed to meet International adequacy standards rather than benefit individual New Zealanders. The discussion document itself identifies the possibility that any perceived benefit may be offset by individuals becoming overwhelmed through 'information overload'.

Other factors to be considered include the additional technology and communication costs which will be incurred by organisations transmitting or receiving personal information data. These costs will inevitably be passed on through increased prices for goods and services.

Q2. What are the advantages or benefits of broadening the notification requirements for both individuals and agencies? What might the disadvantages be?

Clearly individuals would be more informed about who holds their personal information and NZ's Privacy legislation would move towards international 'adequacy' standards, particularly those of the EU.

The major disadvantage would be the increased cost of both staff and technology to manage notifications systems. We know from organisations which have had to adapt to GDPR requirements that complex data

management systems are required and that even large organisations have found it difficult and expensive to comply. Smaller organisations (and NZ is a nation of small businesses) will be particularly affected.

Q3. What form do you think the proposed changes to notification rules under the Privacy Act should take?

There is certainly a case for organisations holding, or receiving, personal information about overseas individuals being required to notify those people. Many of these organisations may already be equipped to do so because of the requirements of GDPR.

If notification of collection is also mandated for New Zealand residents, then it makes sense to amend PP2, PP3 and PP11 of the Privacy Act.

However, there is a logical case for information which is publicly available to be excluded from notification. This is especially appropriate for areas like property ownership the details of which are publicly available from LINZ and local bodies.

Similarly, if contact details are publicly available (e.g. on a website) there is already legislation consenting electronic or digital contact if the message is relevant to the recipient. (Unsolicited Electronic Messages Act 2007)

The discussion document states that the use of codes of practice has been explored. We are interested to know how it has been explored and what are the reasons for rejecting this method? There are already Codes of Practice operating successfully under the jurisdiction of the Privacy Commission.

Q4. If you are a New Zealand business or agency, are there any practical implementation issues you can identify in complying with the proposed changes?

In order to comment on this question, it is important to think about the number of different ways in which personal information may be collected or shared.

- When looking at the example of collection of contact details entered by an individual on a website or response form. We note the discussion document suggests that these details may be indirectly collected by an advertising agency. This is only possible if the individual has been informed of this via a privacy statement on the website or response form. Therefore, it is not an indirect collection. In any event Advertising Agents do not normally collect personal information, we believe the discussion document is confusing advertising agents with Data Service agencies or Marketing agencies who are voluntarily governed by codes and best practise guidelines.
- Data Service agencies and List Brokers collect personal information to rent to businesses and charities for use in outbound marketing and fundraising. Their collection methods are already governed by the Privacy Act 2020. This means that the individuals have already been made aware that their contact details may be shared with marketing organisations. Lists of this type may contain the contact details of hundreds of thousands of individuals. We should consider whether the business sending and receiving this information must notify all the individuals on the list every time the information is shared. This is especially the case when the receiving organisation is only renting the information for one campaign and is not permanently storing the details.
- When we consider personal information, such as property ownership, which is publicly available through LINZ or local authorities, is it useful for every real estate agent, valuer, banker, lender, builder, electrician etc. etc. to notify the property owner every time they access the information?
- Many New Zea and businesses do not manage their own data. There are a number of specialist agencies who provide data management services for customer and client information. These agencies simply hold data on behalf of the data owner. Would the proposed changes require them to notify individuals of information transfer?

3.

Q5. Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?

In our response to Q4, we referred to Data Service agencies and List brokers who rent or sell data collected from various (legal) sources.

The suggested amendment to IPP11 would require those organisations to notify the individuals on those data lists every time their information was disclosed to another agency. Such disclosures could amount to several notifications a week which would surely create notification fatigue for the individuals.

A particular example of this would be the personal information of individuals who have registered for the Name Suppression Service on the NZ Marketing Association website https://marketing.org.nz/do_not-call-do-not-mail. This service is designed to prevent unsolicited marketing to individuals who do not wish to receive such communications via Mail or 'phone. Nearly 200,000 individuals have registered for this service, their details are accessed by subscribing agencies to remove them from outbound marketing campaigns. Notification to these individuals would defeat the objective of this valuable consumer service.

Referring to the mitigation examples in the Justice department document, we are unsure about what circumstances could be in place for an agency to believe they might only be required to take *'any steps that are, in the circumstances, reasonable to notify individuals about the collection of information'*.

We agree that notification is unnecessary when the organisation already holds personal information on an individual and the person concerned is aware of that fact. There is also a strong case for notification to be exempted where the individual has been informed at the point of collection that their details will/may be shared with other organisations.

Q6. Should the proposed changes only apply to personal information collected indirectly from individuals overseas?

(We assume this should read 'about individuals' rather than 'from individuals')

There is a logical case for notification of third party collection or transfer of personal data about overseas individuals, particularly if they are resident in countries which already require notification in their own legislation.

However, the most compelling case for notification for New Zealand citizens appears to be to align the Privacy Act with international regulations, particularly GDPR. Businesses would certainly want to see strong evidence that notification is required for organisations operating exclusively in the domestic market.

Q7. Is there any other feedback you would like to provide?

In order to avoid unintended consequences, we recommend further interaction with the data service sector to more clearly understand how they operate.

Keith Norris,

Compliance Consultant.

New Zealand Marketing Association, 69, St Georges Bay Rd, Parnell, Auckland.

PO Box137266. Parnell Auckland 1151.

s9(2)(a)

14/9/22

MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HIKINA WHAKATUTUKI

DATE	30 September 2022
TO	The Ministry of Justice
PREPARED BY	Christian Hardy, Advisor - Privacy
APPROVED BY	Tania Turfrey, Manager Legal Services
SUBJECT	Submission in response to the Ministry of Justice's consultation on possible changes to notification rules under the Privacy Act 2020

BACKGROUND

1. This is a submission by the Ministry of Business, Innovation and Employment ("MBIE") in response to the consultation document released by the Ministry of Justice, entitled 'Possible changes to notification rules under the Privacy Act 2020'. The consultation document proposes potential changes to broaden current notification requirements under the Privacy Act 2020 ("the Privacy Act") so that individuals would be informed when their personal information is collected indirectly.
2. The Ministry of Justice has proposed three potential changes. Option 1 is an amendment to Privacy Principle 3 so that it also applies to personal information collected indirectly. Option 2 is an amendment to one of the other privacy principles, for example Privacy Principle 2 in order to narrow exceptions that allow agencies not to collect information directly from the individual concerned; or an amendment to IPP 11 to require a disclosing agency to notify the individual concerned that their information has been disclosed to a third party. Option 3 is the introduction of a new sepa ate privacy principle dealing specifically with notification of indirect collection.
3. This submission is made following a request for feedback by MBIE's Privacy Team from a number of business groups across MBIE. Their feedback has been collated and incorporated by the Privacy Team into this submission.

FEEDBACK

What factors do you think are most important when considering changes to indirect collection of personal information?

4. As part of its day-to-day operations, MBIE collects an extensive amount of personal information from various sources. When considering changes to indirect collection of personal information, MBIE must take into account how such changes will impact these operations, e.g., increased workload or increased compliance costs.
5. Another factor MBIE believes to be important is what effect the proposed changes will have on its customers, both within New Zealand and overseas. MBIE takes seriously its role as steward of the personal information it has been entrusted with, and believes it is important to consider whether any proposed changes would be harmful (such as the potential confusion and uncertainty caused by a change in services provided) and/or beneficial (such as the strengthening of people's privacy rights) to its customers.

What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?

6. The Ministry of Justice has stated that the purpose of the proposed changes is to ensure New Zealand keeps up-to-date with privacy laws and best practices in overseas jurisdictions. As an agency whose focus is on ensuring a strong New Zealand economy MBIE appreciates the need for New Zealand to be able to compete in the global marketplace and acknowledges the benefit to trade the proposed changes would bring.
7. MBIE also acknowledges the increased transparency that the proposed changes would bring, better enabling individuals to make more informed privacy choices, hold agencies to account for their privacy practices and exercise their privacy rights under the Privacy Act.
8. In terms of disadvantages, the Ministry of Justice has identified two potential areas of risk that broadening the notification requirements may cause. The first identified risk is notification fatigue and he second is increased compliance costs. MBIE has also identified these risks. In particular:
9. Some of MBIE's business units deal with households in highly stressed and vulnerable situations states that increased notification could cause greater confusion to customers regarding where their information is going.

10. Many of MBIE's business units currently use privacy statements to notify how it handles personal information collected, and these could be further expanded to include information collected elsewhere, for example by an individual's agent, but that anything additional to this would be a further cost.

What form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate.

11. As stated under paragraph 2 above, the Ministry of Justice has proposed three options on what form the proposed changes might take. MBIE is of the opinion that changing the exemptions to how collection of personal information is notified would create unnecessary confusion and uncertainty and so does not recommend the adoption of option 2. Some MBIE business units have advised that being required to collect personal information from individuals directly without exceptions, such as for parties in dispute resolution, would create additional administrative burden.
12. MBIE is also of the opinion that introducing a new separate privacy principle specifically for indirect collection is unnecessary and would cause confusion for those already familiar with the current 13 privacy principles. MBIE therefore does not recommend the adoption of option 3.
13. MBIE recommends option 1 as the least burdensome and most straightforward to implement. It proposes an amendment to the Privacy Act's Privacy Principle 3 not too dissimilar to Australia's Privacy Principle 5 which does not differentiate between direct and indirect collection.

If you are a New Zealand business, are there any practical implementation issues you can identify in complying with the proposed changes?

14. Since the exact shape or extent the proposed changes will take has yet to be determined it is difficult for MBIE to say what practical implementations it is likely to face. Some business groups have advised that the level of difficulty in notifying will depend on what the actual requirement for notification looks like, with general statements in a privacy policy and/or transparency statements and/or notifications on a website being seen as much more manageable than, for example, notifying every time information is indirectly collected.

15. In other jurisdictions, notifying of indirect collection is done in numerous ways, including by email, post or via a privacy statement on a website. The means of communication will therefo e likely depend on what is reasonable in the given circumstance, similar to the current requirement in New Zealand for when information is collected directly. It is therefore expected that expanding requirements to include notification for indirect collection would simply build upon current processes already in place for direct collection.
16. More guidance will be required on how this new notification regime is to be implemented, such as if notification has to occur where the individual is not identifiable, or the party who provided the information cannot be identified, or if information collected indirectly regarding children means also collecting information about the parents/guardians in order to notify them.

Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?

17. An additional concern is that the proposed changes will lead to increased administrative burden. This can range from potentially having to re-negotiate data sharing agreements, the need to notify in many different languages, from the need to collect additional information than usual just to be able to notify, or from call centres such as the Immigration Contact Centre ('ICC') receiving an increase number of calls from customers about notifications, which they are not resourced or trained to handle.
18. There is also concern as to how proposed changes will interact with the many intelligence and compliance functions found within MBIE, with the concern being that the requirement to notify could compromise certain investigations.
19. Specific concerns noted by MBIE teams are as follows:
    - In order to notify it might require the collection of additional contact information, which could lead to 'over collection'.
    - The ICC suggests that an increase in notifications being sent could result in a higher number of privacy breaches.
    - The Dispute Resolution team advises that personal information collected, including about other parties, is only for mediation purposes and can only shared by the mediator with the express consent of the person providing it, meaning it would be difficult to adhere to a requirement to notify other parties when information is collected about them.

- The increase in notifications may present a new opportunity for malicious phishing and spam.
- Where MBIE procures datasets containing personal information, for example, for research and/or development of statistics.

Should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?

20. MBIE is concerned that if the proposed changes were to only apply to information collected from individuals overseas this would create a discrepancy as individuals overseas would be seen to have more rights to privacy that individuals in New Zealand. MBIE therefore recommends that the proposed changes apply to all individuals equally.
21. MBIE suggests that by expanding Privacy Principle 3 to include the requirement for notification indirect collection as well as for direct collection all individuals are given the same protection under the law, whether they are in New Zealand or based overseas.

Is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback

22. MBIE has a number of roles which are based in legislation, and these Acts of Parliament sometimes override the Privacy Act. For example, the Insolvency & Trustee Service advises that all the personal information that it collects indirectly is done pursuant to the Insolvency Act 2006 and the Companies Act 1993. Similarly, the Dispute Resolution team provides mediation services as set out in the Employment Relations Act 2000. MBIE believes that any proposed changes to the Privacy Act with regards to notification of indirect collection should not impact how these other legislations operate.
23. There is also uncertainty as how the proposed changes will be implemented. MBIE would therefore be looking to the Office of the Privacy Commissioner as regulator for guidance on how any proposed changes to the Privacy Act are to best be implemented.
24. Concerns have been raised regarding whether collecting personal information from a third party, who has authority to act on the behalf of an individual, would constitute as indirect collection. It is MBIE's suggestion that any such collection of personal information from agents on behalf of another should be considered as having been collected from the person directly.

25. MBIE is also keen to ensure that a te ao Māori view is reflected in any consultation done on the proposed changes to the Privacy Act.

CONCLUSION

26. Of the three options proposed, MBIE supports an amendment to broaden Privacy Principle 3. This option would require the least administrative burden, as it would simply expand the current requirements already in place for notification of direct collection and would mean less uncertainty for MBIE's customers.
27. MBIE's preference for this option is based on the assumption that the method of notification will be in line with the current requirement in New Zealand for direct collection, i.e. that the means of communication will be reasonable given the nature of the collection. At present though questions have been raised because of the uncertainty with how any new notification regime will be implemented and what level of notification will be required.
28. Concern has also been raised over how any proposed changes affect existing intelligence and compliance functions at MBIE, and how it might compromise investigations. MBIE also does not expect that option would change how existing legislation interacts with the Privacy Act. Ensuring existing exceptions remain in place would offer business groups at MBIE and their customers some assurance of consistency and the least disruption to current processes.
29. MBIE is willing and able to consult further on this topic with the Ministry of Justice if requested. Any communication on this matter can be emailed to privacyteam@mbie.govt.nz.

MINISTRY OF SOCIAL DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

Ministry of Social Development Response - Introduction

1. Thank you for seeking our views on the proposal to expand notification rules in the Privacy Act, by way of a statutory mechanism yet to be confirmed.

2. MSD has a number of concerns about the proposed change and would not be in favour of it proceeding for reasons that include:

   2.1. the scope of the proposed change;

   2.2. the compressed timeframe for comment and consideration;

   2.3. the uncertainty around which specific method will be chosen to put the change into effect;

   2.4. the likely effect on MSD's ability to efficiently carry out its functions where those functions involve the sharing of information;

   2.5. the risk of inducing 'notification fatigue' in individuals; and

   2.6. the marginal increase in privacy protection provided by the change.

3. If the change is to proceed, we would strongly recommend ensuring that all the existing exceptions in IPP3(4) apply.

Question 1 – what factors do you think are most important when considering changes to indirect collection of personal information?

4. In our view the proposed change should not proceed without careful consideration of its practical implications, additional consultation on the specific selected statutory method and review of overseas experiences with notifying individuals about indirect collection.

5. We also note the following factors that should be balanced against the projected privacy benefits of the proposed change:

   5.1. Would the change actually produce significant benefits?

      5.1.1. The transparency obligations imposed by IPP3 are important, but a significant part of that importance is that the notification typically occurs at the point of collection or shortly afterwards. This enables individuals whose information is being collected to exercise their autonomy before the collection occurs, or immediately after. Collection by third parties would tend to be more of a notification without being able to affect the collection, as any disclosure will be in line with purposes already defined or

authorisation already obtained. As such, third party notification requirements would have less impact than existing IPP3 obligations.

5.2. Unsolicited communications should not be increased unless strictly necessary.

5.2.1. Given the amount of information sharing carried out by private and public sector agencies, individuals would receive a large number of notifications. It is likely these unsolicited notifications about indirect collection would be considered equivalent to 'spam'. In most cases the notification will not present an opportunity to exercise autonomy and will just be another piece of irrelevant information to delete. This risks deprioritising public views of the importance of privacy.

5.3. Compliance burden would potentially be very high.

5.3.1. A third factor is the compliance burden of introducing a new obligation to notify individuals when sharing with other agencies takes place. Extending this to require every individual sharing of information to carry with it an individual notification would massively increase the compliance burden on MSD and any private or public sector organisation that collects significant amounts of data about individuals. Agencies would also be obliged to maintain up to date contact details for every individual whose information they collected, which would create collections of personal information that might otherwise be unnecessary.

Question 2 – What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?

6. Advantages

6.1. Increased awareness of information flows for individuals; and

6.2. Increased caution in sharing information where not necessary for agencies, helping ensure sharing is justified.

7. Disadvantages

7.1. Increased volume of trivial communications for individuals, making it more likely they 'switch off';

7.2. Compliance burden on agencies;

7.3. Every third-party collection would also require the sharing of contact details to enable notification, and potentially lead to many more privacy breaches owing to the increased volume of communications and the inevitable use of out-of-date contact information; and

7.4. Requiring agencies to collect accurate contact information solely to ensure subsequent notification can occur would not be in line with data minimisation principles.

Question 3 - what form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate. What are some potential risks and mitigations associated with the proposed changes?

8. An amendment to IPP2 does not appear to be an effective way of accomplishing the goals of the paper.

9. Amending IPP3 appears the most logical way to make the proposed change. If this method is chosen, in our view the exceptions in IPP3(4) should all apply, both for practical reasons and conceptual clarity.

10. A possible option would be to amend IPP11 to require that an agency be satisfied that the individual was aware that the disclosure to the collecting agency would take place, or if not, to obligate them to notify the individual concerned that their information has been disclosed to the collecting agency. This could have the effect of mandating transparency around indirect collection.

11. If the notification requirement is intended to apply to overseas collection, then amending IPP12 to add a notification requirement would be a relatively straightforward and tightly targeted change. However, we do not think such an amendment would accomplish the overall goal of increasing transparency

12. We are also not in favour of an additional principle, as increasing the number of principles has a disproportionate effect in making it harder to understand and communicate privacy ideas. Notification is already conceptually associated with existing IPP3 and adding a new one would blur that association.

Question 4 – if you are a New Zealand business or agency, are there any practical implementation issues you can identify in complying with the proposed changes?

13. A new obligation to notify every individual whenever information about them is collected about a third party would have enormous impacts on day-to-day operational activities, would increase the likelihood of privacy breaches by increasing data flows (essentially doubling every information sharing transaction), and require significant resources to manage the additional communication.

Question 5 – are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?

14. The document does not identify any issues around large-scale information sharing by way of formal programs (e.g. AISA/Information Match) or for approved purposes such as research. Requiring direct communication with every individual who (say) has their information shared by MSD pursuant to an information match would be both excessive and unnecessary, as section 152 of the Act already requires notification before any adverse action is taken.

15 In addition, in our view other sharing arrangements based on existing statutory mechanisms should be exempted from any new notification obligation as they were not developed with an obligation to notify individuals of indirect collection in mind.

16. The document also does not highlight the potential risks to security from sharing information about indirect collections that might, in the wrong hands, lead to an individual being harmed. MSD regularly provides information to Oranga Tamariki, for instance, about family and whanau members who may be at risk of serious harm. It is quite possible that being obligated to disclose information about that sharing would lead, in some cases, to physical harm to individuals.

Question 6 – should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?

17. We appreciate that restricting the changes to information collected indirectly from individuals overseas would minimise the operational impact, and fit cleanly within the existing IPP12 regime.

18. However, it is unclear how it would achieve the stated goal of the proposed change. Accordingly, we do not think restricting the change to offshore information would be helpful or appropriate.

Question 7 – is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback.

19. We would sound a strong note of caution around the changes being proposed for the reasons already stated.

20. We would also note the significant impact on operations for any agency that carries out bulk information sharing via an information match or approved information sharing agreement, and suggest that explicit exemption should apply to sharing under part 7 of the Act or similar provision.

21. Additionally, careful consideration should be given to the practical reality of bulk notification of indirect collection. At a minimum it would require sharing and storage of contact details, even when collecting that information would not otherwise be required. MSD's experience is that contact information changes quickly, particularly with that of its own clients.

22. Large scale use of out of date contact information could well lead to a significant increase in the number of privacy breaches caused by inaccurate information being used. Such breaches would also involve disclosure of the information collected, which could well be sensitive. If the notification were postal, another family member could open it, and if it were by email an inaccurately recorded email address could easily mean the information goes to the wrong person.

23. A final issue is that every existing formal and informal information sharing arrangement, would need amendment to set out the practical steps necessary to give effect to the new change. Similarly, information sharing processes set out in statute that were developed without this change in mind would likely need amendment.

NZ Realtors Network Ltd

C/- Barfoot & Thompson
34 Shortland Street
PO Box 4078
Auckland 1140

30 September 2022

Electoral and Constitutional
Ministry of Justice
PO Box 180
Wellington 6140

BY EMAIL: privacyfeedback@justice.govt.nz

SUBMISSION: POSSIBLE CHANGES TO NOTIFICATION RULES UNDER THE PRIVACY ACT 2020

Thank you for the opportunity to provide feedback on possible changes to notification rules under the Privacy Act 2020.

Introduction

Running for more than 20 years, NZ Realtors Network has grown to become New Zealand's largest independent real estate network (membership organisation) made up of 12 companies across 210 offices spanning New Zealand. We provide access to more than 3,000 salespeople plus 490 property managers and assistants managing over 35,000 properties.

One in five properties in New Zealand (residential, lifestyle, rural) is sold by a member of NZ Realtors Network. Two properties and over $2.5 million of real estate is sold every hour. Over $23 billion of real estate was sold in the last 12 months.

Our members work to best practice and are bound by their established ethical, codes of practice and the high expectations of their colleagues in the network. They are committed to meeting and exceeding industry standards, providing the best service to their clients and customers.

NZ Realtors Network is headed by experts in their field, with the input of Directors who are actively working as owner operators in their respective agencies.

The companies of NZ Realtors Network are:

- Barfoot & Thompson – Auckland, Northland
- Morley & Associates – Auckland
- Richardsons Real Estate – Coromandel Peninsula, Hauraki Plains
- Whangamata Rea Estate – Whangamata, Whiritoa, Onemana
- Cambridge Real Estate – Cambridge
- Lodge Real Estate – Hamilton
- McDonalds Real Estate – New Plymouth, Taranaki
- Property Brokers – Manawatu, Wairarapa, New Plymouth, Hawkes Bay, Gisborne, Waikato, Bay of Plenty, Canterbury, West Coast, Otago, Southland
- Tommys Real Estate – Wellington, Hutt Valley, Kapiti, Mana, Wairarapa
- Summit Real Estate – Nelson, Tasman, Marlborough
- Cowdy and Co – Christchurch
- Edinburgh Realty – Dunedin, Mosgiel, Cromwell.

NZ Realtors Network members are members of the Real Estate Institute of New Zealand (REINZ).

In REINZ's submission it states under their executive summary/background point 2.0 *"whilst REINZ supports The Ministry of Justice's (MoJ) desire to promote and strengthen transparency around the collection, use, and disclosure of personal information, REINZ does not support any change to the Information Privacy Principals under the Privacy Act which would prevent REINZ and our members from collecting sales data (which may contain limited personal information) in the way REINZ and the real estate profession currently does."*

The purpose of NZ Realtors Network's submission is to support REINZ's position and agree with the content of their submission.

We provide some additional comments below.

1. **What factors do you think are most important when considering changes to indirect collection of personal information?**
    - The most important factors when considering changes to indirect collection of personal data are the cost-benefit trade-offs.
    - For our members it will mean they will need to collect more personal data for the third party for them to be able to contact them – currently REINZ would only receive the address and price but no contact details.
    - The overall disruption and cost to a business/agency/organisation if every individual whose information is obtained must then be personally notified. This would be unsustainable for many businesses and adds a complex layer of administration. This has a flow on effect to the services they are then able to provide their customer base.
    - If changes are needed why are they needed? Has there been a breach of information and if so, how many and what is the scale of the issue? Will the proposed changes protect data better or could the data be sourced by someone to use in an inappropriate way?
    - Defining the scope of what is private information. Is an address and sale price of a property considered private information?
    - When people sign a contract of any kind there a clauses or statements included that you must sign and acknowledge regarding one's personal information - that your information may be passed on to a third party. Any individual that is concerned with updating their personal information only must ask the direct party who that information was passed too. Who wants to receive numerous numbers of notifications from third parties upon receipt of your details? This is agreed upon between the direct parties and individuals upon signing agreements and contracts.
    - Our members are concerned they will incur additional expense, ultimately that will need to be paid for by the client, which will not necessarily add any value to the process or reduce privacy concerns.

2. **What re the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?**
    - We see no advantage is broadening the notification requirements apart from individuals knowing who is always accessing their information and for what purpose but this in turn becomes a disadvantage because they will be constantly being notified.
    - It is important to appreciate the gravity of the decisions made with the REINZ sales data collected by the salespeople at the coalface. This data is used by the Reserve Bank to analyse the health of the housing market which is a barometer of the overall health of the economy. This data is fresh, being available monthly and even in real

time as the month progresses. The official cash rate (OCR) is determined by such information which then has a flow on to the interest rates set by the banks and a direct effect on how much money home owners need to find to service their mortgages. This information is available to trading banks and valuers also. It would be fair to say this data is of national importance and the flow of which must be timely and unfettered.

- From a property management perspective, we only provide personal data to government agencies and others who are legally entitled to the information or to contractors undertaking work at a property where the resident(s) have been fully consulted on the work to be undertaken or have requested it. Existing rules are working well.
- A vast number of disadvantages for businesses and agencies as it's yet another layer of admin, time and expense that takes away from their core service offering.
- Creating changes that require for more personal data to be stored, is a disadvantage.

3. What form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate.

Proposed changes to notification regime	Our position
Option 1: *Broadening the notification regime under IPP 3 so that it no longer applies only when an agency collects personal information directly from the individual concerned - but also when an agency collects personal information indirectly from other sources.*	**We are not persuaded there is a problem that needs fixing. We are therefore against any change.** If a change is to be made to the notification regime for indirect collection, our members prefer this option (1), provided a similar approach to indirect notification is taken to that in Australia.
Option 2: *An amendment to IPP 2 to narrow exceptions that allow agencies to collect information indirectly.*	**We oppose this option**. The industry relies on exceptions under IPP 2 to collect sales data indirectly. Depending on which exceptions are narrowed, this would have significant implications for over 17,000 real estate professionals in NZ.
Option 3: *An amendment to IPP 11 to require the disclosing agency to notify the individual concerned that their information has been disclosed to a third party.*	**We oppose this option.** The administrative cost and burden required to notify each individual once their limited personal information has been passed on to REINZ (or their approved services provider, AML provider etc) would be an extraordinary burden on the real estate sector, especially those who are sole independent agents or small agencies. The administrative cost incurred will need to be recovered by REINZ and other service providers meaning an increase in fees charged by REINZ and other service providers to our members. Our members would have to consider cost recovery from their clients/customers.
Option 4: *Introducing a new privacy principle.*	**We do not have enough information to comment on this option**.

- Notification rules should allow for some practical discretion - e.g. in the property management sector, if tenant's contact details are provided to a plumber so they can contact them directly to arrange a time for a site visit, we should not be required to formally notify the tenant that we have done this. Generally the tenant

will have requested the work and will know we will be arranging for a plumber to attend to the issue. The signed contract with the plumber may state they must only use personal data for the purpose for which it was provided.

- Form exclusions for REINZ in this instance is potentially more damaging than it is protective due to the unnecessary increased amount of personal data that would be shared.
- Is a change necessary when individuals are already aware their information may be passed on to third parties? If those third parties are clearly stated in an agreement there should be no need for a change in procedure. The privacy situation and the collection of data of both parties to a real estate transaction (buyer and seller of property) is clearly noted in clause 19.0 in the Agreement for Sale and Purchase of Real Estate (produced by ADLS and REINZ):

  19.0 Collection of Sales Information
  19.1 Once this agreement has become unconditional in all respects, the agent may provide certain information relating to the sale to the Real Estate Institute of New Zealand Incorporated (REINZ).
  19.2 This information will be stored on a secure password protected network under REINZ's control and may include (amongst other things) the sale price and the address of the property, but will not include the parties' names or other personal information under the Privacy Act 2020.
  19.3 This information is collected, used and published for statistical, property appraisal and market analysis purposes, by REINZ, REINZ member agents and others.
  19.4 Despite the above, if REINZ does come to hold any of the vendor's or purchaser's personal information, that party has a right to access and correct that personal information by contacting REINZ at info@reinz.co.nz or by post or telephone.

- No change is warranted for the sake of change.

4. **If you are a New Zealand business, are there any practical implementation issues you can identify in complying with the proposed changes?**
   - The proposed change requiring a third party to affirm the use of the seller's details of their sale is troublesome as it requires the recording of contact details of those individuals. Currently, the contact details of the seller and the buyer are not recorded by REINZ (see 19.2 above). For a third party to gain clearance to use data, the contact details will then be needed to be passed to these third parties. With more data being shared to comply this creates more paperwork, more transfer of personal data and more chances of issues and breaches. This is more opportunity for immoral entities to source this information which previously did not exist in REINZ databases.
   - Also, what is the definition of a third party? So far we have defined REINZ as the third party, But, as an example, when REINZ passes the sales statistics to the Reserve Bank every month, will the Reserve Bank need to contact every agent for clearance to use the data that is legally theirs at that point, because the agent is then the third down the chain of that information? Or would the Reserve Bank need to go to the seller and the buyer or all three? Clearly, this is impractical and opens a vast number of doors for sensitive information that is currently not captured, to be harvested through cyber-crime.
   - As a real estate agency third party information forms a crucial part of services provided, in particular CMA documentation, if this service is delayed or no longer available, it will have a severe impact and flow-on effect to vendors who rely upon

current market information such as comparable sales. Access to this information underpins the service agencies provide.

- A practical implementation issue relates to Body Corporates and Residents' Associations or Societies where there is often a need to provide unit holder contact details to third parties undertaking work in shared spaces. If the strata rules clearly state the circumstances in which such information will be provided, there should not be an additional notification requirement adding unnecessary administration delay and cost to the process of getting repairs and maintenance or security issues addressed.

5. **Are there any other risks or mitigations to the proposed changes you can ident fy that are not mentioned in this document?**
    - If personal information is provided incorrectly from an individual or direct party (e.g. an email address or someone has moved) what are the obligations of the third or indirect party to try and locate these individuals. This adds a near impossible barrier to overcome that in turn adds to an increase in resources required to fulfil such obligation or policy.
    - The facts are clear that the path for a third party to gain authority to use this sales data, would be tedious and in many cases could end in exhaustion due to inability to complete or too higher cost. There for we would end up with gaps in the data and an incomplete data set. REINZ have been compiling sales statistics since 1992 and this data is invaluable - any law change that would threaten the integrity of this data is not sensible.

6. **Should the proposed changes only apply to personal information collected indirectly from individual overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?**
    - Many sellers and buyers of New Zealand property live overseas. Their information regarding their sale or purchase is required for national statistics, like those who reside in New Zealand. Both those who reside overseas and are resident in New Zealand, bind themselves to this requirement upon signing of an agency and/or upon signing of a sale and purchase agreement.

7. **Is there any other feedback you would like to provide of these proposed changes? If so, please provide this feedback.**
    - The changes appear to increase the risk of data breaches. In an agency agreement, we believe we should be able to give the option for the sales information to be shared with REINZ (as is already). As a larger percentage of the information is publicly available in real time and on settlement the information becomes public also, it appears the proposal is creating more harm than good, with the collection of more information.

Thank you again for the opportunity to provide feedback on behalf of our members.

Yours sincerely

s9(2)(a)

s9(2)(a)

Donna Peffers
General Manager
NZ Realtors Network
E: donna@nzrealtors.co.nz
M: s9(2)(a)

Emma Ashworth
Chairman
NZ Realtors Network

NEW ZEALAND BANKERS ASSOCIATION

Submission

to the

Ministry of Justice

on the

Engagement Document: Possible changes to notification rules under the Privacy Act 2020

30 September 2022

NEW ZEALAND BANKERS ASSOCIATION
Level 15, 80 The Terrace, PO Box 3043, Wellington 6140, New Zealand
TELEPHONE +64 4 802 3358 EMAIL nzba@nzba.org nz WEB www.nzba.org.nz

About NZBA

1. The New Zealand Bankers' Association (**NZBA**) is the voice of the banking industry. We work with our member banks on non-competitive issues to tell the industry's story and develop and promote policy outcomes that deliver for New Zealanders.

2. The following eighteen registered banks in New Zealand are members of NZBA:
   - ANZ Bank New Zealand Limited
   - ASB Bank Limited
   - Bank of China (NZ) Limited
   - Bank of New Zealand
   - China Construction Bank
   - Citibank N.A.
   - The Co-operative Bank Limited
   - Heartland Bank Limited
   - The Hongkong and Shanghai Banking Corporation Limited
   - Industrial and Commercial Bank of China (New Zealand) Limited
   - JPMorgan Chase Bank N.A.
   - KB Kookmin Bank Auckland Branch
   - Kiwibank Limited
   - MUFG Bank Ltd
   - Rabobank New Zealand Limited
   - SBS Bank
   - TSB Bank Limited
   - Westpac New Zealand Limited

Introduction

NZBA welcomes the opportunity to provide feedback to the Ministry of Justice (**MoJ**) on the Engagement Document: Possible changes to notification rules under the Privacy Act 2020 (**Engagement Document**). NZBA commends the work that has gone into developing the Engagement Document.

Contact details

3. If you would like to discuss any aspect of this submission, please contact:

Antony Buick-Constable
Deputy Chief Executive & General Counsel
antony.buick-constable@nzba.org.nz

Brittany Reddington
Associate Director, Policy & Legal Counsel
brittany.reddington@nzba.org.nz

Summary

NZBA generally supports developments to bolster an individual's right to privacy. However we also consider that legislative changes should typically occur in response to a clear problem or need.

These changes are likely to have a number of adverse impacts on both consumers and businesses. Therefore, any problem definition and resulting benefits that might flow from the proposed changes should be identified at the outset. In our view, the current notification regime under the Privacy Act sufficiently covers indirect collection of personal information, and is broadly aligned with overseas jurisdictions.

If MoJ decides to go ahead with these changes, we recommend a further consultation clearly outlining the problem definition and proposed changes, with further information on the detail and granularity of the requirements. Any changes should be narrow and directly respond to the problems identified, with clear exceptions to avoid any adverse consequences.

We are happy to discuss any aspects of this submission further if helpful.

Factors most important when it comes to considering changes to indirect collection of personal information

Problem definition

Any proposal of legislative change should always include careful consideration of the problem such change is trying to address. In this instance, we query whether there is in fact a material gap in the current notification regime that warrants legislative change.

Under the Privacy Act's IPP 2, agencies must generally collect information directly from an individual unless an exception applies. In practice, these exceptions are only invoked on a limited basis and where applicable; it may not be appropriate to notify the individual in each instance for legitimate reasons. For example, if the information is already publicly available then a disclosure is not necessary (and could just result in notification fatigue) and if the information was collected for law enforcement purposes, then a disclosure to the individual concerned could interfere with legal proceedings. In any event, under IPP3, an agency is required to tell an individual when it intends to share their information with any third parties – so an individual should be informed from the outset about where their information is, or may be, held. Accordingly, banks, as agencies under the Privacy Act, already have lengthy IPP3 privacy collection notices given their complex business models.

Further, we consider that the status quo is broadly in alignment with overseas regulatory frameworks. Broadly, both the GDPR and the Australian Privacy Act have materially similar outcomes to that of the New Zealand Privacy Act, with the end result being that all individuals are currently entitled to notification of where their personal information is being collected, used and disclosed, unless an exception applies.

Impact of the possible changes

The impact of any proposed changes will need careful consideration. These proposed changes will impact both consumers/individuals and businesses/agencies who collect information from, or share information with, a third-party source. For consumers/individuals, these changes could result in an overload of information, undue anxiety, and confusion. This would likely lead to increased complaints and disputes and an overall worse customer experience.

For businesses/agencies, there may be a number of issues arising depending on the framework. These could include:

- In the banking context, customers are already provided with lengthy privacy collection notices setting out how information collected directly may be used or shared. To overlay a separate obligation may generate overly complicated disclosures.
- Interference with reasonable and required embedded business processes may arise as a result of this change, such as credit checks, identity verification checks or mortgage broker arrangements.
- There may be adverse consequences in some instances e.g. where notification discloses debt collection activity or law enforcement activity that may jeopardise collection or the integrity of the personal information collected.
- Notification may often be impractical as the collector will not necessarily have a relationship with the individual concerned. Legislation should not force more personal information to be collected (address, contact details etc.) in order to comply with legislative requirements.
- There is likely to be an increased compliance burden with no clear corresponding benefit. We believe existing processes are transparent and more than sufficient to ensure that individuals understand how banks are handling and protecting their information. Any further disclosures made to individuals on top of those existing processes, in each and every instance that information is shared, may just result in compliance burden and notification fatigue (as already identified in the Engagement Document). It is important that banks strike the right balance between being transparent and clearly explaining to individuals what information they hold about them, without overloading them with information and draining organisational resource unnecessarily.
- There are likely to be increased compliance costs in keeping disclosures current and up-to date (these would need constant updating for each new agency or supplier). It will be difficult to deal with the frequency of the changing status of vendors/third parties.

Form the proposed changes should take

If the Ministry decides these changes are necessary, any amendments to the existing IPPs, or creation of a new IPP, should be narrowed so that they address only the particular concern at issue.

There should also be carve outs/exceptions for instances where notification would be unnecessary (e.g. where the information is already publicly available or where the individual

has already authorised the collection of such information) or where notification would be inappropriate (e.g. where the information is being collected for law enforcement purposes or where disclosure would undermine the purpose for which the information was being collected). We note that in Australia, there are exceptions available under APP5 for third party collection of information in certain instances.

We also note that some global firms comply with the GDPR requirements by placing the notification onus on the third party providing the information to the firm (in contract). For example, if Party A has a direct relationship with an individual and provides information to Party B, the parties have an agreement that Party A will notify the individual rather than Party B. This may be a way to avoid some of the issues we refer to above.

Copied below is a summary of the contents of an email from NZSIS and GCSB identified as being in scope of your request:

Title of Email: RE: Privacy Act changes

Date: 5 October 2022

Summary:

In accordance with the New Zealand Government's priorities and the Intelligence and Security Act 2017 (ISA), the NZSIS and GCSB (the Agencies) collect personal information in order to achieve their objectives and functions to protect New Zealand's national security, international relations and economic wellbeing. To enable our ability to perform these functions, we request that the Agencies be exempt if a new notification requirement for collection of personal information from third parties is added to the Privacy Act (as we are from the current IPPs 2, 3 and 4(b)). We also consider that appropriate exemptions should be given to third parties receiving personal information from the Agencies for the same reason. This could occur via a general exemption from the notification requirement if one of the Agencies is the provider of the information or an equivalent to those set out in IPP3(4)(b) and (c) (these would apply automatically if the notification requirement is enacted via an amended IPP3(1)).

Exception from any proposed notification requirement would be consistent with the current recognition in the Privacy Act of the Agencies' unique role in collecting, using and disclosing personal information. As well, privacy regimes internationally, including the GDPR, continue to limit their application to intelligence and security agencies like the Agencies.

NZT-7882 – Proposed changes to the Privacy Act 2020

7 October 2022

Waka Kotahi NZ Transport Agency has been asked to provide comments on the proposal to change the Privacy Act's notification rules.

Waka Kotahi NZ Transport Agency's response:

Operational teams do not draw private information from third parties who aren't already acting as agents for Waka Kotahi. The collection of this information is with the knowledge of the individual concerned and with their consent. As a result, we are unlikely to have any need for changes to the way we notify individuals we are collecting their personal information.

Intelligence work is undertaken with other agencies within the boundaries of Information Privacy Principal's (IPP) 2(e), 4 and 11(e).

From the information contained within the proposed broadening of notification rules, we do not anticipate any direct impact on our ability to undertake intelligence analysis. However, with the potential changes only being broadly defined, it is difficult to comment on any impacts with certainty.

Waka Kotahi would appreciate clarification of the below;

- The proposed amendments to IPP3 are in relation to collection from other sources. Does this also apply to open-source intelligence, e.g. social media?
- It would be useful to gain an understanding of what is considered personal information. For example, point to point cameras are a form of tracking – would these changes require an individual to be notified every time their information is collected, even if not held?

Contact Adrian J. Carter

30 September 2022

Ombudsman
Fairness for all

The Ministry of Justice
Wellington, 6140

Via email:
privacyfeedback@justice.govt.nz

Tēnā koe,

Consultation on indirect collection of personal information by third parties

I refer to the engagement document published by the Ministry on potential changes to the notification rules for collecting personal information from third parties.

This is an issue of interest to the Chief Ombudsman as it has significant implications in terms of the principles of fairness and natural justice.

By way of context, successive Ombudsmen have considered a number of complaints raising concerns that information obtained from third parties and relied on by government agencies to make decisions was incorrect, presented unfairly or out of context. In the absence of the individual knowing that adverse information is held, and possibly being relied on, by agencies—particularly where it has been collected from a third party without their knowledge—they are not in a position to seek a copy of that information and to have it corrected under the Privacy Act at an early stage.

The Chief Ombudsman notes that in the absence of a notification at the time of the information gathering exercise, the existence of adverse information may only surface some weeks, months or years later, at which point it may be difficult for the affected individual to fairly contest its accuracy.

In light of this, the Chief Ombudsman offers in-principle support for the proposed notification regime where doing so might permit parties to properly seek and retrieve the information at issue and, where appropriate, to seek its correction or to provide a contextual explanation. However, such a notification regime should not, in and of itself, absolve the relevant agency from its obligations under Principle 8 of the Privacy Act to take proper steps to check the accuracy of information it receives and relies upon to make decisions.

The Chief Ombudsman looks forward to the opportunity to provide more substantive comments in due course.

Yours sincerely

s9(2)(a)

Emma Leach
Senior Assistant Ombudsman

Office of the Ombudsman
Tari o te Kaitiaki Mana Tangata

L 7, 70 The Terrace, Wellington 6011
PO Box 10 152, Wellington 6143
New Zealand

Tel: 64 4 473 9533 Fax: 64 4 471 2254
Free phone: 0800 802 602
www.ombudsman.parliament.nz

ORANGA TAMARIKI
Ministry for Children

Oranga Tamariki—Ministry for Children feedback on proposed changes to notification rules under Privacy Act 2020

Summary of feedback

This feedback responds to the Ministry of Justice proposal to broaden notification requirements in the Privacy Act so they would also apply when agencies collect personal information indirectly via a third party, rather than directly from the individual concerned ("indirect collection of personal information").

Oranga Tamariki recognises and appreciates the call for greater transparency around the collection, use, and sharing of people's personal information and how the MOJ proposal intends to support the principles embodied by the Privacy Act and the Data Protection and Use Policy. However, Oranga Tamariki is uncertain the proposal will achieve this goal or whether it might rather establish a framework that ultimately undermines these privacy objectives. Oranga Tamariki also has significant reservations about the feasibility, suitability, and prudence of the proposal from an operational standpoint and considers it will likely have a variety of unintended outcomes. We would have appreciated more time to work through the likely impact of the proposed changes on our mahi and our Future Direction.

We are concerned that the purposes and proposed benefits of the changes are not well backed up by examples of how they will apply in practice. Given that the changes are modelled on overseas jurisdictions, we hope that research is being undertaken to determine the successes and challenges experienced in those other jurisdictions, including regarding the use and sufficiency of exceptions, and how the New Zealand proposals can reflect those learnings.

We consider that the existing exceptions in IPP 3(4) will need to apply to notifications of indirect collection and that those exceptions will apply to much of our mahi. We would also strongly support an additional exception under IPP 3(4) where non-compliance is necessary to prevent or lessen a serious threat to the life or health of the individual concerned or another individual (as is currently included in IPP 11(1)(f)).

In terms of operational practicalities, it may also be prudent to have an exception where notification has already been made by the disclosing third party, another party, or where the collecting party is reasonably satisfied that the individual concerned is aware that the disclosure would take place.

We are also of the view that information sharing provisions in the Oranga Tamariki Act 1989 (see sections 66C, 66K and 66Q) should be exempted from the proposed notification amendment. In addition to concerns over how the notification amendment might frustrate the purpose of collection (discussed below), we believe section 66K of

the Oranga Tamariki Act (which requires consultation where practicable and appropriate) already encapsulates the function and purpose of the proposed changes.

We have answered your questions as best as we can in the timeframe available. We also attach three worked examples where we have tried to work through how the proposed changes might apply in a child welfare and protection setting. We have made some assumptions about the applicability of exceptions and would welcome further kōrero on this.

Response to questions

1. *What factors do you think are most important when considering changes to indirect collection of personal information?*

   First, what is the purpose of the change? There must be a clear connection between the proposed change and the purpose that it seeks to achieve. The engagement document describes the key purpose as *the promotion and strengthening of transparency*. Secondary purposes mentioned are *keeping up to date with privacy laws and best practices in overseas jurisdictions* and *supporting international trade, in particular the cross-border flow of personal information as a basis for digital trade*.

   Having established the purpose, we then consider how that purpose can be achieved. The engagement paper suggests some options based on amending the IPPs to require notification of indirect collection of personal information.

   We must then consider **how the purpose should be balanced against other interests and whether these options will result in a proportionate outcome when applied in practice**. It is this analysis that we feel is lacking at this time, but we expect that the requested feedback will help inform this analysis.

   For our part, we have identified the following relevant considerations:

   - Factors to be balanced against the purpose of transparency –
     - How can we ensure that existing recognised public interests, such as information sharing in the best interest of tamariki and rangatahi (s66C Oranga Tamariki Act 1989), are not unreasonably impacted?
     - What is the desire of individuals to be notified and what is the risk of notification fatigue? For example, cookie notifications and privacy policies. Who reads them and do they truly promote transparency? Research has shown that it is not humanly possible to read all the privacy notices the typical internet user has to accept. Adding to that framework an as yet unquantified, but likely excessive, number of third-party privacy notifications will likely lead to apathy, anxiety over what they can't really control, and/or greater mistrust of government and business. If individuals begin to receive frequent notifications about indirect information sharing by government

agencies that they cannot opt out of, it is hard to imagine they will feel more empowered.

- Every addition and exception to the privacy framework creates more complexity. The privacy framework should be easily understandable by the community. The more complex it becomes, the less likely it is to promote confidence and transparency.
- Roles and responsibilities will need to be clear e.g. which agency is responsible for making the notification or deciding that an exception applies. Lack of clarity risks duplication of notification, frustration of purpose, non-compliance, and uncertainty as to who is responsible for any corresponding interference with privacy. It may also negatively impact safety and impede our ability to carry out our legislative duties e.g., a provider notifying a potentially volatile client that they have collected information from Oranga Tamariki, or provided information to Oranga Tamariki for the purposes of investigating a report of concern or assessing the needs of te tamaiti and the whānau.
- Is the requirement operationally feasible? Apart from the high compliance cost the proposed change is likely to have, compliance may not always even be possible. The collecting agency may not have a direct relationship with the individual, and therefore may not have up to date contact details. This could lead to inconsistent application of the provisions or overreliance on exceptions which could further impact public trust.
- Likewise, there may be feasibility issues if the responsibility for notification is placed upon the disclosing third-party. Oranga Tamariki collects a high volume of information indirectly from members of the public. It is highly impracticable to expect that a neighbour, teacher, or other concerned member of the public making a report of concern, or providing other information, would also need to notify the individuals concerned.

- Factors to be balanced against the purpose of keeping up to date with other jurisdictions and supporting international trade –
  - What is the practical experience in other jurisdictions? Have we explored how those regimes work in practice, including any negative consequences (such as notification fatigue and any chilling effects e.g., on authorised information sharing for a legitimate purpose)?
  - How do the exceptions to notification in our Act compare with the exceptions in other jurisdictions and what is the effect – does the notification regime achieve its purpose overall and are the exceptions used appropriately? How do those jurisdictions ensure that the notification requirement does not negatively impact social service agencies' ability to support and safeguard children and families? We would be interested to know how child welfare agencies navigate these requirements.
  - An example from our own practice that may be illustrative of these concerns is the Oranga Tamariki International Child Protection Unit and International

ORANGA TAMARIKI
Ministry for Children

Adoptions Service. The work of this team regularly requires the exchange of personal information across borders. The information is highly sensitive and the collection and disclosure of this information is indirect (not to or from the individuals concerned). The purpose of the team's role could not be achieved without these exchanges. One of the organisations the team works closely with for this purpose is International Social Services (ISS) based in the EU. The Directors of ISS raised recent changes to the EU privacy regime as a significant concern. We are not sure how they have resolved the implications of the EU law on their cross-border work, but this is the kind of 'law in practice' research that we consider is necessary for the proper consideration of the proposed changes.

2. *What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?*

We consider that the response from the OPC sets out the advantages of broadening the notification requirements, in particular greater transparency around the collection, use, and sharing of people's personal information. However, we are uncertain the proposed changes will achieve these objectives and ask that those potential advantages be considered and weighed against the following concerns and potential disadvantages:

- General:
  - Notification fatigue and the risk that notification without a real opportunity to object will not promote feelings of being in control. A constant stream of such notifications may result in distress, mistrust, or ambivalence.
  - Compliance costs and uncertainty:
    - Given the huge breadth of personal information and the purposes for which it is collected, it will take significant resource to consider, determine and implement appropriate notification in each situation. In some cases, a statement on a website may be sufficient; in others a face-to-face conversation will be required, and there are many options in between. The personal information we deal with may be about adults, children, young people, or a mix, so notification needs to be appropriately tailored to the audience. There is also likely to be competing public interest considerations that require balancing when deciding whether an exception applies, e.g., transparency vs guardianship rights, privacy, and/or the best interests of the child.
    - As indirect collection often involves third parties who may not have in-house privacy expertise, (e.g., NGOs or offshore organisations), we consider that the OPC will need to provide significant guidance. If agencies are left to upskill each other, compliance costs will be significant (e.g., the time and resources social sector government departments will need to dedicate to assist providers).

ORANGA TAMARIKI
Ministry for Children

  - Depending on the privacy maturity of indirect collectors, the appropriate application of exceptions, and the extent to which guidance is available so that the correct choices can be made, there may also be a corresponding increase in privacy breaches: situations where individuals are put at risk or harmed, and situations where the purpose of collection is frustrated (e.g., where notification goes to the wrong individual as a result of out of date contact information, where inappropriate persons are made aware of the collection through the form of notification, or where an exception under IPP 3(4)(b) or (c) should have applied but either the exception or the particular sensitives of the information were not well understood by the notifier).

- Specific to the child welfare and protection sector:
  - The nature of our work means we indirectly collect information about people we may not have a ready way of contacting. In most cases, it would be impracticable and potentially intrusive to locate them and then verify their identity for the purposes of notifying them. In any event, this exercise would require us to collect more personal information than is necessary to perform our function.
  - Furthermore, it should be recognised that there are additional complexities and risks involved when notifying tamariki and rangatahi about the collection of their information. It is vital that any notification of collection of personal information, especially when that information may be sensitive to them, is done in a way that maintains their safety and trust. It will be particularly difficult to ensure that happens if notification is made by an indirect collector of their information. Moreover, the young people and the families we work with are often transient and change their contact details frequently. This may result in delays or other difficulties when trying to contact them to notify or consult.
  - We also need to consider the trust, safety, and wellbeing of tamariki and rangatahi when they are the ones providing us with personal information about third parties with an expectation of confidentiality. Notification could not only frustrate the purpose of collection but put tamariki, rangatahi, their whānau, or others in danger, and discourage tamariki and/or rangatahi from speaking openly with us in the future.
  - Notification requirements may inadvertently create a barrier, or at a minimum, a delay in providing support services to tamariki and rangatahi.
  - Depending on the breadth of the obligation and the available exceptions, notification of indirect collection may frustrate the purpose and/or operation of information sharing provisions in other legislation or AISAs.
  - If the obligation to notify is on the collector of the information, there is a risk that that collecting agency may not fully appreciate contextual sensitivities that are known to the agency disclosing/sharing the information. This may result in exceptions not being applied appropriately which may result in

privacy breaches or other harm e.g., in situations where notification of collection puts a child or other individual at risk. It may also create a chilling effect whereby agencies are more reluctant to share concerns about a child or whānau, especially if the situation does not clearly meet an IPP 3(4) exception. This would go directly against the policy intent of the information sharing provisions in the Oranga Tamariki Act and Family Violence Act. See also our comments about sections 66 and 66C of the Oranga Tamariki Act 1989, in the attachment.

3. *What form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate.*

   Although we don't believe the change is warranted, if it were to be enacted, it would, in our view, best sit within IPP 3. However, we believe there needs to be further consideration as to whether it is the agency sharing the personal information or the agency receiving it that makes the notification and have particular concerns about notification being made by an agency that does not have sufficient relationship with the individual or the appropriate context to adequately consider the impact of the notification.

   We cannot stress enough how vital it is to our work that the exceptions in IPP 3(4) are maintained in respect of any change to notification requirements. We also would strongly support an additional exception under IPP 3(4) where necessary to prevent or lessen a serious threat to the life or health of the individual concerned or another individual (as is currently included in IPP 11 (1)(f)). In terms of practical application, a further exception may be justified where notification has already been made by the disclosing third party, another party, or where the collecting party is reasonably satisfied that the individual concerned is aware that the disclosure would take place.

4. *If you are a New Zealand business, are there any practical implementation issues you can identify in complying with the proposed changes?*

   We suspect that the change will have a tremendous operational burden unless exceptions can be applied to the majority of our statutory work. Oranga Tamariki needs to collect and disclose high volumes of personal information from and to a variety of third parties on and off-shore in order to promote the wellbeing and best interests of tamariki and rangatahi, to fulfil the purposes of our Act, and give effect to Te Tiriti o Waitangi (see s4 and s7AA). We consider that additional notification requirements will make this process substantially more onerous and ultimately impede our ability to act in the best interests of tamariki and rangatahi.

   Additionally, Oranga Tamariki, the Ministry of Health and others are currently in the midst of a transformation in terms of what Treaty partnership means in practice. We are considering whether the law needs amending to better enable information

ORANGA TAMARIKI
Ministry for Children

sharing with iwi and Māori partners, informed by tikanga Māori and the Treaty, to uphold the right of Māori to care for and raise the next generation and reflect a genuine approach to Treaty partnership. We would appreciate more time to consult with our Māori partners about how this proposed change might impact our relationship with them, current sharing practices, and any affected elements of this transformation.

5. *Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?*

   The short timeframe for consultation means that we have not been able to adequately consult all areas of the organisation whose work may be impacted by the proposed change, or the providers and communities we work with. We have had to make some assumptions and generalise our feedback, whereas we suspect more specific examples might be of more assistance to you in the next stage of consideration. We hope that you are able to get data from other jurisdictions that will provide better evidence of the likely pros and cons of the proposal.

6. *Should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?*

   While it would operationally be preferable for the proposed change to only apply to overseas citizens, this does not seem a reasonable, credible, or trust-building approach that benefits all New Zealanders.

7. *Is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback.*

   There should be substantially more time for agencies to consult with their internal teams and partners and provide thoughtful and informed responses to these proposed changes.

ORANGA TAMARIKI
Ministry for Children

Attachment: Examples of how the proposed changes might apply in a child welfare and protection setting

Information sharing under sections 66 and 66C of the Oranga Tamariki Act 1989

Section 66 of the Oranga Tamariki Act 1989 requires agencies to provide to Oranga Tamariki (or Police), on request, information that may relate to or affect the safety or wellbeing of a child or young person if the information is required for the purposes specified in that section. Oranga Tamariki will be an indirect collector when this section is used, but in many cases, notification would prejudice the purpose of the collection or put individuals at risk of harm.

Section 66C of the Oranga Tamariki Act enables information sharing within the child welfare and protection sector for specified purposes. The provision applies to a number of agencies, organisations, and individuals as defined in section 2. Oranga Tamariki will not always be party to information sharing under s66C (e.g., the Ministry of Education might share personal information with the Ministry of Health under s66C, or an NGO and a midwife might share personal information about a mutual client under this provision).

Section 66K requires consultation prior to disclosing information under section 66C, where it is practicable and appropriate to do so. We consider that this section addresses privacy considerations in a more appropriate way in this context and provides sufficient transparency without the need for legislative change. Alternatively, s66K could be said to be inconsistent with the proposed changes, and therefore prevail by virtue of s66Q(4).[1] In either event, our view is that the proposed notification requirement should not apply to information sharing under s66 or 66C. We note that IPP 3 does not currently apply to the collections of information under s66 and s66C. However, IPP 11 does, which will be an important consideration if the new notification requirement is incorporated into that principle. See section 66Q.

Scenario 1

A midwife identifies some welfare concerns for the older sibling of the pēpē she is visiting. She mentions the concerns to Māmā and, in accordance with s66K consults her about mentioning the matter to Plunket as she is aware that the sibling is due for a B4 School Check. Māmā is happy with this.

Sharing the information with the Plunket nurse is allowable under s66C, because:

- both Plunket and the midwife are within the sector as defined in s2 of the Oranga Tamariki Act;
  the information will be shared for one of the authorised purposes – to ensure that Plunket has the information to contribute to its assessment of need in relation to the child (s66C(a)(ii)); and

[1] This paragraph considers the role of s66K in the event that the proposed notification changes do become applicable to information sharing under the Oranga Tamariki Act.

- the consultation requirement of s66K has been fulfilled.

Plunket, as the collector of the information, would need to notify Māmā that they had collected the information even though the midwife had already consulted. This requirement would apply unless an exception under IPP 3 applied, e.g., IPP 3(4)(a), that non-compliance would not prejudice the interests of the individual concerned.

Scenario 2

As above, but rather than welfare concerns about the sibling, the midwife has safety concerns due to a disclosure made by the sibling. Based on the disclosure, the midwife considers that consulting with Māmā would likely result in harm to te tamaiti and so does not consult under s66K of the Oranga Tamariki Act 1989. The midwife makes a Report of Concern to Oranga Tamariki under s15 of the Oranga Tamariki Act and also raises the issue with Plunket under s66C, so that Plunket can follow up at the B4 School Check.

Plunket notifies Māmā and Pāpā (as guardians of te tamaiti) in accordance with the new indirect collection requirement, not turning their mind to the potential risk to te tamaiti or Māmā. This puts te tamaiti and Māmā at risk and results in Māmā not taking te tamaiti to the B4 School Check, undermining the purpose of the disclosure. It also makes it more difficult for Oranga Tamariki to engage with the family, as Māmā has lost trust in the professionals who were trying to help her and her whānau. While we consider that an exception under IPP 3(4) may apply in this scenario, e.g., prejudice to the maintenance of the law, or prejudice to the purpose of collection, we are not confident that the collecting agency (Plunket) would necessarily consider and apply that exception.

Scenario 3

Cross-border sharing

DIA shares with Oranga Tamariki some concerns about a passport application that suggest possible child trafficking.

Oranga Tamariki, with the assistance of MFAT, works with an international NGO and officials in the country where the application was made to seek to establish the veracity of the application.

The NGO is concerned that it needs to notify the applicant that Oranga Tamariki has shared the applicant's personal information with them.

Our view is that the exception in IPP 3(4)(b) should apply to all agencies involved, whether they are considered direct or indirect collectors of the information. Notification would 'tip the applicant off' and prejudice the investigation of the possible offence. It may also prejudice parallel/concurrent investigations in other jurisdictions (e.g., with respect to child trafficking and/or modern-day slavery). However, as mentioned above, and particularly with the existence of parallel investigations involving multiple agencies, we are not confident that all collecting agencies would consider, let alone understand and apply, the relevant exception to the notification requirement.

Carter, Adam

From: Melvin Plaisier <melvin.plaisier@raywhite.com>
Sent: Wednesday, 14 September 2022 2:24 pm
To: Privacy Feedback
Subject: Privacy act notification rules

To whom it may concern,

Below is my feedback submission for the proposed change to the privacy act in relation to the sharing of sales data to the likes of local authorities, REINZ and the REA.

Your questions are answered below

1. What factors do you think are most important when considering changes to indirect collection of personal information?

the most important consideration is the current flow of data to the likes of REINZ, incl the existing benefits of property sales data being available to the general public. People's privacy is no doubt an important issue, however, the value of this information to all members of the public is hugely significant. The loss of this open information would be very detrimental to homeowners and prospective purchasers

2. What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?
The disadvantages to the agency will be as follows.
If the public begin not to share their house sale data, then not all sales data will be fed through to current agency portals such as REINZ, or even worse, the complexity and cost will make it no longer viable. The cost will increase for information that is no longer accurate or reflective of the market.
Salespeople and agents will not have as much confidence in their appraisals.
Agencies have had access to this data since the 1980's with little to no gaps in the data, if we lose this reliable feed of info, there will be massive holes in future data.

For the buyers and sellers of property.
We may incur more costs as an agency, which will reduce the agencies abilities to reduce client costs.
Sellers may undersell due to a lack of information in relation to sales in the area.
Buyers may be reluctant to pay fair market value as they can not see comparable sales in the area (Loss of confidence)
Buyers may request that their information is not made public, if this buyer is a property trader, they may then hide their purchase info, leaving the next buyer blind to the sales history. Currently, buyers feel empowered with knowledge, giving them the confidence to purchase.

3. What form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate.
An adjustment o agency agreements and possibly sale and purchase agreements in order to allow us to share the sales data would be best.
This will allow fo us to carry on as usual, give the public options as to the us of data and mitigate a massive loss of data
What would not be appropriate is for the reliable third parties that we work with within the industry to then need to gain their won consent, as this will be hugely time consuming, expensive and likely make their service redundant.

4. If you are a New Zealand business, are there any practical implementation issues you can identify in complying with the proposed changes?

Just the time and cost involved in the change of all agency agreements and sale and purchase agreements (Again)

5. Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?
Just as per my notes in Q1 and q2

6. Should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?
No Opinion

7. Is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback.

Melvin Plaisier
Branch Manager and Business Owner | Parklane Real Estate Ltd trading as Ray White Swanson (Licensed REAA 2008)

M s9(2)(a) T s9(2)(a) F 09 832 2783

Whttp://rwswanson.co.nz

A753 Swanson Road, Swanson

Platform Charitable Trust
Salmond House
57 Vivian Street
Te Aro
Wellington, 6011

admin@platform.org.nz
www.platform.org.nz

Friday, 30 September 2022

Electoral and Constitutional, Ministry of Justice, PO Box 180, Wellington 6140

Submitted via email to privacyfeedback@justice.govt.nz

Tēnā koe Electoral and Constitutional, Ministry of Justice,

Thank you for the opportunity to provide feedback on the possible changes to notification rules under the Privacy Act 2020 ('the Act').

Who are we?

Atamira | Platform Trust (Platform) is a peak body organisation representing the mental health and addiction (MH&A) non-governmental organisation (NGO) and community sector. We represent 82 MH&A NGOs and community organisations that provide support to tāngata whaiora (people seeking wellness) including Māori and Pasifika providers, and whānau and peer-led services. Platform has sought input from our members as part of this submission.

In addition to our members, Platform represents a wider network of MH&A NGOs who share the same aspiration of an MH&A system and sector that is driven by the need for better and more equitable outcomes for all. Collectively across 2020/21, MH&A NGO and community providers have supported over 80,000 tāngata whaiora, 36.5% of which are Māori and 6% Pacific Peoples[1], approximately 42% of all people accessing specialist support for their mental health or addiction needs in Aotearoa (1).

Introduction

Thank you for the opportunity to provide feedback on the possible changes to the notification rules under the Privacy Act 2020. Overall, the Act provides sound and clear principles and provisions which enable transparent collection, use and disclosure of information to protect individuals' privacy rights, their dignity and autonomy.

[1]Data from Programme for the Integration of Mental Health Data (PRIMHD) data set, sourced 27/03/22.

Any possible changes to notification rules under the Act, should not weaken the existing principles and provisions which allow for individuals to:

- make informed privacy choices;
- hold agencies to account for their privacy practices; and
- to exercise their privacy rights under the Act.

MH&A NGOs and community providers hold personal information about tāngata whaiora, whānau who they support in the community and often very vulnerable. It is therefore critical that possible changes to the notification rules under the Act do not lead to unintended consequence's resulting in the misuse of personal information held by MH&A NGOs and community providers.

1. Feedback

Our feedback of the seven questions is as follows:

1. What factors do you think are most important when considering changes to indirect collection of personal information?

- Individuals must be informed of the processing of personal information collected indirectly to enable them to exercise their privacy rights under the Act i.e., the right to request access to their personal information.
- It is important that changes to indirect collection of personal information protect and ensure that the information is used and shared appropriately, in line with the intended purpose for which the information was originally collected.
- A key factor to be considered is the potential for increased compliance costs for agencies handling personal information and doing business in New Zealand.
- Notification fatigue may lead to individuals feeling overwhelmed more so for vulnerable population groups such as those receiving support from mental health and addiction services.

2. What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?

- Individuals will know when their information is collected by indirect means and give the ability to question and control how their personal information is collected, used, and shared by different organisations.

3. What form do you think the proposed changes to notification rules under the Privacy Act should take?

- Proposed changes to notification rules under the Act should be legislated to ensure there are legally binding requirements placed on agencies or organisations who share an individuals information through indirect collection.

Please elaborate on your preferred option and explain why you think the other options are not appropriate.

- Introducing in the Act a new separate privacy principle dealing with notification of indirect collection is a preferred option. A standalone principle is likely to be clearer and easily understood in an Act which is already complex.

4. If you are a New Zealand business, are there any practical implementation issues you can identify in complying with the proposed changes?

- Refer to point one above – compliance costs and notification fatigue.

5. Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?

- No.

6. Should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?

- The proposed changes should apply to personal information collected indirectly from individuals overseas, and in New Zealand.

7. Is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback.

- N/A.

Conclusion

Thank you for the opportunity to comment on the possible changes to the notification rules under the Act. Whilst it is desirable to keep up to date privacy laws and best practices with other overseas jurisdictions, in order to support international trade and cross border flow of information, this must not weaken existing provisions in the Act which protect individuals' privacy rights, their dignity and autonomy, as it relates to health information.

If you have any questions, please contact Abigail Freeland, Policy Analyst, at s9(2)(a)

Ngā mihi,

s9(2)(a)

Memo Musa
Chief Executive

s9(2)(a)

Abigail Freeland
Policy Analyst

Privacy Commissioner
Te Mana Mātāpono Matatapu

Submission in response to the Ministry of Justice consultation on the broadening of the Privacy Act's notification obligations

1. The Ministry of Justice ("Ministry") has released its consultation paper, *'Possible changes to notification rules under the Privacy Act 2020'* ("Consultation Paper"). The Consultation Paper identifies several potential changes to the Privacy Act 2020 ("the Privacy Act") to address the lack of a notification requirement for agencies that do not collect personal information directly from the individual concerned ("indirect collection").

2. The potential changes the Ministry proposes are relevant to the Act's operation and the objectives of the information privacy principles ("IPP"). If implemented, they would contribute to enhancing the privacy of individuals and assisting individuals to exercise their privacy rights (including rights of access to and to request correction of their personal information). As such, I am pleased to make a submission setting out my views in support of this amendment.

The basis for the proposed changes

3. Subject to various exceptions, IPP 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:
   3.1. the fact that the information is being collected;
   3.2. the purposes for collection; and
   3.3. whether supplying personal information is voluntary or required by law.

4. The notification requirements do not apply at all where an agency does not collect personal information directly from an individual concerned.

5. The Ministry is considering ways to broaden the Privacy Act's notification requirements so that they apply not only when agencies collect personal information directly from the individual but also when personal information is collected indirectly. The Ministry believes these changes can promote and strengthen transparency, ensure New Zealand keeps up to date with privacy laws and best practices in overseas jurisdictions, and support international trade (specifically, the cross-border flow of personal information as a basis for digital trade).

Possible amendments to the Information Privacy Principles

6. Requiring transparency about how agencies collect, retain, use, and share individuals' personal information is a core function of any privacy framework. Transparency and openness is a precondition to individuals being able to exercise informed choices. The importance of transparency and openness is internationally recognised, for example, in the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* ("OECD Guidelines"). In fact, one of the Privacy Act's explicit purposes is to give effect to internationally recognised privacy obligations and standards, including the OECD Guidelines. For our purposes the most relevant part of the OECD Guidelines is the 'openness principle' which says:

> *There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.*

The 'collection limitation' also emphasises the importance of personal information being collected with the "[…] *knowledge or consent of the data subject*".

7. IPP 3 gives effect to the openness principle and serves a clear and important purpose as it currently stands. Nevertheless, we agree it should now be broadened to help increase transparency for individuals whose personal information is collected from other sources. Not only is transparency a precondition for individuals exercising informed choice but without it, individuals will have real practical issues exercising their rights of access (IPP 6) and to request correction (IPP 7) of their personal information. A broader IPP 3 notification obligation would also better align with the OECD openness principle objectives.

8. As for 'how' I support amending IPP 3 as the option that best meets the policy objectives. Theoretically, only minor adjustments to IPP 3's wording would be needed, making this amendment simpler for agencies to implement. This option also ensures that there is a seamless transparency obligation applying to agencies collecting personal information. The alternative options appear to be more complex to incorporate within the current structure of the IPPs and there may be a risk that some indirect collection would not be covered, therefore creating a gap. For instance, if the obligation is on the discloser under IPP 11, the discloser may be outside the jurisdiction of the New Zealand Privacy Act and

the notification obligation would not be triggered, despite collection by an entity within the ambit of the New Zealand Privacy Act.

9. I expect that some agencies may express reservations from a compliance costs standpoint. Agencies collecting personal information could well incur at least some extra costs from updating their systems. However, as the Ministry identifies in the discussion paper, there is scope to design IPP 3 in a way that ensures the obligation both effects the policy objectives but is also practical, and not unduly burdensome for agencies. My Office will be pleased to assist the Ministry in these matters.

Overseas best practice and international trade

10. I support the Ministry's efforts to achieve greater comity with our overseas partners including the United Kingdom, Australia, and the European Union Member States specifically on the matter of transparency best practice. As the Ministry identifies, a broadened notification obligation would also support international trade and in particular the cross-border flow of personal information as a basis for digital trade.

11. I am mindful that New Zealand is an outlier in not having notification requirements in situations of indirect collection. It is important that New Zealand's privacy law continues to provide a strong platform that will be recognised by our international trading partners. Otherwise, there is a risk that New Zealand businesses may incur other costs if our trading partners impose additional requirements. Having comparable privacy laws that meet internally recognised standards also helps in the negotiation of international trade agreements. The compliance costs therefore must be assessed against the broader national economic benefit of the proposed change.

Online & digital privacy

12. In 2010, the Law Commission considered the indirect collection issue as part of its Review of the Privacy Act 1993. But a lot has changed since 2010. Twelve years later, we live in a world in which personal information has greater economic value and business models relying on the collection, processing, and sale of personal information through websites and apps to diverse entities are now entrenched. Yet there is little transparency for individuals whose personal information may be indirectly collected.

13. A lack of transparency contributes to information and power asymmetries. It also negatively impacts individuals' ability to understand the privacy implications of taking certain actions online. The current lack of transparency may also be

contributing to the palpable sense of distrust around what personal information agencies in extensive data chains are collecting, and what they are doing with sometimes highly sensitive personal information. This distrust is particularly acute in the online environment where the use of tracking technology is both ubiquitous and opaque.

14. Ongoing technological change and the ever-increasing ability for agencies to share information widely and rapidly presents unique challenges, particularly in the online/digital environment. I do not expect that a broadened IPP 3 would be sufficient on its own to solve the many existing transparency and autonomy issues. Nonetheless, a broadened IPP 3 will be a critical platform for the work my Office is already undertaking to understand the extent to which further appropriate regulatory interventions may be necessary or desirable. It may be that these discussions lead to suggestions for further amendments to the Privacy Act in due course, to ensure this legislation remains fit-for-purpose for the digital age.

Conclusion

15. I support an amendment to broaden IPP 3 as the option that best meets the policy objectives of increased transparency and individual agency. This would also achieve greater comity with our overseas partners and support international trade. Furthermore, this amendment would provide a critical platform for the work my Office is already undertaking in the online/digital space.

16. Lastly, I welcome consultations with my Office who will be pleased to assist the Ministry as it considers these matters further.

s9(2)(a)

Michael Webster
Privacy Commissioner

Privacy Foundation NZ

30 September 2022
Privacy Feedback
Ministry of Justice
By email: privacyfeedback@justice.govt.nz

Tēnā koutou

Submission on Proposed Amendments to the Privacy Act

1. Thank you for the opportunity to submit on the proposed amendment of the Privacy Act 2020. The proposed amendment is to add a duty for an agency to notify a person if that agency collects personal information from a third party.

2. We have considered the proposed amendments and make these submissions.

Preliminary Comments

3. The proposal is intended to improve transparency. But these changes are also intended to maintain adequacy with overseas practise. The Privacy Foundation acknowledge that this second purpose is important. Harmonised laws mean New Zealand businesses have less difficulty trading overseas and help New Zealand maintain its international standing as a country that takes rights seriously.

4. Harmonisation is particularly important now because New Zealand has fallen behind international standards for data protection. Our Privacy Act 2020 markedly lags regulation in key trading partners, such as Australia, the United Kingdom, Japan, and member states of the European Union.

5. At a time of unprecedented technological change, it is imperative New Zealand has a modern privacy regime. This regime should protect New Zealanders, but also keep our international commitments. This includes our commitments in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the **OECD Guidelines**). The OECD Guidelines include the 'collection limitation principle' and 'openness principle', which are relevant to this proposal. These commit us to ensuring transparency about how people's personal information is collected, and the key role of knowledge and consent.

The Privacy Foundation's Response to Specific Questions

Question One: What factors do you think are most important when considering changes to indirect collection of personal information?

6. The Privacy Foundation raise these factors.

   6.1. First, a focus should be on improving meaningful notification and consent decisions. This focus should be guided by New Zealand's international commitments and New Zealander's expectations. These consent decisions are affected by the rapid technological change, and the structural power imbalance of consumers accessing online services from and through, large companies. The interactions often occur through take-it-or-leave-it contracts, which provide consumers limited choice. The changes should ensure people are provided with clear,

meaningful, timely and transparent information in relation to the collection of information about them.

6.2. Second, notification should be coupled with meaningful rights to decide what happens next. This should include expanding individuals' rights to control the use of their personal information, allowing them to restrict use of their personal information and request erasure, consistent with the General Data Protection Regulation (the **GDPR**). New Zealanders have limited privacy rights, compared to the GDPR and other modern regimes, particularly due to section 31 of the Privacy Act 2020. Without these rights, notifications will have limited practical use.

6.3. Third, any changes should also incorporate the principles of tikanga Māori and recognise the importance of Māori Data Sovereignty, including individuals having mana whakahaere over their personal information. Māori have a right to exercise control over Māori data and Māori data ecosystems, and there must be transparency as to which agencies hold Māori data. Broadening the notification requirements could better support this law.

6.4. Fourth, recently a significant volume of research has concerned 'dark patterns' and how design tools can be used to manipulate consumer decisions. The Privacy Foundation believe that notifications should be provided without undue complexity or manipulative measures. Care should be taken to consider whether express regulation of these techniques could be beneficial.

6.5. Fifth, any changes should also be set in clear, simple to apply, requirements to ensure agencies can meet their obligations without burdensome compliance costs. Elsewise, new compliance costs incurred by agencies will inevitably be passed on through increased prices for goods and services. Yet, as addressed below, harmonising our laws can reduce compliance costs on many businesses already operating overseas or looking to expand.

6.6. Sixth, while acknowledging the focus on maintaining adequacy, any changes should apply to New Zealanders, not solely to overseas individuals. This would improve privacy for New Zealanders, but also reduce a difficult compliance burden for agencies to decern to who the obligation applies. Doing so would follow modern views on transparency and collection principles, such as those New Zealand has signed up to through the OECD Guidelines.

6.7. Finally, it would be useful to understand New Zealand public's desire for these notifications. There is an acknowledged risk of notification fatigue in the consultation document. Further research could uncover public opinion about these notifications, and creative policy design could ensure harmony, while also improving privacy for all New Zealanders.

Question Two: What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies?

Advantages

7. The primary benefit would be the increase in transparency, and the reduction of 'invisible' data processing.[1] Broader notification requirements would also enable individuals to make privacy choices and exercise their privacy rights in circumstances where they may not have had a direct relationship with an agency holding their personal information. As noted above, these advantages would be augmented by the additional protection of privacy rights, consistent with a modern data protection regime. A secondary benefit would be the clearer picture agencies would be obliged to develop of from where their data comes. That is, to follow the broader notification requirements, agencies will need to have a complete picture of personal information flows, particularly in relation to personal information disclosed to, and received from, third parties. This might be viewed as a

[1] Data processing that happens when the individual is not aware that an agency holds their personal information, because the information was not collected directly from the individual.

compliance cost, but alternatively, it might be viewed as an opportunity to develop privacy maturity within many New Zealand agencies. Afterall, much of this awareness should already be developed to comply with existing obligations, even those dating back to the 1993 legislation.

8. Finally, we note the significant benefit of harmonising New Zealand's data protection laws with other markets. Uplifting New Zealand's privacy regulation is not only a direct good, but it could also reduce compliance cost for many agencies already required to comply with the GDPR or the UK Data Protection Act 2018. We are more than aware that many New Zealand businesses are already struggling under the burden of multiple regulatory regimes. Reducing the diversity of compliance obligations—or harmonisation— ultimately helps these agencies reduce compliance costs.

Disadvantages?

9. The clear disadvantage will be the increased compliance burden of the proposal. This cost can be reduced, by measures already addressed, and may be justified by research, such as that proposed in paragraph 6.7. Ultimately, however, the cost of compliance should be weighed against the substantial economic advantage offered by New Zealand's status as a country trusted for international data transfers and our strong tradition of the rule of law and rights protection.

Question Three: What form do you think the proposed changes to notification rules under the Privacy Act should take?

10. There is a case for organisations holding, or receiving personal information about overseas individuals being required to notify those people. Many organisations may already be equipped to do so because of the requirements of GDPR. The notification requirement could be added by a simple amendment of IPP3.

11. The indirect collection notice should contain the same information under IPP3. The agency should provide the indirect collection notice within a reasonable period after indirectly obtaining the personal information, and no later than a month, consistent with the GDPR and UK Data Protection Act 2019. There should be exceptions to the requirement to provide an indirect collection notice, for instance where the individual has already had access to the information (see below), public information or where any of the conditions in IPP3(4) apply.

12. There is a logical case for information which is publicly available being excluded from notification requirements. For example, there would be a significant compliance cost associated with notifying individuals any time information is accessed from the publicly accessible records, like Land Information New Zealand or the Companies Office. This is especially appropriate for areas contained in public registers. Afterall, personal information includes a broad range of matters that would not traditionally be considered private in any context. Whatever the change is, it should be consider the implications for the Unsolicited Electronic Messages Act 2007, which already covers some use of public details to contact people.

13. It should be considered whether the regulation should dictate not just the content, but also the form. This would help ensure the notifications remain meaningful, especially for children. For example, the GDPR provides that the information should be delivered "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child."

14. An alternative could be an amendment to IPP3(1)(c) to ensure that where an agency intends to disclose personal information to a third party recipient who will be using the information for their own purposes, the disclosing agency must name those third party recipients in their own privacy policy, and the disclosing agency must provide a means (for example, a URL) for individuals to access the third party recipient's information. This extension to IPP3 would cover both direct and indirect collection. But this would be an insufficient step to keep adequacy and do little to improve privacy for New Zealanders.

15. In any solution it will be necessary to consider collection of databases with high numbers of individuals, particularly with little personal information. In some of these examples, the agency would require more information, just to comply with the notification requirement. For example, a

marketing campaign may include thousands of addresses for the point of a single marketing message, and in such cases the compliance burden should not significantly outweigh the privacy risk. One solution could be to move the obligation to the disclosing agency, under a modification to IPP11.

16. The information could be provided in graphic form, such as standardised icons such as permitted by the GDPR.[2]

Question Four: If you are a New Zealand business, are there any practical implementation issues you can identify in complying with the proposed changes?

17. The Privacy Foundation is not a business.

Question Five: Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?

18. We see the following potential risks and mitigations:

Risk	**Mitigation**
Over-notification (notification fatigue) leading to a lack of meaningful notification by agencies.	Reducing the scope of agencies required to make notifications, such as noted in paragraph We agree that notification is unnecessary when the organisation already holds identical personal information on an individual and the person concerned is aware of that fact. Providing people with meaningful choices (privacy rights) would reduce the perception people are being provided meaningless notifications.
Complexity of the information that is provided.	Regulating the form of notifications, to support techniques such as simplifying and standardising notification.
Frustration from individuals who cannot do much with the notification received – particularly considering that there is currently no right to erasure or prohibit further processing of personal information when the individual no longer wants or needs a service.	Implementing privacy rights, enabling people to decide how their personal information is processed.
Unclear obligations on agencies, about "'any steps that are, in the circumstances, reasonable".	Clear statutory drafting and the use of examples or clarifying documents.

Question Six: Should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?

19. We do not consider that New Zealand law should offer individuals based overseas better privacy protections than that offered to New Zealanders living in New Zealand. Transparency is a foundational element of data protection and restricting the right would be a clear and bold departure from modern views of the transparency and collection limitation principles contained in the OECD

[2] See Art 12(7).

Guidelines. Taking that approach would fail to address what we understand to be the primary objective for this proposal; to close the transparency gap in relation to indirect collection.

20. Limited the proposal to offshore people would also squander the opportunity to protect New Zealanders from offshore businesses, doing business in New Zealand, who are known to collect large volumes of personal information through third parties.

21. There are also clear practical challenges with defining that someone is 'based overseas' and distinguishing those people within agencies' data repositories. This distinction would place an unclear and complex compliance burden on agencies. We acknowledge that restricting the broader notification requirements to personal information collected indirectly from individuals overseas would mean businesses operating exclusively domestically should not face any further compliance costs.

22. In any instance, if a New Zealand based agency is already undertaking indirect collection of personal information individuals based overseas, they may already have to comply with overseas laws relating to indirect collection. For example, if a New Zealand based agency indirectly collects information about an individual based in the EU and does so as a Controller, the New Zealand based agency may already have to comply with the indirect collection requirements due to the GDPR. A change to New Zealand law is not needed to give effect to that, because of the extraterritorial provisions of the GDPR.

Question Seven: Is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback.

23. If the proposal is to progress, a great deal of care should be taken regarding the principal-agent relationships and where the obligation belongs.

Conclusion

Thank you again for the opportunity to submit on this proposal.

24. This submission was compiled on behalf of the Privacy Foundation by Louisa Joblin and Kent Newman on the basis of the insights from the members of the Foundation's Working Group on Legislation and Regulatory Reform

25. Contact for any queries: info@privacyfoundation.nz

Best wishes,

Dr Marcin Betkier
Chairperson, Privacy Foundation New Zealand

Property Brokers

29 September 2022

Electoral & Constitutional Team
Ministry of Justice
Via email: privacyfeedback@justice.govt.nz

To whom this may concern.

PROPOSED CHANGES TO NOTIFICATION RULES UNDER THE PRIVACY ACT 2020
Submission in support of REINZ submission

1. Property Brokers Limited is a member of the Real Estate Institute of New Zealand (REINZ), a membership organisation supporting the real estate profession across New Zealand. Our business covers all spectrums of real estate, residential, rural, lifestyle, commercial and property management.

2. REINZ has lodged a submission in respect of the above consultation currently underway.

3. With over 90 branches, predominantly in provincial New Zealand, many of our branches require this data to provide a transparent market analysis which we are legally required to do. Delaying this data will cause significant disruption and will compromise the integrity of the sale process for our clients and customers.

4. Market trends and analysis need to be provided in real time, as a shifting market does not allow for delays in data to ensure a transparent and fair sale process.

5. The data is accessed often and frequently, therefore the logistics of providing notification to respective parties on each occasion would be impossible to maintain. A single source of notification must be our preferred method in achieving both compliance with the law and fairness to both customers and clients. This is covered adequately under our current documentation and processes. For the client, our agency agreement states the following:

13.0 Authority to Use Property Information

13.1 The Agent is committed to compliance with all applicable laws, including privacy and copyright laws. The Client confirms that it has obtained all necessary authorisations (including under privacy law) to allow the collection, storage, use and disclosure of information (including information about an identifiable individual ("Personal Information")) pertaining to the Property for the purposes of:

13.1.1 the Agent's marketing and promotional activities;

13.1.2 listing the Property on real estate and property listing websites (including the Agent's website and third party websites); ..

13.1.3 collating and sharing property information for research, reports, statistical analysis, and other purposes, including in particular sharing listing and sales data with the Real Estate Institute of New Zealand Inc ("REINZ") for inclusion in the aggregated databases, reports and materials made available by REINZ to people in the real estate industry and others;

13.1.4 generating and publishing sales and other reports (whether generated by the Agent, REINZ or by any third party accessing such information); and

13.1.5 and any related purposes.

6. This is also covered for both client and customer under clause 21.0 Collection of Sales Information in the ADLS Sale & Purchase Agreement.

7. We take confidentiality very seriously to the extent that we have processes in place for either party requiring a confidential sale or purchase. This data is not released to any third party whatsoever.

8. We believe that the aforementioned clauses, and our processes of the licensee explaining these clauses to the relevant parties, more than covers the requirement under the Privacy Act.

9. We wholeheartedly support REINZ's submission and note that we are able and willing to participate in direct member feedback sessions as suggested by REINZ, if this would be of use to MOJ.

Please do not hesitate to contact me should you have any queries in respect of this submission

Yours sincerely

s9(2)(a)

Guy Mordaunt
MANAGING DIRECTOR

30th September 2022

Electoral and Constitutional Team

Ministry of Justice
By email only: privacyfeedback@justice.govt.nz

PROPOSED CHANGES TO NOTIFICATION RULES UNDER THE PRIVACY ACT 2020

Submission in support of REINZ submission

1. Ray White Real Estate is a member of the Real Estate Inst tute of New Zealand (REINZ), a membership organisation supporting the real estate profession across New Zealand. Our salespractice is focused primarily on the sale of residential properties.
2. REINZ has lodged a submission in respect of the above consultation currently underway.
3. As outlined by REINZ in their submission, we are dependent on the availability of data on recent home sales to discharge our legal obligations to clients under the Real Estate Agents Act.
4. As the sales market can move with considerable speed, the availability of the REINZ data series is crucial to our ability to provide clients with an accurate assessment of the value of their home – as is our legal obligation as real estate agents.
5. Changes that delay or make this data unavailable would have ramifications for the quality of the service we are able to provide to consumers.
6. We wholeheartedly support REINZ's submission and note that we are able and willing to participate in direct member feedback sessions as suggested by REINZ, if this would be of use to MoJ.

Please do not hesitate to contact the writer should you have any queries in respect of this Submission.

Yours sincerely
Ray White Real Estate Limited Licensed (REAA 2008)

s9(2)(a)

Treena Drinnan
Chief Agency Officer

Ray White New Zealand
Level 2, 12 Viaduct Harbour Avenue
PO Box 6067, Victoria Street West
Auckland
09 377 5069
corporate.nz@raywhite.com

The voice of real estate

REINZ
REAL ESTATE INSTITUTE OF NEW ZEALAND

30 September 2022

Electoral and Constitutional Team
Ministry of Justice

By email only: privacyfeedback@justice.govt.nz

REINZ SUBMISSIONS: PROPOSED CHANGES TO NOTIFICATION RULES UNDER THE PRIVACY ACT 2020

Executive Summary

1. The Real Estate Institute of New Zealand Incorporated (**REINZ**) is a membership organisation with more than 17,000 members. REINZ represent approximately 97% of the real estate profession across New Zealand. Our members span the breadth of real estate services, including residential sales, rural/lifestyle sales, auctioneering, business broking, commercial and industrial sales and leasing, and property management.

2. Thank you for the opportunity to submit on behalf of both REINZ and our members on the proposed changes to the notification rules under the Privacy Act 2020 discussed in the Ministry of Justice's (**MoJ**) Engagement Document released in August 2022. Whilst REINZ supports the MoJ's desire to promote and strengthen transparency around the collection, use, and disclosure of personal information, REINZ does not support any change to the Information Privacy Principles (**IPP**) under the Privacy Act which would prevent REINZ and our members from collecting sales data (which may contain limited personal information) in the way REINZ and the real estate profession does currently.

3. REINZ appreciates that the Government is putting in considerable effort to retain New Zealand's EU adequacy status and acknowledges the work by MoJ in this space. However, REINZ strongly cautions that reform can have unintended adverse consequences where it is not subjected to sufficient rigour.

4. REINZ and our members are **strongly opposed** to any change to the status quo. However, if there is to be a change, Option 1 is preferred (i.e. an extension of IPP 3 to cover indirect collection)

5. Below we discuss how property sales data is collected and used, how the privacy principles are satisfied currently, and why no change to the notification regime is needed or warranted. We also explain the important role REINZ plays in providing timely sales data to the real estate profession, and the critical role this sales data plays in keeping Government, economists, government departments and the wider public informed of changes to the property market in New Zealand. Any change to the status quo risks losing this.

PO Box 5663, Victoria St West, Auckland 1142, New Zealand
FP: 0800 473 469 I T: +64 9 356 1755 I F: +64 9 379 8471 I W: www.reinz.co.nz

Background

6. To understand REINZ's position and that of its members and others who rely on the data that REINZ collects and disseminates, it may be useful for the MoJ if we outline a typical real estate transaction from a data flow perspective:

    a. A vendor who wishes to sell their property approaches a member agent and decides to list the property with that agent.
    b. The agent enters into a listing agreement with the vendor pursuant to which it collects personal information concerning the property, chattels to be included in the sale, and the vendor's instructions for the sale of the property (e.g., how it is to be sold, standard contractual sale, auction, tender, proposed date of settlement etc) and other information necessary for the agent to market and sell the property on behalf of the vendor.
    c. At the same time, the agent is required under the Real Estate Agents Act 2008 and Rule 10.2 of the Real Estate Agents Act (Professional Conduct and Client Care) Rules 2012 under that Act to provide the vendor with a current market appraisal (CMA). The CMA must give the vendor the most up to date information available about the prices at which comparable properties (usually in the same area) have sold.
    d. As soon as the property sale becomes unconditional, the agent is required to provide the property address, sale price and date of agreement to REINZ (unconditional sales data).
    e. REINZ includes that information in its database and uses it to provide data to others. For example, the above unconditional sales data would be included in a CMA provided to a vendor of a similar nearby property, as required under the rules referred to above.
    f. Once the property sale settles, the vendor (usually via its solicitor) must provide full details of the address, sale price, date of settlement and the purchaser's details to the local authority which make that information publicly available. The transfer between the vendor and the purchaser is also registered by Land Information New Zealand on the title to the property, which is also publicly searchable.

7. REINZ and the Auckland District Law Society (**ADLS**) jointly own the copyright in the ADLS/REINZ standard form agreements used to transact almost all sales and purchases of land and buildings, and many sales of businesses across New Zealand. Both the standard form agreements and the agency listing agreement between the agency and the vendor grant REINZ members authority to submit the above data to REINZ for property appraisal, market analysis etc (see below for further detail).

8. REINZ is over 100 years old, and we have been providing data driven products and insights to real estate members and others since 1986. REINZ is a kaitiaki (guardian) of property sales data for the benefit of real estate professionals, but also New Zealanders more broadly. REINZ ensures any personal information it receives within the sales data is protected and respected appropriately.

9. REINZ uses sales data to power digital products for members, including:

    a. a current market appraisal tool enabling real estate professionals to meet their legal obligations referred to above;
    b. an automated valuation model; and
    c. statistics platform, which enables the provision of market insight reports, analytics etc.

10. REINZ ensures there are appropriate contractual and other protections around what data is shared with members and any other recipients, and exactly what unconditional sales data (discussed immediately below) can be used for, how it must be stored and so forth. Terms imposed on recipients include requirements to advise REINZ of any data breach and comply with REINZ's instructions with respect to notification to affected individuals and the Privacy Commissioner.

11. As noted above, the sales data REINZ obtains indirectly via REINZ members contains a limited amount of unconditional sales data (address, sale price and date of agreement). On average, the period between an agreement for sale and purchase becoming unconditional and the sale settling is approximately 6 weeks, after which point the information becomes publicly available. This unconditional sales data is collected securely and closely guarded It is only shared with members or their approved service providers, with appropriate contractual protections and controls in both cases.

12. REINZ's view is that it is not collecting personal information, or at least if it is, then it is not intentionally doing so. It is not interested in identifying particular property owners, past or present. Its data tools are aimed at aggregated data analytics and to enable its members to comply with their agency obligations.

13. REINZ recognises, however, that in some cases merely knowing an address, when combined with other information it may have derived from other publicly available data sources, could identify a property owner. However, this in fact is the same for anyone. Anyone is able to identify a property owner simply by searching local authority records and LINZ records. In some cases, therefore, an address may be personal information and in other cases it is not. It depends what other information REINZ or any other recipient has which enables the address to be matched to the owner.

14. This is highly relevant to this consultation since, if the information supplied to REINZ and then by REINZ to others, is personal information in the recipient's hands, an extension of the obligation to notify would catch all recipients in the above chain of disclosure – first REINZ, then an agent which includes the address in the CMA and even the agent's vendor client that is provided with that CMA. The latter is perhaps not as far-fetched as it sounds. If a vendor at no. 10 High Street sells and two weeks later their neighbour at no 12 lists their property, the CMA given to no. 12's vendor will almost certainly include details of no. 10's sale price, i.e., personal information about the owner of no. 10.

15. REINZ is not alone in collating publicly available information about properties and providing it to agents and other organisations. Some other data providers even provide this information to members of the public. Unlike many others, REINZ, however, collects unconditional sales data since it needs to be able to make this available to members so that they can provide **current market appraisals.**

16. In addition to providing property information to its members, REINZ is a trusted source of property market insights and statistics which are regularly provided to banks, economists, Government departments, regulators and to the public (see our latest press release and REINZ monthly property report). REINZ has a House Price Index built in conjunction with the Reserve Bank of New Zealand, which provides a more accurate observation of market value than median or average house prices. *Note:* No personal information is contained in our market insights and statistical reports. Market trends are displayed using aggregated/non-identifiable data.

17. REINZ fully complies with the Privacy Act and IPP in collecting sales data indirectly from our members. To briefly summarise:

    a. REINZ collects limited personal information for a lawful purpose;
    b. REINZ collects limited data (which may be personal information) indirectly because it is not possible/practicable for REINZ to collect it directly from vendors and purchasers;
    c. REINZ ensures the individuals concerned have consented to/are aware their data is being collected and provided to REINZ;
    d. The limited personal information we may receive becomes publicly available within approx. 6 weeks in any event;
    e. The individuals concerned are able to refuse to provide their information to REINZ, in which case the unconditional sale is suppressed until the sale settles and this information becomes publicly available;
    f. Individuals can ask REINZ whether their information is being held and request correction (or deletion) of any personal information;
    g. REINZ does **not** request or retain contact details for vendors and purchasers who are party to all the individual sales transactions across the country every day (and has no interest in this information);
    h. It would be literally impossible, let alone impracticable, for REINZ to notify every individual that it has received their sales data;
    i. Equally it would be impossible for our members (as the disclosing parties) to notify all individuals that their information has been disclosed to REINZ. For instance, in the past 12 months (for the year ending 31 August 2022), our members sold approximately **85,000** residential and rural properties; and
    j. Furthermore, it would not be possible for recipients of data from REINZ to notify the individuals concerned even if the data could be characterised as personal information of those individuals.

18. Vendors are aware that the information will be used, and have consented to its use:

    a. to effect a sale of their property;
    b. to be supplied to REINZ for use by its members and others in the property industry and for statistical and analytical purposes. The data is not used beyond that to our knowledge and our contracts with recipients very strictly confine use to specific purposes consistent with that collection consent. If a vendor was concerned at the use of its data, it would no doubt complain to its agent and the agent would complain to REINZ. REINZ would then be able to take the matter up with the recipient in question, likely as a contractual issue.

19. Similarly, if a property owner initiates an access request, and that comes through to REINZ, if REINZ is able to identity the affected individual, it would be able to respond to that request.

20. For these reasons, as a significant indirect recipient of data, REINZ has difficulty seeing that there is an issue which needs addressing in the New Zealand context, despite overseas initiatives.

MOJ Engagement Document

21. In MoJ's Engagement Document, the Ministry has posed several questions. Our submissions focus on Questions 3 and 4:

    a. ***Question 3.*** *"What form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate?"*

    b. ***Question 4.*** *"If you are a New Zealand business, are there any practical implementation issues you can identify in complying with the proposed changes"*

22. Below is a table summarising REINZ's position on the four options the MoJ has proposed in the Engagement Document. REINZ is very interested in being closely involved in the consultation. We would be very happy to facilitate members' feedback on the proposal directly to the MoJ (we suggest a workshop so that the MoJ can hear from our members directly).

	Proposed changes to notification regime	REINZ's position
1	***Option 1:*** *Broadening the notification regime under IPP 3 so that it no longer applies only when an agency collects personal information directly from the individual concerned - but also when an agency collects personal information indirectly from other sources.*	**We are not persuaded there is a problem that needs fixing. We are therefore strongly against any change. However, if a change is to be made to the notification regime for indirect collection, REINZ and our members prefer this option,** provided a similar approach to indirect notification is taken to that in Australia.

2	***Option 2:*** *An amendment to IPP 2 to narrow exceptions that allow agencies to collect information indirectly.*	**REINZ opposes this option**. REINZ relies on exceptions under IPP 2 to collect sales data indirectly. Depending on which exceptions are narrowed, this would have significant implications for REINZ and our 17,000+ members.
3	***Option 3:*** *An amendment to IPP 11 to require the disclosing agency to notify the individual concerned that their information has been disclosed to a third party.*	**REINZ opposes this option.** The administrative cost and burden required to notify each individual once their limited personal information has been passed on to REINZ (or their approved services provider, AML provider etc) would be an extraordinary burden on the real estate sector, especially those who are sole independent agents or small agencies.
4	***Option 4:*** *Introducing a new privacy principle.*	**REINZ does not have enough information to assess this option**. Once more information is provided, consultation would be required so that we can assess the implications for REINZ and our members.

How REINZ collects information and satisfies the current privacy principles

23. REINZ is authorised to collect sales data from its real estate members. This means that once an agreement for sale and purchase between a vendor and purchaser has all its conditions met, unconditional sales data may be provided to REINZ. Names and contact details for vendors and purchasers are not provided to REINZ – just address, sale price and date of agreement as discussed in paragraph 8 above. This sales data, enriched by other publicly available data sources (such as council sales and property data, LINZ address and title data etc) powers REINZ's digital products.

24. REINZ ensures, in line with IPP 3, that when a member is collecting information from the individual, that all reasonable steps are taken to ensure that the individual is aware their information is being collected, the purpose for which it is collected, and all elements under IPP 3 are satisfied, even though it is likely in our view that the information supplied to us is not personal information. For instance:

    a. In the ADLS/REINZ standard form agreements, vendors and purchasers agree to the collection of sales information and provision to REINZ (this is clause 19 in the current 11th edition (2) of the sale and purchase agreement) reproduced below:

19.0 Collection of Sales Information

19.1 Once this agreement has become unconditional in all respects, the agent may provide certain information relating to the sale to the Real Estate Institute of New Zealand Incorporated (REINZ).

19.2 This information will be stored on a secure password protected network under REINZ's control and may include (amongst other things) the sale price and the address of the property, but will not include the parties' names or other personal information under the Privacy Act 2020.

19.3 This information is collected, used and published for statistical, property appraisal and market analysis purposes, by REINZ, REINZ member agents and others.

19.4 Despite the above, if REINZ does come to hold any of the vendor's or purchaser's personal information, that party has a right to access and correct that personal information by contacting REINZ at info@reinz.co.nz or by post or telephone.

b. In REINZ's standard real estate agency listing agreement template there is a standard clause covering collection of personal information by the real estate professional and the provision of sales data (including personal information, if any) to REINZ. That clause is reproduced below:

Authority to use property information

1. *The Agent is committed to compliance with all applicable laws, including privacy and copyright laws. The Client confirms that it has obtained all necessary authorisations (including under privacy law) to allow the collection, storage, use and disclosure of information (including information about an identifiable individual ("**Personal Information**")) pertaining to the Property for the purposes of:*

    a. *the Agent's marketing and promotional activities;*
    b. *listing the Property on real estate and property listing websites (including the Agent's website and third party websites);*
    c. *collating and sharing property information for research, reports, statistical analysis, and other purposes, including in particular sharing listing and sales data with the Real Estate Institute of New Zealand Inc ("**REINZ**") for inclusion in the aggregated databases, reports and materials made available by REINZ to people in the real estate industry and others;*
    d. *generating and publishing sales and other reports (whether generated by the Agent, REINZ or by any third party accessing such information); and*
    e. *any related purposes.*

25. In the event that we are collecting personal information, REINZ relies on a number of exceptions under IPP 2 to collect any personal information indirectly, including a belief on reasonable grounds:

    a. that non-compliance would not prejudice the interests of the individual concerned;
    b. that the individual concerned authorises collection of the information from someone else;
    c. that the information is (or becomes) publicly available information;
    d. that compliance is not reasonably practicable in the circumstances of the particular case;

e. that the information will not be used in a form in which the individual concerned is identified; and/or
f. that the information will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

26. In our submission, no change is required to the notification regime for New Zealand (however see our discussion of Option 1 from paragraph 25below). To notify every vendor and purchaser in New Zealand that their data *has in fact been shared* indirectly with the previously authorised party (REINZ) is unnecessary and will lead to angst, notification fatigue and enormous wasted resources. Further, as noted above, if this type of regime were strictly applied, the vendor might then receive a notification from REINZ, then from an agent that has included the sale details in another CMA and then, in theory, from another vendor who has been given that CMA. With respect, we cannot see what that achieves and clearly it is not possible for anyone in that chain to effect such notification in any case. No one has sufficient details of the original vendor to do so. We should note here that the original vendor will have shifted to a new property and that information may not be available even to the original agent, let alone REINZ or others in the chain. More importantly, REINZ does not have the ability to contact all the vendors and purchasers in New Zealand to notify them that REINZ has received their sales data in accordance with the signed agency agreement and signed sale and purchase agreement. **Where a person has previously authorised the sharing of their information, whether directly or indirectly, to a named person (in the legal sense) or a class of persons, there should be no further obligation to notify that person every time their information has in fact been shared with the named person or class of persons.**

27. However, if a change is to be made, we discuss below the four options proposed by MoJ in the Engagement Document for changing the notification rules.

Option 1 – Fallback option if a change must be made

28. Option 1 involves extending the notification regime under IPP 3 so that it applies when an agency collects personal information indirectly.

29. If a change is to be made to the notification regime for indirect collection (and we reiterate that we are against this), REINZ and our members prefer this option, provided the exceptions remain available/a similar approach is taken for indirect notification to Australia. Clear guidance and examples will be necessary to show the threshold of what is satisfactory notification for indirect collection of personal data in New Zealand.

30. We understand Australian Privacy Principle (APP 5) requires an APP entity that collects personal information about an individual to take reasonable steps to notify the individual of certain matters or to ensure the individual is aware of those matters. Australian guidance on what 'reasonable steps' should be taken in collecting personal information is helpful and could be tweaked for the New Zealand context.

31. This APP 5 requirement for collection of personal information applies to all personal information 'collected' about an individual *either directly or indirectly*. Under the guidance provided by the Australian Government, an APP entity can satisfy the requirements of APP 5 if the original entity collecting the personal information has given notice of the relevant matters on behalf of the entity indirectly collecting the personal information, for instance by contractual arrangement.

32. Article 14 of the EU General Data Protection Regulation also requires the data controller ('agencies' under the Privacy Act 2020) to provide the data subject with certain information.

33. We agree that an individual should be aware their personal information will be processed, regardless of whether it is collected directly or indirectly. This option would also avoid the issue of notification fatigue.

34. REINZ and our members would support IPP 3 being extended to cover indirect notification provided the various exceptions remain available/ APP 5 is followed.

Option 2 - Not viable

35. REINZ and our members oppose option 2, which would narrow the exceptions under IPP 2 which enable the collection of information indirectly. REINZ relies on IPP 2 exceptions as discussed in paragraph 22 above. Narrowing the exceptions is likely to have significant implications for REINZ and our 17,000+ members. We do not believe narrowing the exceptions is the right approach.

36. We also note that Australia's APP 3 also has a list of acceptable exceptions.

Option 3 - Not viable

37. Option 3 proposes an amendment to IPP 11 to require a disclosing agency to notify the individual concerned that their information has been disclosed to a third party.

38. REINZ and our members oppose this option. As we note above, there are a number of recipients in the chain. The administrative cost and burden required to notify each individual once their personal information has been passed on to REINZ (or their approved services provider, AML provider etc), other agents or users of REINZ data and then their vendor clients, would be an extraordinary burden on the real estate sector, particularly independent agents and small agencies. It would also lead to vendors and purchasers suffering notification fatigue and angst with unwanted emails.

39. Notification after the fact is unnecessary in our view in circumstances where the individual has already consented/is on notice that their information will be shared with a named person (in the legal sense) or class of persons. The information cannot be used for any purpose beyond that which was consented to. We prefer option 1 above.

The voice of real estate

REINZ
REAL ESTATE INSTITUTE OF NEW ZEALAND

Option 4: Introducing a new privacy principle

40. Option 4 will require clarification by MoJ. Until we know what is proposed and have an opportunity to consider the implications with our members, we are unable to assess this option.

41. The Engagement Document discussed potentially confining broader notification requirements to personal information collected indirectly from individuals overseas. REINZ does not manage or collect personal information from individuals overseas and accordingly, does not take a position on whether any change should be confined to personal information collected indirectly from individuals overseas.

Conclusion

42. Overall, REINZ supports this review of the notification regime for indirect collection of personal information under the Privacy Act 2020. REINZ appreciates that the Government is putting in considerable effort to retain New Zealand's EU adequacy status.

43. However, REINZ strongly cautions that reform can have unintended adverse consequences where it is not subjected to sufficient rigour. We are not persuaded there is any need to change the status quo, but if there is to be a change, Option 1 is preferred (i.e. an extension of IPP 3 to cover indirect collection).

44. REINZ has a very important role to play, not just in terms of the provision of sales data to assist our 17,000+ members, but as the most reliable source of property data because of the unconditional data in particular, we also play a very important role in keeping the public abreast of movements in the property market and it enables us to keep Government, economists and other key commentators informed. REINZ also plays a key advocacy role supported by statistical data. REINZ does not support any change to the privacy principles which would prevent REINZ and our members from collecting sales data in the way REINZ and the real estate profession does currently and the using it to comply with agent and other obligations.

45. REINZ would be very keen to engage closely with the MoJ on this. We could facilitate member feedback direc to MoJ in the same way we did with the AML/CFT statutory review.

46. Thank you for the opportunity to make a submission on behalf of REINZ and our members. If the Electoral and Constitutional Team have any questions, please direct them to mbeight@reinz.co.nz.

Yours sincerely

s9(2)(a)

Melisa Beight
General Counsel

PO Box 5663, Victoria St West, Auckland 1142, New Zealand
FP: 0800 473 469 I T: +64 9 356 1755 I F: +64 9 379 8471 I W: www.reinz.co.nz

SUBMISSION

Broadening the Privacy Act's notification rules

September 2022

Restaurant Association of New Zealand submission to Electoral and Constitutional, Ministry of Justice

(09) 638 8403
info@restaurantnz.co.nz
Restaurant Association of New Zealand
45 Normanby Rd, Mt Eden
Auckland 1024

Executive Summary

The Restaurant Association believes that all hospitality patrons should feel safe in knowing their private information is being protected to the highest standards. We are also acutely aware that the hospitality industry is deeply interconnected internationally through the use of bespoke reservations and CRM software which is why we are supportive of the Government's efforts to align our privacy frameworks with those of other jurisdictions—particularly those with which we have strong business and trade relationships.

Relationships have always been at the heart of the success of our restaurants and cafés as integral parts of our communities, so we believe that in the age of the digital economy, robust privacy measures are crucial to strengthening trust between businesses and customers.

While we support the principles behind the proposed changes to information sharing requirements, we are concerned these changes have the potential to drastically increase the administrative burden on small and medium sized businesses in New Zealand, of which many of our businesses are.

The Restaurant Association would welcome the opportunity to work with officials to establish a framework which would protect consumers and ensure that all businesses operating in the digital economy are aware of their duty to protect the data of their patrons.

As such, the Restaurant Association makes the following recommendations:

- **Recommendation 1**: that any changes or new requirements - particularly for small businesses—must be as simple and cost-neutral as possible
- **Recommendation 2**: of the options provided, the Association recommends the implementation of a new IPP requirement
- **Recommendation 3**: that the amendment contain an exemption for small businesses
- **Recommendation 4**: that should indirect notification be required - that Government provide adequate resources, tool kits, and education campaigns to aid hospitality businesses to come into compliance
- **Recommendation 5:** that the draft amendment be circulated for consultation.

Introduction

1. The Restaurant Association of New Zealand (the Restaurant Association) welcomes the opportunity to make a submission on the potential changes to the notification rules for collecting personal information under the *Privacy Act 2020*.

2. While we support the intent of the proposed changes to the *Privacy Act 2020* (the Act) we are concerned about the disproportionate impact these changes will have on our small and medium-sized businesses.

3. We believe that transparency in the collection, use, and disclosure of personal information is fundamental to protecting individuals' privacy rights as well as their dignity and autonomy—particularly as the evolution of business models and technology in the past few years has seen a rise in the indirect collection of personal information.

4. We also appreciate the Government's efforts to align our privacy framework with those of our international counterparts, especially the European Union, to preserve Aotearoa New Zealand's international credibility.

5. Although supportive of the principles behind these proposed amendments, we are concerned these changes have the potential to drastically increase the administrative burden on small and medium sized businesses across New Zealand.

6. It is important for the Government to keep in mind the direct and indirect impacts of the pandemic on many industries when developing or amending legislation - in particular those sectors that are still recovering from the pandemic, such as hospitality and tourism.

Timing

7. Acknowledging the pandemic has also thrown the Government's legislative agenda off course, we put on record our concern at the rate and pace of legislative change currently being advanced.

8. Despite the Act being less than two years old, feedback is once again being sought on proposed privacy-related changes. This sits alongside the sweeping legislative reforms across both employment and immgration, compounding the pressure felt by many sectors.

9. For a sector that is currently walking a tightrope between recovery from the pandemic and ensuring long-term sustainability, the short turn-around times for consultation on extremely complex topics—that are not immediately relevant to our sector—is often out of touch with the realities of running a business.

10. Within our membership, many businesses are constantly adapting their operations to meet ever-evolving compliance standards in light of the rapid and drastic changes that have occurred in the privacy space over the past two years.

11. The Hospitality sector is doing all it can to ensure a just, sustainable recovery from the impacts of COVID-19 with the already limited resources at its disposal.

12. With severe time, resource, and staff shortages, we implore the Government to adopt a pragmatic approach to changes of these kinds, prioritising only those changes or new requirements for the private sector that are as simple and cost-neutral to implement as possible—particularly for small business.

Question 1 - What factors do you think are most important when considering changes to indirect collection of personal information?

13. The Association submits that the most pertinent considerations regarding changes to indirect collection of personal information are:

    - increased ***administrative burden*** on hospitality businesses
    - significant ***compliance costs*** at a time where business remain time and resource strained, and
    - potential ***customer fatigue*** related to online third-party platforms bombarding users with privacy related notifications.

Increased administrative burden and compliance costs:

14. The majority of the hospitality sector would fall into the 'small' category of business if defined by the proposed revenue scale of <$20m.

15. Given the natural limits on small businesses regarding their capacity and available resources, we maintain that the government should make it as simple as possible to comply with any proposed amendments to the *Privacy Act 2020*.

16. Throughout our recovery from the pandemic, hospitality businesses have also faced record-high levels of inflation, and a rapidly changing legislative environment that increasingly demands more of them.

17. It is no secret that the hospitality industry has undergone drastic changes since COVID-19 arrived on our shores. Business owners have become increasingly reliant on the digital economy, in order to meet shifting customer behaviours and ensure continued trade during COVID-19 restrictions.

18. Furthermore, for hospitality businesses, data collection is a critical tool for business growth, development, and the improving customer experience.

19. Hospitality owners often rely on multiple third-party platforms for taking online bookings, orders and deliveries. For example, there are a range of SaaS softwares (such as Quandoo, Restaurant Hub and Kitomba) used by a range of hospitality businesses in New Zealand to make table reservations and place online orders, where the details provided by patrons are stored (where permitted) by the third-party booking system, and not by the business in question.

20. Some larger hospitality businesses may receive and store these details themselves in their own CRM, but where this is the case, these are usually businesses of a size that there are staff—either employed directly or contracted as part of an external agency—with the sole responsibility for communications functions.

21. Therefore, the requirement to notify customers of indirect data collection would come with a disproportionate administrative burden and compliance cost to smaller hospitality businesses.

22. If information sharing of this kind within the broadening of Privacy Act's notification rules, we recommend that the Government support the development of opt-in software integrations be explored as a first step to prevent additional administrative requirements of small business owners and operators. An example of this working well in recent years was the approach taken by Inland Revenue Department (IRD) to integrate the Xero and MYOB payroll systems into IRD payday filing.

23. In the end, if regulatory burdens on micro-SMEs are too high, consumer safety will not improve in practice. It is therefore essential that any changes or new requirements for the private sector—particularly for small businesses—must be as simple and cost-neutral as possible.

Customer fatigue:

24. As referenced in page three of the Ministry of Justice's consultation document, an important consideration when proposing changes to the current notifications requirement under the *Privacy Act 2020*, is the potential for notification fatigue - resulting in individuals feeling simply tuning out rather than trying to understand how their personal information is being collected.

25. Although the consultation document highlighted the impact notification fatigue can have on individuals it failed to recognise the impact it will have on businesses.

26. The hospitality industry uses many external services in its operations, so consumers may come across several different privacy notifications when engaging with a hospitality business online platforms.

27. As a result, patrons may feel discouraged from engaging with these platforms due to notification fatigue, which would be detrimental to our sector's recovery. Ensuring that future requirements do not force businesses to bombard consumers with notifications to the point of preventing online utility must be a top priority.

Question 2 – What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?

28. The Association believes broadening New Zealand's notification requirements could be advantageous on two key fronts.

29. The first is that these changes would align us with many of our international counterparts who have already adopted similar legislative reforms which would strengthen the cross-border flow of information and in turn, New Zealand's position in the international digital economy.

30. The second is that the continued rise of misinformation and disinformation, protecting users' through robust privacy law and data sovereignty is important. However, this should not come at the expense of the business.

31. At the same time, the advantages must be balanced with the additional administrative requirements of companies who only operate domestically and may not be as well resourced to implement these changes. These include:

- financial cost of compliance
- significant administrative and time burden on small businesses
- customer notification fatigue and aversion to engaging in online platforms

- small businesses may be subjected to complaints simply for lacking the knowledge and resources to make their operations compliant with the Act.

Question 3 - What form do you think the proposed changes to notification rules under the Privacy Act should take?

32. The Restaurant Association submits that these changes would be best placed in the form of a new Information Privacy Principle (IPP).

33. In the hospitality context, details provided by patrons are stored (where permitted) by the third-party booking system, and not by the business in question. As a result, extending IPP3[1] may be impractical.

34. Furthermore, businesses will be required to implement even longer privacy notices, which users are less likely to read. It would be unlikely to give individuals any more autonomy over their own data.

35. Similarly, amending IPP11[2] would merely cause significant administrative workload for already spread out small business who often utilise multiple downstream service providers in their operations.

36. The consequence would be that businesses with direct relationships with individuals would have to continuously update their privacy notices whenever they swap or work with new downstream service providers - to the determinant of their revenue and time.

37. Moreover, amending IPP2[3] may significantly affect the routine processing of data - a critical aspect of contemporary hospitality operations whose operations depend heavily on data exchanges.

38. The Restaurant Association submits that for the purpose of clarity and accessibility, a new IPP principle[4] would be the best step forward. However, for the new principle to be equitable and effective in practice—it is essential that stakeholders are adequately consulted.

39. Furthermore, the Restaurant Association submits that a new IPP principle should include an exemption for small businesses. While not provided for in the European

[1] From MoJ Consultation Document: *'an amendment to IPP 3 to introduce a notification requirement for all agencies covered by the Act. IPP 3 would be broadened so that it no longer applies only when an agency collects personal information directly from the individual concerned. It would apply when the agency collects the personal information indirectly from other sources'.*
[2] From MoJ Consultation Document: *'an amendment to IPP 11 to require a disclosing agency to notify the individual concerned that their information has been disclosed to a third party (regardless of whether or not the disclosure itself is allowed).*
[3] From MoJ Consultation Document: *'introducing an amendment to IPP 2 to narrow exceptions that allow agencies not to collect information directly from the individual concerned (i.e. that allow agencies to collect the information indirectly).'*
[4] From MoJ Consultation Document: *'introducing a new separate privacy principle dealing with notification of indirect collection.'*

Union's General Data Protection Regulation (GDPR), a similar exemption is provided in the California Consumer Privacy Act (CCPA)[5].

40. The Association submits this would be the most equitable and practicable stepforward so that small businesses are not placed with the same compliance burdens of a large business who has the time and resources to adjust to these amendments.

Question 4 – If you are a New Zealand business or agency, are there any practical implementation issues you can identify in complying with the proposed changes?

41. A key issue in regards to implementation that is true for not just the hospitality industry but small business at large, is that business owners simply do not have the capacity to keep up to date with the constantly changing legislative environment.

42. A survey[6] on the impact on the preparedness of SMEs for the GDPR found that:

    - 28% were not familiar with the GDPR
    - more than half believe the GDPR is too complex for small and medium businesses and for middle market business (51%).

43. Our concern is that smaller operators may be unfairly sanctioned for non-compliance simply because they are unaware of changes or lack the required resourcing to update their systems.

Question 5 – Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?

44. In light of the COVID-19 tracing requirements, the public has become increasingly suspicious about how their information is stored. Unfortunately for hospitality, café and restaurants have been on the receiving end of much of the public's distrust and frustration as they were on the frontline of enforcing COVID-19 contact tracing requirements.[7]

45. Therefore, the Restaurant Association remains concerned at the possibility of vexatious and unwarranted complaints targeted at the hospitality sector as a result of a heightened sense of distrust by the public. This is especially true since

[5] California Consumer Privacy Act of 2018 s1798.140 (C)
[6] How the GDPR impacts and suffocates small and medium businesses
[7] 'A breach of privacy': Government issues reminder to hospitality sector over contact tracing details

hospitality businesses often run multiple loyalty programs or marketing campaigns for which customers sign up without a great deal of thought.

46. The Ministry of Justice could help mitigate this with a comprehensive education campaign for the general public, that outlines what kind of behaviour warrants a complaint and how to better understand their rights when it comes to the collection of their private information.

47. To combat customer fatigue, the Restaurant Association submits that a more effective way to report and record privacy breaches is for the Government to create a central register where relevant details of a breach can be provided by businesses and checked by consumers. This register could then be integrated with RealMe accounts, through which individuals are notified of any breaches.

Question 6 – Should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?

48. Given New Zealand's hospitality industry attracts numerous overseas visitors, many who often book their dining experiences from overseas - this separation would be unnecessarily administratively burdensome. The Restaurant Association submits that if an amendment is made it should apply to information collected both domestically and overseas for clarity and consistency.

Question 7 – Is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback.

49. The Restaurant Association welcomes the Government's work to update our data privacy frameworks and appreciates the Government's efforts to align our privacy framework with those of our international counterparts.

50. We believe that transparency in the collection, use, and disclosure of personal information is fundamental to protecting individuals' privacy rights as well as their dignity and autonomy—particularly as the evolution of business models and technology in the past few years has seen a rise in the indirect collection of personal information.

51. However, we are concerned these changes have the potential to drastically increase the administrative burden and compliance cost to small and medium sized businesses in New Zealand.

52. While we agree with the objectives of this proposal, we urge the Government to consider our submission and adopt practical, sensible measures to mitigate these concerns.

About the Association

53. The mission of the Restaurant Association of New Zealand is to be the link between good food and good business so that our Member's restaurant or café can succeed. We're passionate about our vibrant industry, which is full of interesting, talented and entrepreneurial people.

54. Since 1972, the Association has worked to offer advice, help and assistance in every facet of the vibrant and diverse hospitality industry. We are the representative body for more than 2,500 hospitality businesses, with Members covering the length and breadth of the country. We are organised into 13 regional branches and led by a national office located in Mt Eden, Auckland.

Proposed changes to the notification requirements in the Privacy Act 2020

I am writing to provide some thoughts on the suggested changes to the Privacy Act 2020

1. What factors do you think are most important when considering changes to indirect collection of personal information?

Whether there really is a need for changes, and whether the proposed changes will meet that need without introducing other issues.

2. What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?

The intended benefits are great – more transparency and control for individuals, although I think this is unlikely to be achieved in a material way

Even the example given in the consultation material describes a situation where the individual has consented to the sharing/indirect collection. While there are broader issues around the nature of informed consent, I don't think this is mitigated by a notification requirement on the collecting agency.

The biggest disadvantage I think, is the risk that agencies need to collect more information than they really want in order to give effect to their new notification obligations, or that they collect more information to future-proof their use case (to avoid having to notify again for a subsequent collection).

3. What form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate.

I don't think any of the proposed changes will significantly improve individuals' control over their information.

It is hard to come up with examples that engage the exceptions in the Act allowing for indirect collection, but would not be undermined by notification.

For this reason, I think the most effective approach would be to amend IPP2 to limit the reasons indirect collection can occur. If the concern really is giving people more control over

who is collecting and using their data I think this is the only option that achieves that. Giving people more opportunity to decline to share information is much more powerful than giving them the chance to acknowledge a notification, with no control over the collection itself.

4. If you are a New Zealand business, are there any practical implementation issues you can identify in complying with the proposed changes?

Agencies may be required to notify individuals about indirect collection that does not include contact details. It is not clear to me how an agency would notify them without collecting even more information than they initially intended to.

5. Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?

Changes might lead to increased collection of personal information. For example, an agency indirectly collecting some limited personal information may now be required to also collect contact details they wouldn't have otherwise, in order to make the necessary notification.

They might also collect more information than they strictly need at that time, to avoid notification processes in subsequent collections (getting it all done with one notification).

6. Should the proposed changes on y apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?

Any changes made should apply to all personal information/individuals equally. Differentiating in this way only adds unnecessary complexity, and if the issue is significant enough to warrant legislative changes two years after the new Act came into force, it must be offering protections that everyone should enjoy.

7. Is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback.

I struggle to see how these proposed changes really give more control to the individual. There may be rare cases where inappropriate collection is uncovered by this obligation, but

for the most part it seems likely that these notifications will experience the same issues direct collection consent forms have i.e. poorly written, too long, not well read or understood, and just adding to the mountains of tick-box compliance material consumers blindly click through.

Privacy Act Notification Submission

Dr Paul Roth
Professor Emeritus
Faculty of Law
University of Otago

Introduction

1. New Zealand's Privacy Act 2020, like its predecessor, has a weak notification requirement in relation to the collection of personal information from individuals. This can be attributed to the Act's vaunted "light-handed" form of regulation, and the largely "harm-based" nature of a privacy regime that normally requires that the data subject must have suffered some harm or loss arising from breach of an IPP (except IPPs 6 and 7). This renders the task of implementing a "*broader* notification requirement" mechanically difficult within the Act's current framework.

2. The Act contains no formal notification requirement in IPP 3, which covers the collection of personal information directly from individuals. It merely requires that the collecting agency must ensure that the individual is "aware of" the matters set out in IPP 3(1), whether before or after the collection takes place. This is not "notification" at all in its active sense. The language of the GDPR is that the controller "shall provide the data subject with …. information" (articles 13 and 14), which is a somewhat stronger requirement. There is also no formal requirement of "fixing" purpose in New Zealand as there is in some overseas jurisdictions Moreover, New Zealand's transparency requirements, such as they are, can be so loose that they are in many instances satisfied merely by implication, or else the burden of being "aware" of the matters set out in IPP 3(1) can lie on the individual, who may be merely "put on notice" (rather than expressly or formally "notified"). Often enough, "notification" is accomplished by the data subject ticking a box agreeing to terms and conditions as a prerequisite for obtaining some necessary or desired service or product, or a discount or the like, and such terms may have embedded in them a privacy policy (often enough going unread) that contains matters set out in IPP 3(1). The use of the term "notification" in an IPP 3(1) context generally is therefore somewhat exaggerated. It is really a making "aware" to a greater or (usually) lesser extent in respect of the various matters set out in IPP 3(1).

3. New Zealand thus arguably has an ersatz requirement of "notification" to begin with. To broaden the notification requirement should entail the introduction of a requirement of *real* notification as a first step as far as IPP 3 is concerned, at least where formal notification is reasonable and practicable. Otherwise, it might be sufficient even to rely on some bolstered form of IPP 4(b) to ensure that the manner of collection is fair, so as to include, for example, some elements of consent and transparency to the collection of personal information. Where personal information is collected from a source other than the individual concerned, then a modified IPP 2 should apply if it is proposed to introduce a new requirement of notification. The introduction of an entirely new IPP to deal with this alteration seems unnecessary and would only make the IPPs more complex than they already are. (I have written elsewhere that IPPs 2 and 3, and 10 and 11, could be condensed into just 2 IPPs, thus making the IPPs less numerous and simpler to follow).

4. As a prerequisite of broadening existing notification rules to cover the indirect collection of personal information, therefore, the rules governing the direct collection of personal information should be re-examined to make transparency under the Act more meaningful for data subjects. Otherwise, the law would only be broadening a rule that is somewhat weak in the first place.

Strengthening transparency where personal information is collected directly from the data subject (IPP 3(1))

(1) A requirement of consent to underpin the right to transparency

5. New Zealand's Privacy Act does not contain an express provision that requires the individual's consent to the processing of personal information (ie, collection, holding, use, and disclosure). Consent is only weakly implicit in the transparency requirements of principle 3(1), and the exceptions to IPPs 2, 3, 10 and 11 where the individual may have "authorised" some departure from the relevant IPP.

6. Article 6 of the GDPR provides that processing must be "lawful". "Lawfulness of processing" is satisfied in a number of different circumstances set out in article 6. These include that "the data subject has given consent to the processing of his or her personal data for one or more specific purposes": article 6(1)(a). New Zealand's Privacy Act, however, does not contain a requirement of explicit consent to the processing of information along these lines. Article 4(11) defines data subject "consent" as "any freely given, specific, informed and unambiguous indication of the data subject's wishes which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". If the Privacy Act is to strengthen the right to transparency, then IPP 3(1) of the Privacy Act is the place in which to achieve this.

(2) A requirement to continuously update notification in IPP 3(1) as circumstances change

7. Once personal information has been collected and the data subject "is aware of" the matters in IPP 3(1), it is very likely that the circumstances of holding or using the information may change over time. For example, the purpose for which the information was collected may alter (IPP 3(1)(b)); the intended recipients of the information may change (IPP 3(1)(c), which could mean that the information may be made available to other agencies, though (perhaps to be pedantic) a "recipient" is not necessarily the same as an indirect "collector" of the information); the name and address of the collecting or holding agency may change (IPP 3(1)(d)); or the legal basis for the collection of information may change (IPP 3(1)(e)). The requirement for transparency should ideally entail that the data subject is made aware of such developments as a continuous obligation if it is reasonably practicable for the agency concerned to do so.

8. There is a precedent in the Privacy Act for a continuous obligation of notification in IPP 7(5), which requires an agency that has corrected personal information or has attached a statement of correction sought but not made to "inform every other person to whom the agency has disclosed the information" of the correction, insofar as it "is reasonably practicable".

9. However, there is no obligation on the source agency to follow up whether the agency to which the information was disclosed has properly acted on it: *Case Note 7327* [2002] NZPrivCmr 7 (June 2002).

10. Moreover, if the individual concerned has suffered no harm or loss because of a breach of IPP 7(5), there is no obvious remedy against the agency that has the obligation of notification. A failure to comply with the duty under IPP 7(5) is not covered under s 69(3) or (5) (i.e., it does not amount to an "interference with the privacy of an individual").

11. A breach of IPP 7(5) would occur if the agency concerned failed to inform every other person to whom the agency has disclosed the information if the complainant can prove that it was "reasonably practicable" to have done so. This is likely to be a difficult matter to prove, but a remedy for failure to comply with IPP 7(5) should nevertheless be available under s 69(2)(a)(i), on the basis that the non-compliance amounts to a breach of IPP 7. In such a case, however, the complainant would also need to show some harm or loss in terms of s 69(2)(b), a matter that need not be proved under s 69(3) or (5) in respect of other breaches of IPP 7.

Introducing transparency where personal information is collected from a source other than the individual concerned (the IPP 2 exceptions)

12. A requirement to notify or make individuals aware that their personal information has been collected from a source other than themselves could either be folded in with IPP 3, which might be an unwieldy exercise, or else be provided for in a new IPP 2(3). Such a requirement would not apply to all of the exceptions in IPP 2(2), since some of these raise issues of relevance, applicability (eg, IPP 2(2)(a), (b), (e), (f), (g)), or practicality (IPP 2(2)(d)). However, IPP 3(1)(c), the requirement to make data subjects aware of "the intended recipients of the information", could be strengthened by requiring the agency that originally collected the information to continuously update any new recipients of the information of whom it is aware and notify the data subject of these. An obligation of continuous updating of notification was discussed above at para 7.

13. IPP 2(2)(d), the publicly available publication exception, raises two issues: firstly, the practicality of notification, and secondly, the particular agency that would have the obligation of notification: the original collector of the information which has been published in a publicly available publication; the agency that subsequently collects the information from the publicly available publication; or both? It might only be the original collector of the personal information that has the contact details of the data subject in order to effect notification. There could instead be a general requirement of notification along the lines of s 44(3) of the Data Protection Act (UK): that notification is required, if reasonably practicable, where personal information has been collected without the knowledge of the individual concerned.

14. Perhaps the easiest and most cost-effective way of providing for transparency in respect of personal information collected from a source other than the data subject is for agencies simply to publish widely (e.g., on websites, newspapers) the entitlements of individuals under IPPs 6 and 7. In addition, a new bundle of rights could entitle individuals to enquire on their own motion (after requesting and receiving confirmation under IPP 6(1)(a) that an agency holds their personal information) concerning the purpose for collecting their

information, the agency that is holding the information, the intended recipients of the information, and any other relevant matters set out in IPP 3(1), with the burden being put upon individuals to exercise their IPP 6 entitlements in the first instance.

Should the application of changes be limited only to personal information collected indirectly from individuals overseas?

15. As for whether the proposed changes should apply only to personal information collected indirectly from individuals overseas (and not necessarily to personal information collected from individuals in New Zealand), the former position would best satisfy EU concerns. However, this would still leave EU residents exposed whose personal information is indirectly collected while they are visiting or working in New Zealand, which means coverage of overseas residents would be incomplete. It would seem overly complex to draft a carve-out for individuals from overseas as this would involve, for example, having to provide for dual nationals, and the accommodation of web-based collections of personal information.

Carter, Adam

From: Campbell Scott <campbell.scott@harcourts.co.nz>
Sent: Friday, 30 September 2022 10:26 am
To: Privacy Feedback
Subject: SUBMISSION - Proposed Changes To Notification Rules Under Privacy Act 2020

Importance: High

Good morning

I have read the REINZ's submissions regarding proposed changes to the notification rules under the Privacy Act 2020 discussed in the Ministry of Justice's Engagement Document, released in August 2022. I fully support the REINZ's submissions.

Given real estate companies' vendor clients have authorised the sharing of their information to REINZ both by way of the agency agreement at the commencement of their campaign and again in the sale and purchase agreement at the time of sale, there should be no further obligation to notify that person every time their information has in fact been shared with REINZ. The information itself is limited to the property address, sale price and date of the agreement. It is provided to REINZ upon a sale becoming unconditional with the information becoming publicly available when the sale settles (typically 3-6 weeks later).

I am not persuaded there is a problem that needs fixing. I am therefore strongly against any change and it is my submission that no change is required to the notification regime for New Zealand.

Regards,

Campbell SCOTT

Director
Monarch Real Estate Limited
Liceensed REAA 2008

M s9(2)(a)
D s9(2)(a)
W www.hamiltonharcourts.co.nz

Harcourts Hamilton

Carter, Adam

From: Mushtaq Sheikh <m.sheikh@harcourts.co.nz>
Sent: Saturday, 1 October 2022 6:41 pm
To: Privacy Feedback
Subject: Privacy Act Engagement

Hi
The submission made by REINZ on the matter is fully supported by me as well.

Kind Regards

Mushtaq Sheikh JP, DipRE, AREINZ
Managing Director / Principal
Harcourts Reliable - Licensed REAA 2008
M +64 21 479 365
PO Box 75418, Manurewa, Auckland, 2243
190b Great South Road, Manurewa, Auckland, New Zealand

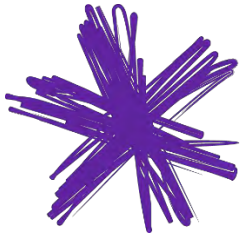
Carter, Adam

From: Geoff Smith <geoff_smith@raywhite.com>
Sent: Wednesday, 28 September 2022 9:14 am
To: Privacy Feedback
Subject: Possible Changes to Notification Rules Under the Privacy Act 2020.

To Whom It May Concern,
My main problem with the possible changes in regard to the Privacy Act 2020 relates to Market Appraisals. We, as licensed salespeople, are legally required to provide a prospective vendor with a written market appraisal, which includes recent comparable sales to the subject property, prior to listing their property for sale. The proposed changes to the privacy act could potentially make this very difficult. If we are unable to access recent comparable sales data, due to privacy issues, how are we to then establish a realistic sale price indication for the prospective vendor? If we cannot access this information , it basically means the legally required market appraisal is irrelevant & pointless.

Regards,
Geoff Smith.

Geoff Smith
Licensee Salesperson | Ray White Greerton
Crockford Real Estate Limited
Licensed (REAA 2008)
M s9(2)(a) T s9(2)(a)
Whttps://rwgreerton.co.nz
A212 Chadwick Road, Greerton



Possible changes to notification rules under the Privacy Act 2020

Public Version

Ministry Of Justice

30 September 2022

Spark welcomes the opportunity to provide its views on the Ministry of Justice's consultation on possible changes to notification rules under the Privacy Act 2020. The changes proposed will have implications for agencies, as well as individuals, so it is important that they are designed to be as practicable as possible.

Consideration of any changes to notification rules needs to balance three key factors:

1. **Maintaining New Zealand's adequacy status**

   It is important for businesses like Spark that New Zealand maintains our EU adequacy status.

   As a matter of principle, we consider notification requirements should only be modified to the minimum extent required to help New Zealand maintain adequacy with the EU.

2. **The benefits for and risks to individuals**

   We note that in the website example described in the consultation, the individual concerned would be notified twice – firstly by the website when the information is collected, and secondly by the collecting agency. This second notification would seem to offer very limited benefits.

   As noted by the Ministry while there are potentially some benefits for individuals, these are potentially offset by factors such as notification fatigue and 'overloading' of information for individuals. As the volume and types of notifications increase, the marginal benefits for individuals diminish, to the point that they create more harm than good for individuals, and become a costly exercise in compliance for organisations.

   As such, care needs to be taken to ensure that requiring notification of indirect data collection does not have an adverse effect on individuals who may increasingly 'tune out' all privacy notifications (and not just the new ones). It would be a very unfortunate consequence if some of the benefits of the current privacy regulation were lost because of the sheer volume of notifications which are issued.

   Conversely a simple notification regime that focuses on the actual risk of material harm will support agencies to maintain simpler privacy policies and notification frameworks. Individuals are therefore more likely to benefit from, and engage with, a simpler regime.

3. The costs for agencies

Finally, it is important to factor in the costs for agencies in complying with the notification rules. Depending on how it is implemented, the costs of developing, implementing, and maintaining an extended notification process can be considerable.

In view of the potential costs relative to the benefits and possible risks we submit that any changes should be limited to the minimum required to maintain international compatibility, including EU adequacy. This would help limit the risks to individuals of notification fatigue and minimise the increased costs for agencies.

With a view to helping keep individuals informed while reducing the risk of notification fatigue and excessive compliance costs for organisations, we recommend that any new requirements for notifications for indirect data collection are designed so that they may be satisfied through the privacy policies of the disclosing agency (preferably) or the collecting agency when necessary. Avoiding duplication of privacy messaging is important to help minimise notification fatigue.

If indirect information collection notification requirements are to be extended, we strongly support a further round of consultation on the specifics of the implementation options so organisations can give more consideration to the likely implementation and ongoing costs they would face and likely benefits of each approach, and provide more detailed feedback on the relative benefits and risks.

We would therefore welcome further engagement on the specifics to ensure the benefits to individuals are appropriately balanced with the compliance cost to industry, while avoiding customers being swamped with notifications which they will ultimately ignore.

QUESTIONS:

1. **What factors do you think are most important when considering changes to indirect collection of persona information?**

   It is important that New Zealand privacy legislation enables us to maintain our EU adequacy status.

   It is critical that any changes are subject to proper regulatory impact analysis. This should take account of the impact and costs of compliance measures for agencies, the degree of actual harm to individuals today and the incremental benefits (and possible harms) expected for individuals by the proposed changes.

   We also support more New Zealanders engaging meaningfully with Privacy policies and information. Every individual already faces a multitude of Privacy Policies and privacy related notifications across the different agencies they deal with.

Ideally, we want to encourage people to engage with privacy policies and notifications more rather than less. Requirements that add to the length, complexity and the volume of privacy information are unlikely to encourage increased engagement. There is a risk that increasing notifications may deter some of those people who are currently attempting to engage meaningfully.

If the intention is to require a form of notification for indirect data collection that is additional to / instead of privacy policies (of either the collecting or disclosing agency) we believe that the compliance costs could be prohibitive for agencies, and in some cases it may not be possible to implement. Plus, the risk of notification fatigue described above would be significantly magnified.

2. What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?

Disadvantages

i. *Over notification and notification fatigue*

If changes include requirements to notify indirect data collection that has minimal or no impact, or is simply very standard practice, then this is likely to cause individuals to further 'tune out' of privacy policies and notifications. The risk of this is that these individuals will also ignore other types of notifications, including those which contain information about material risk that could have a serious impact on them, such as notification of data breaches where the individual needs to take action to avoid further consequences.

Similarly, duplicating messaging already provided by the collecting agency is of minimal value, and contributes to notification fatigue.

ii. *Overloading privacy policies*

Adding further notification requirements to existing privacy policies increase the complexity for individuals as they become "'overloaded" with information for minimal additional benefit. Again, the risk is that individuals are turned away from engaging with privacy policies

iii. *Compliance costs for agencies*

Broadening the notifications requirements creates direct costs on agencies. Further consultation is needed on the specific form of the proposed options so we can provide more detailed feedback on the likely cost for agencies

Advantages

i. Increasing likelihood of maintaining international compatibility with key overseas privacy legislation, including maintaining New Zealand's EU adequacy status.

ii. If restricted to material data collection practices, notifications can assist individuals who engage with them in identifying potentially "high risk" or unusual practices of agencies so they can make informed decisions on whether to use their services.

3. **What form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate**.

Further consultation is required on the specific form of the proposed options so we can fully understand their implications, and the extent to which existing exceptions to these IPPs would apply. However, on our current understanding of the proposals, they have the potential to trigger extensive notification requirements for agencies, in return for little benefit for individuals, or even a potentially detrimental impact.

This is particularly the case if IPP 3 or IPP 11 are expanded. Indirect collection does not fit comfortably within either and as currently proposed, there do not appear to be limits on what, how and when agencies would be required to notify individuals. The costs of developing, implementing and maintaining such a notification process would likely be significant and the number of notifications generated is likely to be such that individuals tune them out.

a. We consider Option 1 to be too broad. Extending notification to all indirect collection scenarios via IPP 3 is problematic because it triggers the same level of notification for indirect information collection as is justified as for direct information collection. However the actual potential for harm to an individual of collecting data from indirect sources, such as

- publicly available sources, and
- where the individual concerned has authorised (via a third party) collection from someone else

is likely to be minimal.

b. Option 2 depends on the IPP and proposed amendment.

Restricting (or preventing) indirect data collection via IPP 2 would appear a disproportionate mitigation in the absence of analysis quantifying any actual harm to individuals due to indirect data collection. It also may harm progress towards a data economy and facilitating business by placing undue restrictions on the use of data.

Amending IPP 11 to require the disclosing agency (who has the direct

relationship with the individual) to inform the individual may be a pragmatic way to help reduce compliance costs. However we would need to see more details including examples of how this would work in practice, to help inform our feedback.

c. Option 3 may be the best option. While IPP3 requires notification that is "reasonable in the circumstances" this is a very high bar (see Australian application of similar wording Chapter 5: APP 5 — Notification of the collection of personal information - Home (oaic.gov.au)). A new privacy principle could enable inclusion of an appropriate standard of materiality for indirect data collection without softening the notification requirements for direct data collection. It could also be crafted to ensure that notification requirements are able to be managed pragmatically via privacy policies of the disclosing agency where possible.

4. **If you are a New Zealand business, are there any practical implementation issues you can identify in complying with the proposed changes?**

Further consultation is needed on the specific form of the proposed options. The options proposed in the consultation document are not sufficiently detailed for us to fully understand the practical implementation issues. However, we do note that the costs for agencies could be high, and the benefits for individuals questionable, under any option which results in a high level of notifications.

5. **Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?**

Our recommended approach is that any new requirements for notifications for indirect data collection are designed so that they may be satisfied through the privacy policies of disclosing agency (preferably) or the collecting agency when necessary. Avoiding duplication of privacy messaging is important to help minimise notification fatigue.

Any framework that requires additional notification communications to individuals is likely to be resource intensive and costly to implement, and in some circumstances may not even be feasible. We also consider that such notification methods would be unlikely to result in more informed decision making on data sharing for most individuals, and may in fact be overwhelming and have a detrimental impact on the value of existing privacy practices.

We consider there are certain types of information sets which could be excluded from notifications. For example:

i. Publicly available information (e.g. real estate listings)

ii. Personal information where the individual has already been advised how it will be used / disclosed by the agency directly collecting it

iii. Personal information where the individual concerned has authorised (via a third party) collection from someone else

We also support the three risk mitigation examples set out in the consultation paper.

6. **Should the proposed changes only apply to personal information collected indirectly from individuals *overseas*, or should they also apply to personal information collected indirectly from individuals in *New Zealand?***

We support the approach of only applying the changes to personal information collected about individuals overseas as a way to minimise change and reduce over notification. In theory this would reduce compliance cost.

However, there are significant operational complexities in being able to differentiate between data of different sources. The practical outcome is likely to be that many organisations end up taking the same approach to the notification of indirect personal information collected about individuals whether overseas or in New Zealand.

Carter, Adam

From: Blair Stewart s9(2)(a)
Sent: Wednesday, 24 August 2022 12:16 pm
To: Privacy Feedback
Subject: Possible changes to notification rules under the Privacy Act 2020

Dear Ministry of Justice

I refer to your engagement document seeking feedback by 30 September 2022.

As I will shortly be travelling and be out of the country for part of that period and will be quite busy on my return I offer only this very quick initial response. In relation to my experience in this area of law I mention that I was Asssiatnt Privacy Commissioner (1993-2018) and, since 2018, have co-authored Lex sNexis *Privacy Law and Practice* (with Paul Roth).

You seek feedback on seven questions to which I offer my views.

1. What factors do you think are most important when considering changes to indirect collection of personal information?

I think reform of the privacy law obligations in relation to indirect collection will address a longstanding gap in the law, thereby strengthen consumer rights and raise the standard of our privacy law to the standard in other countries. It will also help address risks aerising from this that have grown with the digital economy.

2. What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?

Advantages that I consider important are transparency for individuals, accountabiility of agencies for their practices and alignment of NZ law with existing and emerging international standards. Individuals will gain more rights and thus more control over thier information. Failure to act to reform NZ law might leave NZ's status as providing an adequate level of protection in terms of the EU GDPR in jeopardy and loss of that status would be detrimental to some NZ business.

3. What form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate.

Whatever the precise form, in my view alignment with international standards will be a prime consideration. In this respect alignmemet with EU GDPR should be a starting point. However, I'd also like to think that any change will also ensure that 'do not track' obligations will also be suupported byy any change.

I don't think voluntary guidance will suffice. Codes of practice will have a role in tweaking and supplementing any statutory change but I agree that codes are not the right tool for a general accross the board change.

4. If you are a New Zealand business, are there any practical implementation issues you can identify in complying with the proposed changes?

N/A

5. Are the e any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?

I have no particular suggestions to offer.

6. Should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?

I would advise against any suggestion that the obligations apply only when information is collected overseas. I infer that this is a variation on the approach taken in Japan to meet EU expectations when handling EU sourced data. It is my view that if any change is warranted it would work to benefit New Zealand individuals and not merely be some device to assuage consumers in other economies.

7. Is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback.

Not at this stage.

s9(2)(a)

Sent from Mail for Windows

Te Whatu Ora
Health New Zealand

05 October 2022

2022 Privacy Feedback Ministry of Justice

By email: privacyfeedback@justice.govt.nz

Proposed changes to notification rules under Privacy Act 2020

Importance of transparency in data collection

At the outset it is important to say that Te Whatu Ora Health New Zealand (Te Whatu Ora) accepts that transparency and openness about the collection, retention, use and disclosure of personal information is important. Broadening the notification requirement should see people are better informed about what happens with their personal information.

There is a range of positions on the proposed changes within Te Whatu Ora. Some strongly believe that all information sharing with third parties should be notified to individuals, others have concerns that the proposed changes may adversely impact the ability of the public health sector to provide timely and safe care to individual patients, manage public health issues and commission services.

Our comments on the proposed changes are set out below.

Health sector context

It is important to understand how the health sector works and the complexities associated with the collection and sharing of information in the health sector.

The health sector works primarily under the Health Information Privacy Code (HIPC) as opposed to the Privacy Act 2020 (Privacy Act), but we assume that the proposed changes to the Privacy will flow through to the HIPC. This is important because the HIPC while broadly based on the Information Privacy Principles in the Privacy Act is specifically tailored to the provision of health care services.

The recent health sector reforms in some ways simplified the sector and in other ways complicated it. Former District Health Boards and shared services organisations have been amalgamated into a single entity (Te Whatu Ora | Health New Zealand), a reduction of approximately thirty mostly geographically defined organisations to one. However, three national health organisations have been created where only one existed previously (Te Whatu Ora | Health New Zealand, Te Aka Whai Ora | the Māori Health Authority and Manatū Hauora | Ministry of Health. Parts of the Ministry of Health have been transferred to Te Whatu Ora. Sharing of data between the 3 new national organisations needed to be accounted for so a mechanism called a Data Tripartite Agreement effectively a MoU) was created to enable that sharing. (Note however that sharing under the Data Tripartite Agreement is still subject to privacy analysis).

The health sector's current focus is on creating information systems which make information about individual's health more accessible to the individuals themselves and to all the health providers involved in providing care or treatment to an individual. Greater accessibility will also increase individuals' control over their information and their care. This is consistent with the approach to health information internationally. The proposed changes are likely to create complexity and compliance hurdles for this work.

Te Whatu Ora
Health New Zealand

The health system and data/information

How the health system operates in relation to data/information

- Information about the health of individuals is collected by service providers e.g. public hospitals and community services, general practices, non-government organisations
- Limited (but individual level and personally identifiable) data flows from service providers to operational, funding, service commissioning and policy organisations, such as the Manatū Hauora/ the Ministry of Health, Te Whatu Ora Health New Zealand, Te Aka Whai Ora/Maori Health Authority, Te Aho o Te Kahu/Cancer Control Agency, Pharmac.
- Te Whatu Ora – Health NZ make this available to Manatū Hauora/ the Ministry of Health, under the Tripartite data Agreement mentioned above.
- Te Whatu Ora – Health NZ may share data with researchers or other parts of the sector for specific purposes.
- Data is used and shared by these funding, service commissioning and policy organisations to improve health outcomes for New Zealanders.
- Sometimes the information flow is through intermediaries.

Public health agencies frequently work in situations where a particular agency did not collect the information directly from individuals. They frequently do principal-principal transfers of information and sometimes principal-agent transfers. Exceptions to Rule 11 of the HIPC are often relied on when on-sharing data.

Some health sector sharing involves information about large cohorts of people e.g., all people in a particular region, or enrolled in a particular organisation, or eligible for a particular programme, or with diagnoses with a particular condition. Some of these cohorts may run to hundreds for thousands of people (albeit with limited and targeted information for specific purposes).

Some examples of situations where Manatū Hauora | Ministry of Health and Te Whatu Ora Health New Zealand shares information with third parties may assist:

(a) Inpatient and outpatient data is shared with a cross government analytics group (currently run out of ACC) which is looking at road traffic crashes across NZ as part of an ongoing cross-government study of road traffic accidents.
(b) Hospital inpatient and outpatient data is shared with ACC for the purposes of the Public Health Acute payment i.e. where ACC re-imburses Manatū Hauora | Ministry of Health for the costs of acute accident care.
(c) Information is shared with Police when requested for their investigations.
(d) Vaccination data is shared with other parts of the health sector for outreach purposes
(e) Medical warnings data is shared CARM – the Centre for Adverse Reactions to Medicine.
(f) Details of young people diagnosed with cancer with the regional cancer network so that they can support those patients
(g) Information is shared with inter-agency groups focused on domestic violence, elder abuse and child safety
(h) some of our systems are interconnected e.g. the National Health Index (NHI) so that updates made by in one system (e.g. a name or address change) may be widely distributed or made available to other parties. For example, an update to a patient's NHI record by a public hospital is then shared with a GP or other health providers. Hospitals submit ACC claims to ACC electronically.

(i) Other agencies share information with the public health sector. For example, the Department of Internal Affairs shares information about births and deaths with the NHI to enable records to be updated.

With respect to sharing of information via electronic information systems, two particularly significant examples of information systems currently being proposed for the public health sector illustrate the complexity of information sharing in the health sector are set out below.

- The Ministry of Health's National Health Information Platform (HIRA). HIRA will draw together a person's latest health data from multiple trusted source systems on a virtual platform to create a virtual electronic health record which can be accessed as needed. Patients will have better access to their health information and can control who they share information with. Providers will have secure, easy access to patient information, in the right context and at the right time. Individuals will not need to have direct engagement HIRA as role-based access and business rule for recording individual consent for access will developed as part of the system. Tranche 1 of HIRA will provide access for providers and consumers to health information such as demographics such as gender, ethnicity, name and ate of birth, enrolled general practice, community service card entitlements, prescribed and dispensed medicines, Covid-19 vaccination status, lab test results and summary primary care data. Consumers will have the ability to update information in the National Health Index such as their contact details. Access will be via websites and apps. HIRA will continue existing arrangements where health care records are shared between providers to provide health care. If a provider is directly providing care to an individual (e.g. a GP providing care to a patient enrolled with their practice) and is or has been involved in the patient's care, then the provider will be able to access the individual's health information in HIRA. HIRA will also enhance and 3expand on information sharing practices like this. Over time it is expected that a wider group of health services will be able to access and contribute to shared Consumer health records via HIRA.

  Similarly, the Hira system is designed to enable a connected a connected ecosystem of disparate data sources (Agency A) who have collected data from many people (Individual B). Other organisations (Agency C) will then connect to the Hira platform to access data from multiple data sources to create a new digital health service that provides value to New Zealanders. Agency C may not have a direct relationship with Individual B.

  The implementation of a notification pathway to individual B via an automated data platform would therefore be difficult if Agency C does not have a direct relationship with Individual B.

  Other questions arise out of the Hira example:

  - Would Agency A need to share more personal data than was required by Agency C so that Agency C could notify Individual B that they had their data?
  - Would that notification need to be via a phone call, an email, or a letter to their address, if Agency C has no other way of contacting Individual B?

- Alternatively, would Hira need to require all data sources who connect their data to Hira to provide a mechanism to notify all Individual Bs every time their data was shared with Agency C? What if they don't have the technical ability to do this?

It important to note that Hira is privacy enhancing as data access will often be only allowed by Individual B using Agency C's application and so Individual B will be providing explicit purposed based consent for their data to be accessed by Agency C

- The Regional Collaborative Community Care (RCCC) information platform. The Northern Region Districts of Te Whatu Ora (Northland, Auckland, Counties-Manukau and Waitemata) are commencing implementation of a regional information system RCC will give individuals accessibility, visibility, control and choice over who accesses their information, make information from secondary and tertiary treatment providers accessible to workers in primary or community contexts and vice versa.
  An underpinning principle of RCCC is transparency, meaning that individuals will be able to see all the actions taken in relation to their care. RCCC is an example of such an information system. The goal of the system is to create greater cohesiveness and connection between individuals receiving care and the agencies/organisations involved in providing care to them. It will allow agencies/organisations involved in an individual's care to access information about that individual whether that information is held by the individual's primary (General Practitioners), secondary and tertiary health providers (hospitals and community health services), other government agencies (MSD, ACC etc) and non-government agencies (NGO). The increased connectedness will improve health outcomes for the individual, ensure more "joined up" services are

Difficulties with complying with a notification requirement include:

Potential difficulties with complying with a notification requirement must be considered. Difficulties include:

1. Inaccurate/out of date contact information

Te Whatu Ora does not hold accurate and up to date contact information for all the individuals about whom it holds information. This means we will not be able to notify all patients that we are sharing their information with a third party.

Contact information is generally checked and updated each time an individual has contact with the health system, but beyond this there is no rigorous process for ensuring that all contact details are accurate and up to date.

It is difficult to keep contact information up to date because some individuals have only infrequent contact with the health system, others leave New Zealand to live overseas, tourists or short-term visa holders who were only ever visiting New Zealand return to their home countries. Some individuals are itinerant or homeless or provide false details for reasons which range from being illegal immigrants to avoiding arrest to being ineligible for free health care. Some individuals have simply moved house or changed email address or phone number since the last time they had contact with the health system.

There are also gaps for New Zealanders who die overseas could be New Zealanders, or those who have used health services while visiting NZ, because death registration information is not provided by other countries.

2. Overheads associated with notifying patients

There will be significant overhead in notifying individuals when information is transferred to third parties given the frequency of sharing and the large numbers of individuals whose data may be transferred. This overhead is not currently resourced.

For some individuals, Te Whatu Ora will have email addresses, for others only phone numbers and for many only their physical address. That means notification to al of the people whose data is being transferred to a third party will be via a range of communication channels. There is significant over head in that which is not currently resourced.

3. Shared contact details

How are agencies to comply with notification requirements where individuals have shared contact details?

Some people share an email address and phone number (eg spouses sharing one email address or a family using one email address). Some who live in rest homes give the phone number or email of the rest home they live in as their contact details. For most children, the contact details are those of their parents.

Will notification to whatever contact address an agency holds be sufficient, even if that address is shared?

4. Safety

How will safety be ensured if third party disclosures must be notified. For example, if a parent has protection orders against their partner because of family violence issues, how can the risk that the safety of the parent or the child will be put at risk through notification processes be mitigated. What about situations where a child is in the care of the State or has been adopted or where there are protection orders which specify that a parent is not to be told where their child is living? Will departures from the notification requirement be permitted in these kinds of situations?

Authority for sharing information

It is not clear whether/how the proposed requirement for notification will impact current provisions mandating or authorising information sharing. This is a significant concern for the public health sector as provision of timely and fully informed care is critically dependent on information flowing smoothly between health care providers.

Authority for sharing information is derived from a number of mechanisms including:

- direct consumer authorisation
- informing about information uses via privacy statements
- information used/shared for the purpose it was collected

- exceptions in Rule 11 of the HIPC
- statutory provisions mandating information sharing or giving a discretion to share

Multiple statutes allow or mandate the sharing of health information and by implication the indirect collection of information. Section 24 of the Privacy Act 2020 provides that nothing in IPP6, 11 or 12 limits or affects a provision in any NZ enactment that authorises or requires personal information and an action taken by an agency does not breach IPPS 1-5, 6-10 or 13 if the action is authorised or required by or under New Zealand law

As an example, section 22F of the Health Act 1956 makes it mandatory for a person/agency which holds health information about an individual to provide health information to any person who is providing or is to provide, services to that individual. Section 22F ensures that health care providers are able to obtain the information they need to safely treat patients. Its scope is broad and is utilised by all manner of health care providers.

The party requesting information under section 22F will be collecting health information about the individual indirectly. It would appear that this indirect collection would activate an obligation to notify the individual if the proposed changes go ahead. Section 22F is a key mechanism for information sharing in the health sector which ensures that health providers are able to access information about patients they are treating, or anticipate treating, smoothly. Any erosion on section 22F through the proposed changes to IPP2 and 3 will seriously impact the health system's ability to provide safe and timely care to patients.

Another example would be the collection of information under Production Notices under the Search and Surveillance Act 2012 by departments of State, Crown entities, local authorities or other bodies that employ or engage enforcement officers as part of their functions. The Police regularly obtain Production Notices to gain access to information held by Te Whatu Ora Health New Zealand's hospital and community services. The Police are indirectly collecting the information they access via Production Notices. Will the Police be required to notify the individuals whose information they collect under Production Notices and how will any negative impact of a notification requirement on Police investigations be mitigated?

There is a mandatory requirement to share information with Oranga Tamariki on request under section 66 of the Oranga Tamariki Act and mandatory requirements for family violence agencies to consider sharing information about family violence under the Family Violence Act 2018.

If the proposal to require notification of indirect collection of information is adopted, section 24 should be amended so that there is clarity as to whether the requirement to notify applies to indirect collection of information under statutory provisions like section 22F of the Health Act 1956 and statutory processes like Production Notices under the Search and Surveillance Act 2012.

The proposed changes to IPP 2 and 3 have the potential to disrupt an established set of public sector processes where information is shared in order to deliver health care services and improve health and social outcomes. Te Whatu Ora submits that careful consideration needs to be given to the impact of the proposed changes on a complex sector like health. The Ministry of Justice must understand the sector at depth and in detail to truly appreciate the impact of the proposed changes.

We suggest that consideration be given to creating an exception to any notification requirement similar to that in Rule 11(2) of the Health Information Privacy Code where compliance "… is not

necessary if the health agency believes on reasonable grounds, that it is either not desirable or not practicable to obtain authorisation from the individual concerned …"

Impact will differ markedly depending on which of the proposed options is adopted

The proposed options for notification are broad and impacts will differ depending on which of the options is adopted. For instance, the requirement for notification may only apply to organisations collecting data about people overseas or may apply broadly to all third party sharing of information within NZ.

The effects will be significantly different for health sector and other government organisations depending on which option is chosen.

If the changes were to apply only to personal information collected indirectly from individual overseas, this would simplify things considerably and reduce the compliance overhead for domestic health sector organisations. If this change would be sufficient to retain GDPR equivalency which is the stated driver for the proposed changes, it would be a significantly less disruptive option and probably favoured in the health sector context

Impact on urgent sharing

Sometimes information must be shared urgently in order to provide life-saving treatment to an individual patient or to protect the life/safety of individuals or public safety. Sharing in such situations may occur under section 22F of the Health Act 1956 or under the serious threat exceptions in IPP 11(1)(f) and Rule 11(2)(d) of the Health Information Privacy Code.

Clarity is required as to whether notification will be required for disclosures in urgent circumstances.

Requirements for notification must be clearly defined

If the proposed notification requirement is introduced, there must be clear guidance in IPP2 and 3 as to what is required to comply with the requirement. The guidance should cover issues such as:

- What information must be contained in a notification
- Whether notification be considered effective if sent by email or post to the last known address for an individual
- Whether notification by public notice in the news media or on social media be permissible as a backstop when current contact details are not held
- Whether providing specific information about intended uses and disclosures of data at the point of collection be required or communicating a broader set of purposes at the point of collection be sufficient.

To illustrate, in the case of HIRA, it is proposed that standardised privacy notice materials will be produced and provided/made easily available to, individuals including via providers. Notification may also be provided through web-based explanations and a variety of accessible media, including video and verbal presentations may be used. In other words, a layered privacy notice approach is proposed.

It will be critical for the agencies designing and promoting a new information platform like HIRA to know whether measures like these will comply with the notification requirements for indirect collection.

Will notification be effective in ensuring transparency?

The examples of sharing in the health sector I have provided demonstrate the extent of sharing. Individuals are therefore likely to receive large numbers of notifications. Notification fatigue is likely to set in and bring into question the mechanism's effectiveness as a tool for achieving transparency.

Other tools for achieving transparency?

The proposal does not appear to have considered other options for achieving transparency. Giving individuals access to the systems in which their data is held so that they can see for themselves what data is held and who has accessed it would be a more effective way of achieving transparency and avoid issues like notification fatigue.

This submission was compiled on behalf of Te Whatu Ora Health New Zealand with input from the following groups:

Te Whatu Ora Corporate Privacy Team, Te Whatu Ora District Privacy Officers Group

Contact:

Contact for queries: Te Whatu Ora National Office Privacy Team

hnzprivacy@health.govt.nz

Te Whatu Ora
Health New Zealand

Proposed changes to notification rules under Privacy Act 2020

Importance of transparency in data collection

At the outset it is important to say that Te Whatu Ora Health New Zealand (Te Whatu Ora) accepts that transparency and openness about the collection, retention, use and disclosure of personal information is important. Broadening the notification requirement should see people are better informed about what happens with their personal information.

There is a range of positions on the proposed changes within Te Whatu O a Some strongly believe that all information sharing with third parties should be notified to individuals, others have concerns that the proposed changes may adversely impact the ability of the public health sector to provide timely and safe care to individual patients, manage public health issues and commission services.

Our comments on the proposed changes are set out below.

Health sector context

It is important to understand how the health sector works and the complexities associated with the collection and sharing of information in the health sector.

The health sector works primarily under the Health Information Privacy Code (HIPC) as opposed to the Privacy Act 2020 (Privacy Act), but we assume that the proposed changes to the Privacy will flow through to the HIPC. This is important because the HIPC while broadly based on the Information Privacy Principles in the Privacy Act is specifically tailored to the provision of health care services.

The recent health sector reforms in some ways simplified the sector and in other ways complicated it. Former District Health Boards and shared services organisations have been amalgamated into a single entity (Te Whatu Ora | Health New Zealand), a reduction of approximately thirty mostly geographically defined organisations to one. However, three national health organisations have been created where only one existed previously (Te Whatu Ora | Health New Zealand, Te Aka Whai Ora | the Māori Health Authority and Manatū Hauora | Ministry of Health. Parts of the Ministry of Health have been transferred to Te Whatu Ora. Sharing of data between the 3 new national organisations needed to be accounted for so a mechanism called a Data Tripartite Agreement effectively a MoU) was created to enable that sharing. (Note however that sharing under the Data Tripartite Agreement is still subject to privacy analysis).

The health sector's current focus is on creating information systems which make information about individual's health more accessible to the individuals themselves and to all the health providers involved in providing care or treatment to an individual. Greater accessibility will also increase individuals' control over their information and their care. This is consistent with the approach to health information internationally. The proposed changes are likely to create complexity and compliance hurdles for this work.

The health system and data/information

How the health system operates in relation to data/information

- Information about the health of individuals is collected by service providers e.g. public hospitals and community services, general practices, non-government organisations
- Limited (but individual level and personally identifiable) data flows from service providers to operational, funding, service commissioning and policy organisations, such as the Manatū Hauora/ the Ministry of Health, Te Whatu Ora Health New Zealand, Te Aka Whai Ora/Maori Health Authority, Te Aho o Te Kahu/Cancer Control Agency, Pharmac.
- Te Whatu Ora – Health NZ make this available to Manatū Hauora/ the Ministry of Health, under the Tripartite data Agreement mentioned above.
- Te Whatu Ora – Health NZ may share data with researchers or other parts of the sector for specific purposes.
- Data is used and shared by these funding, service commissioning and policy organisations to improve health outcomes for New Zealanders.
- Sometimes the information flow is through intermediaries.

Public health agencies frequently work in situations where a particular agency did not collect the information directly from individuals. They frequently do principal-principal transfers of information and sometimes principal-agent transfers. Exceptions to Rule 11 of the HIPC are often relied on when on-sharing data.

Some health sector sharing involves information about large cohorts of people e.g., all people in a particular region, or enrolled in a particular organisation, or eligible for a particular programme, or with diagnoses with a particular condition. Some of these cohorts may run to hundreds for thousands of people (albeit with limited and targeted information for specific purposes).

Some examples of situations where Manatū Hauora | Ministry of Health and Te Whatu Ora Health New Zealand shares information with third parties may assist:

(a) Inpatient and outpatient data is shared with a cross government analytics group (currently run out of ACC) which is looking at road traffic crashes across NZ as part of an ongoing cross-government study of road traffic accidents.
(b) Hospital inpatient and outpatient data is shared with ACC for the purposes of the Public Health Acute payment i.e. where ACC re-imburses Manatū Hauora | Ministry of Health for the costs of acute accident care.
(c) Information is shared with Police when requested for their investigations.
(d) Vaccination data is shared with other parts of the health sector for outreach purposes
(e) Medical warnings data is shared CARM – the Centre for Adverse Reactions to Medicine.
(f) Details of young people diagnosed with cancer with the regional cancer network so that they can support those patients
(g) Information is shared with inter-agency groups focused on domestic violence, elder abuse and child safety
(h) some of our systems are interconnected e.g. the National Health Index (NHI) so that updates made by in one system (e.g. a name or address change) may be widely distributed or made available to other parties. For example, an update to a patient's NHI record by a public hospital is then shared with a GP or other health providers. Hospitals submit ACC claims to ACC electronically.
(i) Other agencies share information with the public health sector. For example, the Department of Internal Affairs shares information about births and deaths with the NHI to enable records to be updated.

With respect to sharing of information via electronic information systems, two particularly significant examples of information systems currently being proposed for the public health sector illustrate the complexity of information sharing in the health sector are set out below.

- The Ministry of Health's National Health Information Platform (HIRA). HIRA will draw together a person's latest health data from multiple trusted source systems on a virtual platform to create a virtual electronic health record which can be accessed as needed. Patients will have better access to their health information and can control who they share information with. Providers will have secure, easy access to patient information, in the right context and at the right time. Individuals will not need to have direct engagement HIRA as role based access and business rule for recording individual consent for access will developed as part of the system. Tranche 1 of HIRA will provide access for providers and consumers to health information such as demographics such as gender, ethnicity, name and ate of birth, enrolled general practice, community service card entitlements, prescribed and dispensed medicines, Covid-19 vaccination status, lab test results and summary primary care data. Consumers will have the ability to update information in the National Health Index such as their contact details. Access will be via websites and apps. HIRA will continue existing arrangements where health care records are shared between providers to provide health care. If a provider is directly providing care to an individual (e.g. a GP providing care to a patient enrolled with their practice) and is or has been involved in the patient's care, then the provider will be able to access the individual's health information in HIRA. HIRA will also enhance and 3expand on information sharing practices like this. Over time it is expected that a wider group of health services will be able to access and contribute to shared Consumer health records via HIRA

  Similarly, the Hira system is designed to enable a connected a connected ecosystem of disparate data sources (Agency A) who have collected data from many people (Individual B). Other organisations (Agency C) will then connect to the Hira platform to access data from multiple data sources to create a new digital health service that provides value to New Zealanders. Agency C may not have a direct relationship with Individual B.

  The implementation of a notification pathway to individual B via an automated data platform would therefore be difficult if Agency C does not have a direct relationship with Individual B.

  Other questions arise out of the Hira example:

  - Would Agency A need to share more personal data than was required by Agency C so that Agency C could notify Individual B that they had their data?
  - Would that notification need to be via a phone call, an email, or a letter to their address, if Agency C has no other way of contacting Individual B?
  - Alternatively, would Hira need to require all data sources who connect their data to Hira to provide a mechanism to notify all Individual Bs every time their data was shared with Agency C? What if they don't have the technical ability to do this?

  It important to note that Hira is privacy enhancing as data access will often be only allowed by Individual B using Agency C's application and so Individual B will be providing explicit purposed based consent for their data to be accessed by Agency C

- The Regional Collaborative Community Care (RCCC) information platform. The Northern Region Districts of Te Whatu Ora (Northland, Auckland, Counties-Manukau and Waitemata) are commencing implementation of a regional information system. RCC will give individuals accessibility, visibility, control and choice over who accesses their information, make information from secondary and tertiary treatment providers accessible to workers in primary or community contexts and vice versa.

  An underpinning principle of RCCC is transparency, meaning that individuals will be able to see all the actions taken in relation to their care. RCCC is an example of such an information system. The goal of the system is to create greater cohesiveness and connection between individuals receiving care and the agencies/organisations involved in providing care to them. It will allow agencies/organisations involved in an individual's care to access information about that individual whether that information is held by the individual s primary (General Practitioners), secondary and tertiary health providers (hospitals and community health services), other government agencies (MSD, ACC etc) and non-government agencies (NGO). The increased connectedness will improve health outcomes for the individual, ensure more "joined up" services are

Difficulties with complying with a notification requirement include:
Potential difficulties with complying with a notification requirement must be considered. Difficulties include:

1. Inaccurate/out of date contact information

Te Whatu Ora does not hold accurate and up to date contact information for all the individuals about whom it holds information. This means we will not be able to notify all patients that we are sharing their information with a third party.

Contact information is generally checked and updated each time an individual has contact with the health system, but beyond this there is no r gorous process for ensuring that all contact details are accurate and up to date.

It is difficult to keep contact information up to date because some individuals have only infrequent contact with the health system, others leave New Zealand to live overseas, tourists or short term visa holders who were only ever visiting New Zealand return to their home countries. Some individuals are itinerant or homeless or provide false details for reasons which range from being illegal immigrants to avoiding arrest to being ineligible for free health care. Some individuals have simply moved house or changed email address or phone number since the last time they had contact with the health system.

There are also gaps for New Zealanders who die overseas could be New Zealanders, or those who have used health services while visiting NZ, because death registration information is not provided by other countries.

2 Overheads associated with notifying patients

There will be significant overhead in notifying individuals when information is transferred to third parties given the frequency of sharing and the large numbers of individuals whose data may be transferred. This overhead is not currently resourced.

For some individuals, Te Whatu Ora will have email addresses, for others only phone numbers and for many only their physical address. That means notification to all of the people whose data is being transferred to a third party will be via a range of communication channels. There is significant over head in that which is not currently resourced.

3. Shared contact details

How are agencies to comply with notification requirements where individuals have shared contact details?

Some people share an email address and phone number (eg spouses sharing one email address or a family using one email address). Some who live in rest homes give the phone number or email of the rest home they live in as their contact details. For most children, the contact details are those of their parents.

Will notification to whatever contact address an agency holds be sufficient, even if that address is shared?

4. Safety

How will safety be ensured if third party disclosures must be notified. For example, if a parent has protection orders against their partner because of family violence issues, how can the risk that the safety of the parent or the child will be put at risk through notification processes be mitigated. What about situations where a child is in the care of the State or has been adopted or where there are protection orders which specify that a parent is not to be told where their child is living? Will departures from the notification requirement be permitted in these kinds of situations?

Authority for sharing information

It is not clear whether/how the proposed requirement for notification will impact current provisions mandating or authorising information sharing. This is a significant concern for the public health sector as provision of timely and fully informed care is critically dependent on information flowing smoothly between health care providers.

Authority for sharing information is derived from a number of mechanisms including:

- direct consumer authorisation
- informing about information uses via privacy statements
- information used/shared for the purpose it was collected
- exceptions in Rule 11 of the HIPC
- statutory provisions mandating information sharing or giving a discretion to share

Multiple statutes allow or mandate the sharing of health information and by implication the indirect collection of information. Section 24 of the Privacy Act 2020 provides that nothing in IPP6, 11, or 12 limits or affects a provision in any NZ enactment that authorises or requires personal information and an action taken by an agency does not breach IPPS 1-5, 6-10 or 13 if the action is authorised or required by or under New Zealand law

As an example, section 22F of the Health Act 1956 makes it mandatory for a person/agency which holds health information about an individual to provide health information to any person who is providing or is to provide, services to that individual. Section 22F ensures that health care providers

are able to obtain the information they need to safely treat patients. Its scope is broad and is utilised by all manner of health care providers.

The party requesting information under section 22F will be collecting health information about the individual indirectly. It would appear that this indirect collection would activate an obligation to notify the individual if the proposed changes go ahead. Section 22F is a key mechanism for information sharing in the health sector which ensures that health providers are able to access information about patients they are treating, or anticipate treating, smoothly. Any erosion on section 22F through the proposed changes to IPP2 and 3 will seriously impact the health system's ability to provide safe and timely care to patients.

Another example would be the collection of information under Production Notices under the Search and Surveillance Act 2012 by departments of State, Crown entities, local authorities or other bodies that employ or engage enforcement officers as part of their functions. The Police regularly obtain Production Notices to gain access to information held by Te Whatu Ora Health New Zealand's hospital and community services. The Police are indirectly collecting the information they access via Production Notices. Will the Police be required to notify the individuals whose information they collect under Production Notices and how will any negative impact of a notification requirement on Police investigations be mitigated?

There is a mandatory requirement to share information with Oranga Tamariki on request under section 66 of the Oranga Tamariki Act and mandatory requirements for family violence agencies to consider sharing information about family violence under the Family Violence Act 2018.

If the proposal to require notification of indirect collection of information is adopted, section 24 should be amended so that there is clarity as to whether the requirement to notify applies to indirect collection of information under statutory provisions like section 22F of the Health Act 1956 and statutory processes like Production Notices under the Search and Surveillance Act 2012.

The proposed changes to IPP 2 and 3 have the potential to disrupt an established set of public sector processes where information is shared in order to deliver health care services and improve health and social outcomes. Te Whatu Ora submits that careful consideration needs to be given to the impact of the proposed changes on a complex sector like health. The Ministry of Justice must understand the sector at depth and in detail to truly appreciate the impact of the proposed changes.

We suggest that consideration be given to creating an exception to any notification requirement similar to that in Rule 11(2) of the Health Information Privacy Code where compliance "… is not necessary if the health agency believes on reasonable grounds, that it is either not desirable or not practicable to obtain authorisation from the individual concerned …"

Impact will differ markedly depending on which of the proposed options is adopted

The proposed options for notification are broad and impacts will differ depending on which of the options is adopted. For instance, the requirement for notification may only apply to organisations collecting data about people overseas or may apply broadly to all third party sharing of information within NZ.

The effects will be significantly different for health sector and other government organisations depending on which option is chosen.

If the changes were to apply only to personal information collected indirectly from individual overseas, this would simplify things considerably and reduce the compliance overhead for domestic

health sector organisations. If this change would be sufficient to retain GDPR equivalency which is the stated driver for the proposed changes, it would be a significantly less disruptive option and probably favoured in the health sector context

Impact on urgent sharing

Sometimes information must be shared urgently in order to provide life-saving treatment to an individual patient or to protect the life/safety of individuals or public safety. Sharing in such situations may occur under section 22F of the Health Act 1956 or under the serious threat exceptions in IPP 11(1)(f) and Rule 11(2)(d) of the Health Information Privacy Code

Clarity is required as to whether notification will be required for disclosures in urgent circumstances.

Requirements for notification must be clearly defined

If the proposed notification requirement is introduced, there must be clear guidance in IPP2 and 3 as to what is required to comply with the requirement. The guidance should cover issues such as:

- What information must be contained in a notification
- Whether notification be considered effective if sent by email or post to the last known address for an individual
- Whether notification by public notice in the news media or on social media be permissible as a backstop when current contact details are not held
- Whether providing specific information about intended uses and disclosures of data at the point of collection be required or communicating a broader set of purposes at the point of collection be sufficient.

To illustrate, in the case of HIRA, it is proposed that standardised privacy notice materials will be produced and provided/made easily available to, individuals including via providers. Notification may also be provided through web-based explanations and a variety of accessible media, including video and verbal presentations may be used. In other words, a layered privacy notice approach is proposed.

It will be critical for the agencies designing and promoting a new information platform like HIRA to know whether measures like these will comply with the notification requirements for indirect collection.

Will notification be effective in ensuring transparency?

The examples of sharing in the health sector I have provided demonstrate the extent of sharing. Individuals are therefore likely to receive large numbers of notifications. Notification fatigue is likely to set in and bring into question the mechanism's effectiveness as a tool for achieving transparency.

Other tools for achieving transparency?

The proposal does not appear to have considered other options for achieving transparency. Giving individuals access to the systems in which their data is held so that they can see for themselves what data is held and who has accessed it would be a more effective way of achieving transparency and avoid issues like notification fatigue.

Carter, Adam

From: Barry Thom <barry@uprealestate.co.nz>
Sent: Wednesday, 28 September 2022 10:57 am
To: Privacy Feedback
Subject: MOJ submission

To whom it may concern

Re: The REINZ submissions to the MOJ

I am writing as the Principal for UP Real Estate. I have read the MOJ proposed changes to the Privacy Ave and the response by the institute, which we support.

Given the requirement by the Real Estate Agents Authority to supply a likely selling range to prospective vendors prior to listing, it would seem the MOJ proposal is undermining such requirement.

The ability for both buyers and sellers to source sale outcomes is fundamental to our duty of care and fairness to both customer and client.

Given that the current system is well known, acknowledged and accepted and has been in play without issue for years, I can't see a practical reason of the need for change.

Regards

Barry Thom
AREINZ
Principal

Grant Lynch
Managing Director

M s9(2)(a)
barry@uprealestate.co.nz

T 09 529 1478 F 09 529 1223
2 Dilworth Ave, Remuera
Auckland 1050, New Zealand
PO Box 28848

Licensed Agent REAA 2008

Carter, Adam

From: Roanna Vining s9(2)(a)
Sent: Wednesday, 28 September 2022 12:22 pm
To: Privacy Feedback
Cc: Phil Robson; Carissa Tarrant
Subject: Unity Submission - Broadening the Privacy Act's Notification Rules

Good afternoon,

Unity is a Credit Union, based in Hastings, with branches and a member base across NZ – from Auckland to Invercargill. We handle personal information as a key part of how we do business. We are very aware of our current obligations under the Privacy Act, and we strive to ensure these are met.

We have reviewed the current consultation by the Ministry of Justice - Broadening the Privacy Act's Notification Rules. We have several clarification questions around the potential impact of the proposed changes:

1. As a general point, clarity is needed around what would need to be disc osed to our members and when. (Note – Members are people who transact, deposit and borrow money from us). E.g. - what is meant by 'collecting' information? Would 'receiving' information (e.g. through a referral), be treated in the same way as 'collecting' information ourselves? We receive referrals from financial brokers as part of our core business operations, which is discussed further in point 2 below. Would receiving this information necessitate a notification to the individual concerned, regardless of whether they go on to be a member?
2. We currently receive approximately 300-500 broker referrals per week for Unity services, each referral is a different individual, and contains PII. These individuals have already agreed to disclose their PII to lending institutions such as Unity via their engagement and agreement with a broker. The additional requirement to notify potential members that we have received their information seems to double up on the proposed requirement to notify individuals, as they have already agreed to the disclosure of information through the broker.
3. Should 'receiving' information be included as 'collecting' information? If so, this would see an increase in compliance costs for the business and also add, we believe, unnecessary complexity to our operations. Given these individuals are informed at the broker referral stage of how their PII will be used and disclosed, we consider that an additional notification from the receiver (us) is unnecessary.

We look forward to reviewing a summary of submissions and the final direction that MoJ choose to take for any future legislative change.

Kind regards,

Roanna

Roanna Vining - Operational Risk Manager

s9(2)(a)

Broadening the Privacy Act's notification rules - Submission – University of Canterbury

1. **What factors do you think are most important when considering changes to indirect collection of personal information?**

    - How many other third parties are being given the information?
    - What sort of companies are these?
    - Where is the information stored?
    - Is it being sold?
    - Does the company make money from this?

2. **What are the advantages or benefits of broadening the notification requirements, for both individuals and agencies? What might the disadvantages be?**

    Advantages:

    - Clearer for the individual who/what is using their information.
    - Better control for individuals of their own information.
    - Particularly relevant in NZ as most info stored overseas which has implications around sovereignty/jurisdiction.
    - Might be clearer for the Agencies, they may not know what is happening at this stage, may not be clear to them what they are doing, or this may be clear to an individual/team within an organisation, but not clear to the wider organisation e.g. Management.

    Disadvantages:

    - Notification fatigue, people will stop caring e.g. the way cookies are now notified globally. It is good to know, but most people just click agree.
    - There is the potential that this will scare people out of using technology which is to their benefit otherwise.
    - There is the potential that people will miss important notifications e.g. a privacy breach of their information where they should be doing something, as they will be used to seeing (and ignoring) lots of notifications.

3. **What form do you think the proposed changes to notification rules under the Privacy Act should take? Please elaborate on your preferred option and explain why you think the other options are not appropriate.**

    We think that a new privacy principle should be introduced as this will be simpler than changing the already well understood principles. Changing these would muddy the water. This would also be in line with the approach taken under the last Privacy Act amendments/changes to the principles.

4. **If you are a New Zealand business, are there any practical implementation issues you can identify in complying with the proposed changes?**

Compliance costs to implement this across the nation could be large.

5. **Are there any other risks or mitigations to the proposed changes you can identify that are not mentioned in this document?**

   NZ shouldn't get out of synch with Australia in terms of their notification requirements in this space. A large proportion of NZ business records and information are stored in the Australian jurisdiction and a large proportion of businesses are trans-Tasman. To get out of step with them would be setting up the companies to fail or have a dual system.

6. **Should the proposed changes only apply to personal information collected indirectly from individuals overseas, or should they also apply to personal information collected indirectly from individuals in New Zealand?**

   Should apply to all. If you are going to do this it should be for everyone.

7. **Is there any other feedback you would like to provide on these proposed changes? If so, please provide this feedback.**

   It is not clear to us at this stage how a business would implement these changes and what this would practically look like. With the way that info is on-sold and the ability to set up shell companies how would this work and how would this be monitored for compliance?

Title: Draft submission for broadening of notification requirements of the Privacy Act

To: Electoral and Constitutional, Ministry of Justice

From: Privacy Assurance, Resilience and Assurance Services, Ministry of Justice

Date of submission: 2022

Context

The Ministry of Justice is seeking submissions from agencies on broadening the current notification requirements under the Privacy Act. Specifically, on broadening the current notification requirements, impacts and which Information Privacy Principle (IPP) 2, 3, or 11 should be amended to reflect this.

Currently, agencies are not required to notify individuals if they receive information about an individual from another agency.

The change to the current Act is intended to align the Privacy Act more closely to the EU GDPR (European Union General Data Protection Regulation). It will also provide better protection and greater transparency of usage of an individual's personal information in Aotearoa.

Current Information Privacy Principles

(Source: Office of the Privacy Commissioner | Privacy Act 2020 and the Privacy Principles)

IPP2

Personal information should be collected directly from the person it is about. The best source of information about a person is usually the person themselves. Collecting information from the person concerned means they know what is going on and have some control over their information.

It won't always be possible to collect information directly from the person concerned so organisations can collect it from other peop e in certain situations. For instance:

- if the person concerned authorises collection from someone else
- if the information is collected from a publicly available source
- if collecting information from the person directly is not really practicable or would undermine the purpose of collection.

Sometimes, information can be collected from other sources for law enforcement and court proceedings.

IPP3

Organisations should be open about why they are collecting personal information and what they will do with it. This principle is about helping people understand the reasons you are collecting their information.

When an organisation collects personal information, it must take reasonable steps to make sure that the person knows:

- why it's being collected

- who will receive it
- whether giving it is compulsory or voluntary
- what will happen if the information isn't provided.

IPP11

An organisation may generally only disclose personal information for the purpose for which it was originally collected or obtained. Sometimes other reasons for disclosure are allowed, such as disclosure for a directly related purpose, or if the person in question gives their permission for the disclosure.

For instance, an organisation may disclose personal information when:

- disclosure is one of the purposes for which the organisation got the information
- the person concerned authorises the disclosure
- the information is to be used in a way that does not identify the person concerned
- disclosure is necessary to avoid endangering someone's health or safety
- disclosure is necessary to uphold or enforce the law.

Submission

IPP3

This is Privacy Assurances' preferred option as it:

- currently covers notification requirements for individuals, specifically, the purpose of collection and the recipient(s) of their personal information
- could be adapted reasonably easily to include the extended notification requirements

Potential impacts and challenges

Citizens

- individuals discover their information has been shared with another agency/used by an agency without their consent
- citizens lose trust in the government's ability to be transparent or appropriately care for and protect individuals' personal information
- citizens refuse to share information or are slower to share information due to lack of trust
- citizen access to community services is delayed by notification processes
- notification overload for the individual

Community service providers/NGOs

- reduced levels of service as staff are diverted into administering notifications
- lower compliance with Privacy Act
- increased rates of errors notifying individuals
- decrease in trust with NGOs and Community providers as they struggle to notify individuals appropriately and efficiently

Agencies

- increase to workload for Privacy/Legal/Policy/Information management/Senior Leadership teams to draft/review/approve new notification
- increased administration by Privacy teams to update guidelines, policies, processes, training, and training material
- increase to ongoing workload to notify individuals

- increase to workload administering/investigating privacy breaches due to non-notification of personal information received through indirect collection
- lower levels of compliance with the Privacy Act e.g., lack of timely notifications to individual(s)
- may cause a downgrade of collection requirements from highly identifiable to anonymised, aggregated to the extent that notification to the individual is not required.

Office of the Privacy Commissioner

- increased administration/investigations relating to privacy complaints reported to the Office of the Privacy Commissioner (OPC) as individuals discover their information has been shared with another agency without their consent

Examples of scenarios and challenges

Scenario One - A non-government organisation (NGO) the Food Bank must notify individuals when they use information shared from the Ministry of Social Development and Ministry of Health to better support their clients.

- Challenges for NGOs may include:
    - staff are mainly part-time, volunteers with varying literacy levels and computer skills
    - no dedicated privacy professionals
    - small resourcing for dedicated office administration
    - availability of privacy guidance and training for staff
    - difficulty notifying clients if they are transient and mistrustful of agencies
    - difficulty notifying clients if they have limited literacy, have English as a second language, or have cognitive impairments, or disabilities
- Increase of privacy breaches through:
    - no anonymisation of personal details
    - difficulty obtaining consent for personal information to be shared
    - re-use of personal information shared without consent

Scenario two - Ministry of X wants to publish 'good news' stories in their agency newsletter. Ministry X contacts abc community group for stories.

Challenges may include:

- Notification process
    - Increased administrative burden for smaller agencies with limited resources to make notifications in a timely and appropriate manner to individuals
    - Ministry of X have low privacy maturity and generally do not follow/promote good privacy practices so will give this low priority over more immediate privacy issues
- Increase of privacy breaches through:
    - no anonymisation of personal details
    - difficulty obtaining consent for personal information to be shared
    - re-use of personal information shared by Ministry without consent

General recommendations and suggestions for broadening notifications

- Joint development of a generic statement by GCPO/Privacy Commissioner/SPWG:
    - for all agencies to use which will cover off the primary collection and any on-sharing of personal information with other agencies

- Suggested statement “Agency A is collecting personal information from you for the purpose of x, y, z. Agency A will also share this personal information with Agency B. Agency B will use this information for a, b, c.”

- Notification process:
  - notify once - at the start by the primary agency (who originally collected the information)
  - the individual is notified by the primary agency collecting information as per usual process AND they are also told that the information supplied by them will be shared with other (named) agencies for a specific purpose (high level description)
  - if recipient agency on-shares information with another agency, they MUST notify the individual concerned
  - include a timeframe for notifying individuals – as soon as practicable or within set timeframe prior to use
- Include an opt out preference if that is applicable or appropriate, i.e , information is voluntary, unless it is a legal requirement to collect/share this information
- Information sharing agreements written before the broadening of the notification process will not be amended
- Information sharing agreements after the amendment to an IPP (yet to be specified) will name agencies it will share information with, purpose for sharing and how/why the agency will use this information