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