Proposed approved information sharing agreement between Inland Revenue and MBIE: detecting questionable business practices

By email: policy.webmaster@ird.govt.nz

The Privacy Foundation of NZ welcomes the opportunity to make a submission on this proposal.

General comment on information sharing and AISAs

The Privacy Foundation agrees that it is important for government agencies to work together to provide better and more efficient public services, including sharing information where appropriate. It is often frustrating for people and businesses to be asked to repeat information that could easily be shared for clear and acceptable purposes. Duplication in government systems can also be inefficient and unnecessarily costly.

However, people generally do not have a choice about whether to deal with government, or to supply the information that government asks for. There is also an inherent power imbalance between the State, with its significant powers, and individuals or entities. As a result, government agencies have a particularly strong obligation to act as a responsible and trustworthy custodian for the information that they collect and use.

This means that it is important:

- for any sharing of personal information to have a clear and justified purpose, and to be supported by clear legal authority
- for information sharing systems and processes to be designed to operate safely
- for both the shared information and any new information or insights to be accurate and fit for purpose
- for agencies to be transparent with the public about what is shared and why
- to give people an adequate opportunity to correct any errors in the information, and to have a say before adverse action is taken (for instance, enforcement action).

The Approved Information Sharing ("AISA") model under the Privacy Act 2020 is specifically designed to manage all of these privacy issues successfully and to ensure that government information sharing is well designed and trustworthy. The Privacy Act does not *bar* sharing (as the paper suggests in places): in fact it *permits* sharing. We agree with the positive assessment of the benefits of AISAs in the paper at pages 9-11 of the paper. However, AISAs are under-utilised. It is therefore excellent to see Inland Revenue and MBIE proposing a new agreement.

Comments on the consultation

The Privacy Foundation would welcome being specifically informed about consultations such as this in future. As a small not-for-profit organisation, we do not have systems that can easily scan websites for consultations in which we may be able to contribute a valuable perspective. We only found this one by accident, and have had a very limited time to look at it so we may have misunderstood some aspects of what is being proposed. We hope, however, that our comments are useful.

Lack of PIAs in consultation pack

We notice that IR and MBIE have not included a privacy impact assessment as part of the consultation pack. This is unusual, as it makes it harder for submitters to see whether the potential privacy risks have been adequately identified and addressed in the proposal. The AISA itself is obviously one major privacy control (addressing both legal authority and some operational details). But it is not the only control required.

We would anticipate that there should be several separate privacy risk assessments covering each of the different use cases listed in chapter 3 of your paper. It is important both that that analysis is done and that the agencies are transparent with the public about the results of that analysis.

Even though the consultation closes today, we therefore **recommend** that IR and MBIE:

- publish any current privacy impact assessments relating to this proposal
- and update those privacy impact assessments to reflect any changes made as a result of the consultation

Phoenix companies

We agree that the issue of phoenix companies is a significant one and that sharing certain types of information may help to detect and prevent such behaviour.

The paper accurately identifies that 'phoenixing' creates economic, taxation and consumer protection problems. We would add that it also often creates significant problems for workers in those businesses, and may mask exploitative behaviour by business owners.

We note, however, that information sharing in itself will not directly resolve the wider aspects of the problem, at least in the short term. This is because, as the paper states, there are different definitions of "phoenix company" only a limited range of which are addressed in the current Companies Act (see section 386B). The sharing will only allow enforcement in a limited number of cases.

However, this does not mean that the sharing is not worthwhile. As the paper states, there is a lack of data about business patterns that can broadly be defined as "phoenixing". Sharing information will allow for an analysis of such patterns, which

could then be used as an evidential basis for legislative change to clarify definitions. The sharing may also indicate breaches of duties in other areas, such as breaches of directors' duties.

As long as the information to be shared is clearly identified and accurate, sharing for this purpose appears justified.

Compliance and enforcement

On the surface, information sharing to support the compliance and enforcement activity reflected in the paper seems sensible. The types of information to be shared (as noted in chapter 3) also seem to be clearly targeted at achieving the desired purposes.

However, it is not clear from the paper what the barriers are to information sharing at the moment. We are aware that the Tax Administration Act sets out a general prohibition on sharing tax information unless there is an AISA in place (or another exception applies). The current proposal would therefore resolve that issue.

However, we are unclear what the barrier is from MBIE's side. In particular, without being able to see a PIA, we have not seen the analysis that suggests the existing exceptions in the information privacy principles of the Privacy Act are insufficient to allow the agencies to fulfil the purpose (though this may be the case). Also if, for instance, there are *legislative* prohibitions on sharing information that sits behind the published fields on a public register (eg for Insolvency or for Companies), then an AISA will not solve the problem. That would require a legislative change: an AISA cannot be used to override primary legislation.

Nor is it always clear exactly *what* information would be shared to resolve the problem. Some references in chapter 3 – especially to 'information relevant to offences' (category 5) - are very high level. Some items, like sharing policies and guidelines relevant to enforcement, can be shared anyway: an AISA is not needed. And it is not clear what itemised information about individuals or businesses would be shared. For example, would it just be information that an investigation into a named director or entity was under way, or would it extend to sharing investigation files or even undertaking joint investigations? The category 5 information listed in the AISA suggests the latter (or something approaching it) is the case. If so, the legal and privacy safeguards required are much more significant than they would be with the former level of sharing. The operational protocols will need to be very specific about how such shares will operate and what safeguards are in place to ensure the sharing is fair and accurate.

Supporting the Official Assignee

Sharing of the information detailed in Chapter 3 (category 8) may well be justified for the reasons detailed in the paper. However, unlike many of the proposals, these arrangements will predominantly affect individuals, rather than businesses. The privacy

implications are therefore more significant for the bankrupted person. Obtaining greater access to tax-related information about those people is an incursion into an area that is generally perceived as private. It is important that those people are fully aware that this share will happen and what the effect on them might be. Given that the information was gathered for different purposes, it will also be important to ensure that it is fit for the purpose to which it will be put by the Assignee. Use of information beyond the purposes for which it was originally collected can create inaccuracies that can disadvantage individuals and that need time and resources to iron out.

Sharing of deaths information is clearly something that is desirable from an estate management perspective, and to prevent unnecessary and potentially distressing regulatory contact with surviving family or business partners. However, it is somewhat surprising that the Assignee is proposing to acquire deaths information from Inland Revenue (3.93). There are existing sharing arrangements for deaths information with the Department of Internal Affairs (the core system owner for such information, and therefore the best source of 'truth'). While we appreciate that there is a pragmatic opportunity to include this type of information in the share, getting it from a secondary source increases the chances of errors perpetuating through the system. It would therefore be preferable to get deaths information direct from DIA.

Providing information to New Zealand businesses

We agree that it is desirable for businesses to get clear and targeted information that helps them to comply with their obligations easily and get any support that may be available.

However, it is unclear from the paper why information sharing under an AISA would be needed to fulfil this purpose. Also, an evidential basis for the value of such sharing may exist as a result of the COVID-19 experience referred to in paragraph 2.16, but the paper does not reflect it.

To the extent more information may be needed, it is not clear why MBIE does not *already* hold sufficient contact information or industry segment information that would allow it to conduct targeted or tailored information campaigns. Alternatively, the agencies could work together to develop guidance and information for agencies and the agency with the best contact and segmentation information could send it on behalf of both of them.

Admittedly, the stated intention appears to be largely neutral from a privacy perspective, so our concerns are limited. With the exception of sole traders, it will often involve company information rather than personal information (though we note that the information may also involve employees to some extent). Also the proposal is targeted at providing advice that is useful for businesses, rather than taking action against them. However, it is important to ensure that any information shared is ring-fenced for the stated purpose of assisting businesses. Re-using that information for compliance

purposes would certainly give rise to concerns as it would raise completely different privacy issues that would need to be resolved.

Policy development

It appears likely from chapter 3.5 that the intention is not to share new information but to state that policy development is an alternative permitted purpose for using the shared information. If that is correct, then that seems sensible. If new information were to be shared, however, then we could not comment about whether the share was justified without further details about what that information would be.

We note that using other options such as research use of the rich business information held by StatsNZ may also negate the need for direct information sharing between IR and MBIE for policy development purposes (or at least may limit what needs to be shared). It is undesirable to build up new databanks where the information is already made available for the purpose elsewhere in the government system.

Parties to the AISA

We agree that it is both necessary and desirable to specify the branches in MBIE that are parties to the AISA rather than having MBIE as a whole designated as a party. That specificity allows for greater control over the information that is to be supplied and the permitted uses of that information. The AISA framework in the Privacy Act allows for an AISA to be with one or more parts of an agency, and that is appropriate here.

As the paper notes, names of business units can change over time. However, the AISA framework allows for minor and technical changes (such as name changes) to be made easily without consultation beyond the Privacy Commissioner's office, as long as the change does not introduce new privacy risks. We would therefore oppose any move to make the information more generally available.

Disclosures within MBIE

With that in mind, though, we note that clause 9(b)(ii) of the AISA permits disclosures of the information within MBIE "as long as that is reasonably necessary for a lawful business purpose connected to the purposes of this Agreement". That phrase is open to a wide variety of interpretations about what a business purpose connected to the purposes of the Agreement might be, including much broader sharing within MBIE than could be anticipated from the fairly tight justifications presented in this paper. Some of those onward shares may create very different privacy implications and require different safeguards that will not be provided under the AISA. Tax-related information is also generally more closely held.

As a result we **recommend** that at this stage, clause 9(b)(ii) should be **deleted**. It is entirely foreseeable that onward sharing for directly related purposes within MBIE might be justifiable. However, those shares should be designed based on evidence of need rather than by giving a broad permission to share in this AISA, bounded only by a general reference to having some kind of shared purpose. The clause has the capacity to defeat the benefits of being specific about MBIE's business units as parties to the AISA and to inadvertently circumvent the privacy protections that the AISA provides.

If – or more probably when – a clear case for sharing the information is developed, this AISA can be adapted to meet that need transparently and clearly, using the amendment mechanisms in the Privacy Act.

The form of the AISA and operational protocols

The AISA appears to be an "umbrella" AISA, incorporating a variety of shares for a variety of purposes listed in Chapter 3. By their nature, umbrella AISAs are stated in fairly general terms. Core privacy safeguards such as requirements to be met before taking adverse action (here, clause 6 and schedule 2 of the AISA), and protections against onward disclosure (here, clause 9(b)) are included. But the way in which the shares actually operate are not set out in detail. Instead, those details are commonly captured in 'operational protocols' that sit under the AISA. Existing examples include the AISA between Inland Revenue and the Ministry of Social Development, and the multi-party Gang Harms Insights Centre AISA.

While this is a much more efficient approach than developing many (here, nine) separate AISAs governing shares for separate purposes, it creates some privacy risks that need to be carefully managed.

The first risk is the potential for scope creep. If the AISA designates fairly broad categories of information to be shared and broad purposes for the sharing, that often leaves significant room for discretion about expanding shares over time, provided that the agencies stay within the designated parameters. However, this proposed AISA is designed to mitigate the possibility of scope creep: it usefully incorporates a very specific schedule (schedule 1) detailing what can be shared for what purposes. This is a useful model for other agencies to follow in future.

The second risk is the potential lack of transparency for the public when the details of individual shares are contained in operational protocols rather than in the AISA itself. While AISAs themselves have to be published on the lead agency's website (and reported on in their annual report), operational protocols are generally not published. Yet the devil, as they say, can be in the details. From the perspective of public trust, it is also desirable to be as completely transparent about information shares as possible.

We therefore strongly recommend that IR and MBIE commit to **publishing** the resulting operational protocols, with the sole proviso that they should withhold any details that could:

- compromise the security of the share (or the security of the underlying systems)
- or allow those under investigation to evade compliance action.

We hope that these comments are helpful as you consider these proposals.

Katrine Evans
Chair, Privacy Foundation of NZ Inc.