



NEW ZEALAND
LAW SOCIETY

NZLS EST 1869

Enhancing Identity Verification and Border Processes Legislation Bill

26/10/2016

Enhancing Identity Verification and Border Processes Legislation Bill

1 Overview

1.1 The New Zealand Law Society welcomes the opportunity to comment on the Enhancing Identity Verification and Border Processes Legislation Bill (Bill). Its comments relate to the proposal to introduce a new Part 10A (Identity Information) to the Privacy Act 1993.

1.2 The Law Society submits that:

1.2.1 No clear policy rationale supports the introduction of proposed Part 10A. The Government Inquiry into Matters Concerning the Escape of Phillip John Smith/Traynor (Inquiry)¹ did not identify any barriers in the Act that prevented information sharing;² rather the Inquiry noted that the cultures of the relevant agencies primarily explain why information was not shared. The introduction of Part 10A cuts across the legislative design of the Privacy Act, which is based on generic Information Privacy Principles (IPPs) and generic mechanisms for the enforcement, adjudication and accommodation of the IPPs.

1.2.2 If Part 10 A proceeds despite the absence of a compelling rationale for its introduction, then it needs to be amended in several respects so as to provide greater protection of privacy interests.

2 Part 10A: Identity Information

Need for new Part 10A questioned

2.1 Clause 6 of the Bill introduces a new Part 10A of the Privacy Act, authorising specified agencies to access and use identity information, including biometric information, to verify the identity of individuals within the justice system and at the border, for law enforcement purposes.³

2.2 New Part 10A authorises accessing agencies,⁴ when carrying out specified functions, to verify the identity of an individual by accessing identity information held about that individual by a holder agency.⁵ An accessing agency can only have access to an individual's identity information for the purposes specified in schedule 4A and only from the specified holding agencies set out in schedule 4A (see s 109D).⁶

Existing mechanism preferred – Part 9A of the Privacy Act (AISAs)

2.3 It is unclear why the Bill proposes a new Part 10A, rather than using existing information sharing mechanisms under the Privacy Act.

¹ Government Inquiry into Matters Concerning the Escape of Phillip John Smith/Traynor, August 2015, <https://www.ssc.govt.nz/sites/all/files/report-inquiry-escape-phillip-smith-traynor-aug2015.pdf>.

² The Privacy Act has well established principles which guide agencies in how to look after personal information (which includes identity information); Privacy Principle 11 allows an agency, at its discretion, to release information where it reasonably believes that it is necessary to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences.

³ Explanatory Note to the Bill, p1.

⁴ The accessing agencies are set out in schedule 4A: Corrections, Department of Internal Affairs. MBIE (Immigration), Ministry of Health and Health Boards, New Zealand Customs Service, and New Zealand Police.

⁵ The holding agencies are also set out in schedule 4A, which are, in addition to the above agencies, the Ministry of Justice, and the New Zealand Transport Agency.

⁶ For example, an access request from the Ministry of Health or District Health Boards can only be to Department of Corrections, Department of Internal Affairs, MBIE (Immigration), and New Zealand Police.

- 2.4 It is possible that Part 10A is seen as a practical measure to avoid the need for agencies to draft separate approved information sharing agreements (AISAs) under Part 9A of the Privacy Act.
- 2.5 After an exhaustive and fully consulted review, the Law Commission recommended the AISA process as an acceptable compromise between administrative convenience and protection of privacy.⁷ However, the effect of this Bill is to create an alternative mechanism that circumvents many of the carefully crafted protections that the Law Commission devised.⁸ These provide checks and balances on the process of information sharing between government agencies.
- 2.6 The rationale for this Bill circumventing the AISA mechanism is not clear. It has not been demonstrated that AISAs could not work to facilitate the sharing of identity information between this group of agencies, or that AISAs would be unreasonably time-consuming or impractical to develop.
- 2.7 For example, the matters listed in the schedule could probably be dealt with by six AISAs (one for each accessing agency or group of accessing agencies). Each could use the same basic template to avoid duplication, which could then be adjusted as necessary to cater for the differences between the sharing arrangements. The same agencies are involved throughout, which would reduce the time required for consultation and negotiation.
- 2.8 The Law Society supports the reasoning of the Law Commission, and suggests that AISAs provide the best framework to use for the sharing of identity information. On this basis the Law Society submits that new Part 10A should not be introduced.
- 2.9 There is also a legislative design reason not to proceed with Part 10A. The core structure of the Privacy Act is based on generic IPPs, enforced and managed within a generic framework. The introduction of a specific Part to deal with a very narrow and specific problem will set a precedent that may see the Privacy Act become a patchwork of bespoke regimes. That would undermine the working of the Act.

New Part 10A omits certain protections that are important when sharing identity information

- 2.10 However, if Parliament proceeds with the proposed new Part 10A, rather than requiring agencies to use the AISA mechanism, it is important to add sufficient protections to Part 10A to ensure that future arrangements are equally justifiable and proportionate and that privacy is properly considered and protected.
- 2.11 The key privacy protections that should be added to the proposed Part 10A (or to individual statutory provisions) are set out below.

Include processes to ensure greater transparency and public accountability

- 2.12 It is important the public can see what arrangements are in place to share identity information, and can be confident that those arrangements are justified. This is particularly the case with highly sensitive identity information such as biometrics.

⁷ Section 96A enables the sharing of personal information to facilitate the provision of public services, and it is recognised that information sharing agreements reduce any uncertainty about whether personal information can be lawfully shared for the provision of the public services, and in what circumstances.

<http://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20MB2.pdf>

⁸ The privacy enhancing features of Part 9A are transparency, the form and content of the agreement (including minimising interference with privacy), consultation, high level approval (order in council), operation of the information sharing agreement including notice of adverse action as a result of receiving the information, responsibilities, reporting and review.

- 2.13 A major advantage of the AISA arrangements in Part 9A of the Privacy Act is that the agreements themselves must be in writing and must be made available, including on a publicly accessible website (section 96S). The lead agency is also required to report regularly on the operation of the agreement (section 96T).
- 2.14 The proposed schedule 4A usefully brings together information about the permitted purposes for the sharing and the agencies that can disclose and receive identity information. These are important limitations on the sharing of information and it is important to maintain them. However, the schedule falls well short of the transparency provided as part of the AISA framework. In particular:
- 2.14.1 It does not state that information sharing is in fact occurring, or between which agencies – it just provides authority for it to occur.
 - 2.14.2 It does not require agencies to document their underlying information sharing arrangements and to make those details available to the public.
 - 2.14.3 It does not require agencies to report on the operation of the information sharing arrangements, either to the public or to the Privacy Commissioner. For instance, there is no obligation to report on how much sharing occurs, whether it has proved effective, or whether problems with false positives have arisen and been corrected.

Include a requirement to notify individuals before taking adverse action in certain circumstances

- 2.15 The proposed Part 10A does not require agencies either to provide notice of adverse action to individuals, or to justify why notice is not appropriate in the circumstances of the sharing arrangement.
- 2.16 Agencies are generally required to provide individuals with notice before taking adverse action against them on the basis of information shared under an agreement (see in particular section 96Q and section 103 of the Privacy Act). This is an important backstop right, particularly in circumstances where, as here, misidentification or other errors can have serious consequences for individuals. The individual should in principle have an opportunity to correct information in a timely way, before it affects them in a more lasting manner.
- 2.17 Sharing of identity information will not always, in itself, lead to “adverse action” against an individual (see the definition in section 97 of the Privacy Act). However, in most instances proposed by this Bill, it is likely to be an integral part of investigating whether the individual has committed an offence, or taking action against them (for example prohibiting travel).
- 2.18 On occasion, there are sound reasons for notification to be waived or delayed or for the notification period to be shortened. For example, this Bill deals with several instances where urgent action is required, or where notification may prejudice the maintenance of the law.
- 2.19 However, the legislative starting point should still be that agencies should be required to provide notice of adverse action. If there is a reason to depart from that either on all occasions or under some conditions, the agency should be required to justify its stance and record the reasons for its inability to notify (see section 96R of the Privacy Act).

Include specific obligations to identify and mitigate privacy risks

- 2.20 Sharing identity information will contain some privacy risks that are common across all programmes. It may be possible to address such risks in a uniform way. However, different information-sharing projects are also likely to create their own risks.

- 2.21 For example, if the quality of identity information held by particular departments is poor or incompatible, sharing that information may raise particular risks of error that require additional checks. Also, the sensitivity of identity information will vary according to the context of the transaction.
- 2.22 It is therefore important to require agencies to undertake an individual – even if brief – analysis of each sharing arrangement to identify whether specific privacy safeguards are required and, if so, to include those safeguards in their sharing arrangements (see for instance section 96(2)(d) of the Privacy Act).
- 2.23 Parliament has already acknowledged that undertaking such analysis is important in the field of biometric information. In particular, section 32 of the Immigration Act 2009 requires the Ministry of Business, Innovation and Employment to complete and publish a privacy impact assessment for the collection and handling of biometric information, and to update it when processes change. Such a provision is notably absent from other legislation amended by this Bill, including the Customs and Excise Act 1996.

Include criteria that the responsible Minister must consider before recommending amendment of schedule 4A

- 2.24 The proposed schedule 4A dictates which agencies can share personal identity information and for what purposes. It is the terms of the schedule that dictate the extent to which privacy can be compromised in the interests of border control, or other situations in which government agencies wish to verify or link identity. As mentioned earlier, those situations will often involve adverse action against the individuals concerned.
- 2.25 The terms of schedule 4A can be amended by way of Order in Council; the result is that the number of agencies and the purposes for which information can be shared can be increased by Order in Council, without Parliamentary involvement. As with all Henry VIII clauses, it is important that such a provision be properly justified and, if it proceeds, be made subject to appropriate safeguards.
- 2.26 The contents of the schedule contained in this Bill have emerged from in-depth consideration of existing gaps in border sector and law enforcement information sharing by the independent Inquiry. There is therefore a reasonably sound basis on which to claim that the particular information sharing listed in the schedule is necessary, proportionate and likely to be effective. However, there is no guarantee that future amendments to the schedule if made by Order in Council will have been equally thoroughly considered.
- 2.27 If the schedule can be too readily amended, the restrictions that it is supposed to place on sharing of identity information may prove to be largely illusory. The requirement to consult with the Privacy Commissioner is useful – indeed, essential – but consultation alone does not ensure that changes to the schedule are justified. The Commissioner may make public statements if he or she is dissatisfied, but has no power of veto. Parliamentary oversight, through the Regulations Review Committee, is also useful but is limited.

Recommendation

- 2.28 The Law Society therefore recommends that either:
- the power to amend schedule 4A by Order in Council is deleted; or
 - if that power is to be retained, there should be additional legislative controls on the process of changing the schedule, to ensure that amendments to the schedule have been properly considered and that they do not unjustifiably intrude into personal privacy.

- 2.29 If the latter option is to be adopted, a useful precedent exists in section 96N of the Privacy Act. That section sets out matters to which the relevant Minister must have regard before recommending an Order in Council relating to an AISA. Those matters are (slightly paraphrased):
- (a) that the information sharing will facilitate the provision of a public service;
 - (b) that the type and quantity of personal information to be shared under the agreement are no more than is necessary to facilitate the provision of that public service;
 - (c) that the agreement does not unreasonably impinge on the privacy of individuals and contains adequate safeguards to protect their privacy;
 - (d) that the benefits of sharing personal information are likely to outweigh the financial and other costs of sharing it; and
 - (e) that any potential conflicts or inconsistencies between the sharing of personal information under the agreement and any other enactment have been identified and appropriately addressed.

Recommendation

- 2.30 The Law Society therefore recommends that if the power to amend schedule 4A is retained, an equivalent to section 96N is included in proposed new Part 10A to govern the process of amending the schedule. This will require the Minister to be satisfied that amendments to the schedule are justified and proportionate. Such a provision will make it less likely that the amendments will create unnecessary privacy risks, or that they will need to be called into question through other review mechanisms.

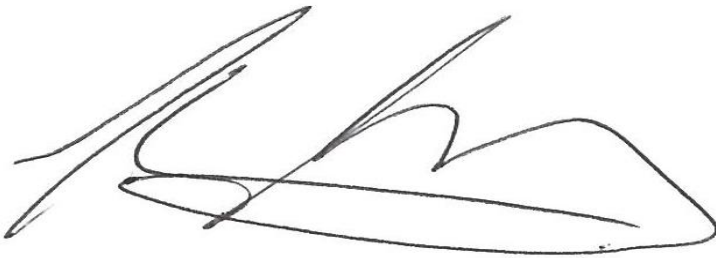
Particular care is needed with biometric information

- 2.31 The Law Society accepts that identification of people can be significantly assisted by biometric information. It also accepts that agencies may need to maximise certainty with respect to identification in the situations that this Bill is intended to cover.
- 2.32 However, particularly important privacy interests are at stake with biometric information,⁹ which underscore the Law Society's recommendations in relation to this Bill, namely that:
- 2.32.1 The collection and use of biometric information must be transparent, using a "privacy by design" approach.
 - 2.32.2 If there is any doubt about whether the biometric information is accurately matched to the correct person, it should either not be shared, or the sharing should be accompanied by a strong caution that it may not be accurate. Failure to do this could create mistakes (false positives) that can prove difficult or impossible for the individual to correct, and cause significant distress, inconvenience and other harm.
 - 2.32.3 While biometrics can be useful, they are not perfect. Some biometric information cannot be accurately recorded – for instance a person may have damaged fingerprints, or disfigured facial features. People should not suffer discrimination or unjustified suspicion simply on the basis of an automated matching process that may be inaccurate.

⁹ As outlined in the Law Society's submission on the Customs and Excise Act Review – Discussion Paper 2015, 1.5.15 http://www.lawsociety.org.nz/__data/assets/pdf_file/0009/90369/l-Customs-and-Excise-Act-Review-1-5-15.pdf.

- 2.32.4 The minimum amount of biometric information necessary for identification in specific circumstances should be determined, and only that amount of information should be shared.
- 2.32.5 Automatic access to data by recipient agencies such as Police should be carefully assessed. Citizens do not have to provide their biometrics to all agencies unless particular conditions (such as arrest) or particular statutory provisions apply. That right should not be changed without clear justification and providing direct access to biometric databases creates particular risks of circumventing limitations that exist for sound reasons. While this Bill sets out some situations in which automatic access may be more justifiable than in the general course of affairs, it is important to restrict the ability to broaden access in the future (for example by amending schedule 4A).
- 2.32.6 The use of biometrics should not become a unique identifier across government.
- 2.32.7 It is essential to ensure security of biometric information, as compromised biometrics can prove particularly difficult to correct and can have serious adverse consequences for the individual.

The Law Society wishes to be heard.

A handwritten signature in black ink, appearing to read 'Kathryn Beck', written in a cursive style.

Kathryn Beck
President
26 October 2016