Australian Privacy Foundation

post: GPO Box 1196
Sydney NSW 2001
email: mail@privacy.org.au
web: www.privacy.org.au

Verifying Identity under the AML-CTF Act 2006 – Privacy Impact Assessment

Submission to the Commonwealth Attorney-General's Department via IIS Consultants

August 2009

The Australian Privacy Foundation

The Australian Privacy Foundation is the main non-governmental organisation dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians. Since 1987, the Foundation has led the defence of the right of individuals to control their personal information and to be free of excessive intrusions. The Foundation uses the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed. For further information about the Foundation and the Charter, see www.privacy.org.au

Introduction

APF welcomes the commissioning of the Privacy Impact Assessment (PIA) and the opportunity that is being given for input before legislation is tabled. In our submissions to the ALRC Privacy Inquiry, we argued for the issue of access to credit reporting information for AML-CTF Act e-verification to be dealt with as a wider identity management issue rather than simply by means of amendments to the Privacy Act. We are pleased that the ALRC accepted this and that as a result the issue is now being addressed primarily by means of AML-CTF Act amendments, together with any consequential Privacy Act changes.

However, we are disappointed with two aspects of the Consultation document.

Firstly it fails to canvass the alternative sources that are or may be available for e-verification. The document merely invites submissions on this issue, whereas we would have expected the consultants to have identified other sources and expressed a professional opinion as to whether they achieve the objectives and whether they are more or less privacy intrusive than the current proposal. This would have been consistent with our preference for this issue to be addressed in the context of wider identity management strategies. The consultants have not taken the opportunity to do this. We are disappointed that much of the discussion in the ALRC Report preceding Recommendation 57-4 has not been carried over into the consultation paper, meaning that we have to raise the same points again and that stakeholders are not reminded of all the issues.

Secondly, the document accepts unquestioningly the use of the term 'consent' in the proposed amendments. The consultants, and AGD, will be aware, not least from ALRC Report 108, that there is a major issue about the meaning of 'consent' and its use in privacy law. We submit that in the current proposal, a requirement to seek consent for e-verification would be meaningless if some reporting entities, as expected, use the new provisions to make e-verification the only

option for their customers. In such circumstances, it would be more appropriate to require specific notice of the proposed e-verification (involving both disclosure and collection of personal information), and perhaps express acknowledgement of this by the customer. Inappropriate use of 'consent' is unfortunately embedded in the credit reporting provisions of the Privacy Act (Part IIIA), but this error should not be replicated in the proposed AML-CTF Act amendments.

Specific Issues and Questions

We challenge the statement in the description of the proposal, on page 3 of the Consultation Document, that 'a reporting entity will not be able to obtain any information from the credit reporting agency's file.' We understand the intent of this being a re-assurance that no information *other than* the confirmation of identity will be disclosed. However, whether an enquiry results in a simple yes/no answer or a score (see later) we contend that information will still have been disclosed. While this may seem like a semantic point, it is a significant one in privacy terms and we are disappointed that the consultants have not ensured that the proposal description is more accurate. It would be unfortunate if this error was carried forward into the Explanatory Memorandum or Second Reading speech.

1. Whether the proposal will result in organizations … gaining access to new information…

We submit that the suggested characterization of the proposal as not involving any new information is not correct. Underlying this characterization is a simplistic assumption that individuals have only one 'correct' name, date of birth and address combination. We submit that in many cases, e-verification with credit reporting agencies would be likely to result in them receiving information about new or different addresses and in some cases also name variations (and possibly but rarely different dates of birth).

2. Whether the proposal will result in individuals having the same …. control…

Apart from the misleading use of 'consent' discussed above, we submit that individuals may not be offered the option of an off line means of verification. We understand part of the rationale for the proposal is to allow businesses which operate *only* online to be able to verify customer particulars (although any business, whether transacting with its customers online or not, could use e-verification) .

We acknowledge that a positive result of the proposal might be to replace existing online identity verification schemes which are not subject to the requirements and penalties for misuse of Part IIIA. But we would require more analysis of this, with examples of such existing schemes, to be able to make informed comment.

3. Whether credit reporting information is sufficiently accurate …

We submit that there are likely to be major data quality issues arising from the proposal which would need to be addressed. – See our comments on issue 5 below.

4. Whether there are other existing means of electronic identity verification …

As already noted above, we believe that more information needs to be provided about other existing schemes to inform consideration of the proposal. It should not be left to submissions to identify these other schemes – it is part of the job of the consultants to do this, and look forward to seeing these findings presented and analysed in the final PIA report. We are aware that reporting entities are currently using a range of sources for verification, but also that there may be some doubt about the legality of some sources, including existing use of credit bureau information. The PIA should explore this.

5. What the consequences of rejection might be.

This is a critical issue. Rejection (failure to verify) could have significant adverse consequences for individuals. Any amendments should clearly limit the secondary uses that organizations (including credit reporting agencies) could make of the result of the verification request. There should also be an express requirement to report any rejection to the individual concerned, whether or not the organization making the request seeks other evidence of identity. These two controls would address, for instance, the situation where an organisation fails to verify a prospective customer's identity and decides to decline to continue with the application/transaction.

6. Whether use of a scoring system …. provides a more viable option …

If scoring is to be permitted it should be clear what level of verification (criteria) is acceptable. It may be that this is prescribed elsewhere in the AML-CTF Act or subordinate instruments (Rules etc). It would have been helpful to see this analysed in the consultation document. We submit that the final PIA report should explain and analyse the discretion allowed to reporting entities to apply a scoring system rather than an exact match decision.

Consistent with our response to issue 5, we also submit that organisations should not be permitted to make wholly automated decisions about individuals without reporting results of verification requests to them.

7. Whether or not there is on balance benefits … from the proposal.

Consumer and financial counselling NGOs are in a better position to comment on the question about marginalizing individuals without credit histories. We hope that they have been consulted and that there will be an assessment of this risk in the final PIA report.

In relation to the suggestion that e-verification could become unduly focused on credit reporting information when other more effective mechanisms are not explored, we refer to our general concern about inadequate analysis of other options, and our responses to issues 2 & 4 above.

8. Whether there are harms or benefits … that have not been so far identified.

We submit that the final PIA needs to address the wider issue of the potential privacy 'harm' from the introduction of yet another means by which individuals are pressured into using a single 'identity' descriptor (name and address combination and specification). Any proposal for the use of one set of personal information, collected and held for a specific purpose, for unrelated secondary purposes inevitably raises privacy issues and brings with it unavoidable data quality and matching problems.

We suggest that the final PIA report needs to canvass these wider identity management issues. The report could also usefully make reference to the existing body of guidance on data-matching. It may be, for example, that the Data matching Guidelines issued by the Commonwealth Privacy Commissioner could be usefully applied to any e-verification activity allowed under this proposal.

For further contact on this submission please contact
Nigel Waters, Board Member
E-mail: Board5@privacy.org.au

Please note that postal correspondence takes some time due to re-direction – our preferred mode of communication is by email, which should be answered without undue delay.