Australian Privacy Foundation

email: mail@privacy.org.au

website : www.privacy.org.au

Combating the Financing of People Smuggling and Other Measures Bill 2010: Exposure Draft

Submission to the Commonwealth Attorney-General's Department

December 2010

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

This submission covers both the remittance and e-verification aspects of the Bill, but there is also a precursor issue.

Misleading Title of the Bill

The proposed legislative reforms are concerned with the broader issues of improper use of remittances and of identity e-verification, relevant to all offences covered by the AML-CTF Act (which itself has a misleading title, given the breadth of offences now covered and uses to which AUSTRAC information is put). People smuggling is an illegal activity that may or may not involve improper use of Australia's financial system. By highlighting only one offence, the current title is uninformative and misleading and should be amended to more properly reflect the intent and content of the Bill, which is to modify the administrative machinery associated with Australia's financial monitoring law.

Remittance Providers

The proposed amendments broadly reflect the need to regulate remittance providers who have been identified as a source of improper and illegal transfer of funds in and out of Australia, and the objective

of relieving the compliance burden and cost of the regime on the remittance sector without undermining its objectives. For the most part the proposed provisions appear well drafted. However, we endorse the following two comments made by Liberty Victoria:

- Under the Bill, the AUSTRAC CEO will be given broad powers to deregister (Clause 75G(1)) or choose not to register a remittance provider (Clause 75C(4)) where satisfied that they pose a significant risk of money laundering, financing terrorism or people smuggling. While these are necessary powers, 'significant risk' should be defined.

- As is increasingly common in such legislation, a failure by the regulator to advise those being regulated of a decision does not invalidate the decision. In contrast, the failure of a remittance provider to comply with a notice requirement may give rise to civil and criminal penalties. Principles of good government dictate parity of regulation and further, that penalties should only be imposed where there has been an intentional or at least negligent contravention of the legislation.

Identity e-verification

APF welcomes this being addressed in the AML-CTF legislation rather than just in the Privacy Act – a point we made in our submissions to the ALRC privacy review and reflected in Recommendation 57-4 (ALRC Report 108, 2008)

APF commends the Department for having commissioned a Privacy Impact Assessment (PIA) to assess the impact of using credit reporting entities for e-verification purposes, and for allowing the consultant assessors to consult with interested parties (Consultation Document dated July 2009). APF, as well as several other civil liberties and consumer rights organizations, provided written comments in August 2009, which we attach to this submission (Attachment A). We note that some of the concerns raised in our submission have been addressed (and welcome this) but others have not.

We particularly welcome the requirement that reporting entities must obtain an individual's express consent before disclosing his or her personal information to a credit reporting agency. In the PIA process, we expressed concern that where an individual was not given any alternatives, 'consent' became a meaningless term. Clause 35A(2)(c) now requires that the reporting entity must provide an individual with an alternative means of verifying their identity. This is not only important in this specific context but is also a welcome and overdue recognition of the general principle that where consent is to be relied on as a legal authority, it should be genuine, free and informed.

We particularly welcome Clause 35C which requires reporting entities to notify individuals where they are unable to verify the identity of an individual following an e-verification request. However, it is not clear what 'unable to verify' means in the context of the provision for an assessment of the 'extent of the match' (of name, address and date of birth), rather than a simple yes/no response (Clause 35B) – this is explained in the Explanatory Memorandum as allowing for an assessment score e.g. a percentage. It is also unclear what 'score' or level of match resulting from e-verification will be acceptable under the legislation's customer identification requirements, as implemented in the AML and CTF Rules Instrument

2007, Part 4.2. Without knowing these thresholds, the notification safeguard in Clause 35C cannot be effective.

Matching of identity information is a complex task and one which runs up against the reality that many individuals legitimately operate under multiple identities. Government agencies frustration with this reality, and attempts to suborn individuals into accepting a single 'official' identity are at the heart of many privacy issues. As we said in our comments to the PIA assessors, "It may be … that the Data matching Guidelines issued by the Commonwealth Privacy Commissioner [but aimed primarily at Commonwealth agencies] could be usefully applied to any e-verification activity allowed under this proposal." We seek confirmation that this will be the case.

We also welcome the requirement that personal information obtained through identity e-verification must be stored separately (for 7 years) with Credit Reporting Agencies prohibited from including verification information in credit information files (Clauses 35D, E & F) and only used for that purpose or as otherwise authorized by law, with unauthorised access, use or disclosure made an offence (Clauses 35H, J & K). These controls are welcome, although we note that they are of course subject to future legislative amendment, and that history shows that such function creep is likely as new uses are found for this valuable resource of personal information.

We also restate our concern, expressed in our submission on the PIA, that it may be unrealistic in practice for credit reporting agencies not to use at least some of the information obtained from AML-CTF e-verification requests for other purposes. Given their data quality obligations under the Privacy Act, will CRAs not be put in an impossible position of having a reasonable suspicion that information in their credit information files is inaccurate or incomplete yet not being able (under the AML-CTF Act – Clauses 35D & K) to make use of that information even to make follow up enquiries? We seek feedback on whether the CRAs have raised this as an issue of concern and if so how it will be addressed.

APF is pleased to note clause 35L which states that a breach of the requirements of the Division constitute an interference with privacy under section 13 and 13A of the *Privacy Act 1988,* although the value of that safeguard will be undermined by continued weak enforcement of that Act – we refer to our submissions the ALRC privacy review, to the government on its response to the ALRC, and to the current inquiry into Online privacy by the Senate Committee on Environment, Communications and the Arts.

APF appreciates the opportunity to comment on the exposure draft Bill and looks forward to its further refinement.

Attachment A – APF Submission to the Privacy Impact Assessment, August 2009

Contact for this submission: Nigel Waters, Board Member, Australian Privacy Foundation
Email: Board5@privacy.org.au; Telephone: 0407 230342

Please note that APF no longer has a dedicated postal address. Our preferred mode of communication is by email, which should be answered without undue delay. If postal correspondence is required, please contact us by email or phone to obtain an address.