PARLIAMENTARY JOINT COMMITTEE ON LAW ENFORCEMENT
ATTORNEY-GENERAL'S DEPARTMENT

Inquiry into Financial Related Crime

Written Questions on Notice

Received 2 February 2015

1. Does the Attorney-General's Department agree with the evidence presented by Northern Territory Police that the decision in *Momcilovic v The Queen & Ors* [2011] HCA 34 encourages state and territory police to use Commonwealth legislation to charge and prosecute for certain crimes? (See: Committee Hansard, 8 September 2014, p. 7; Committee Hansard, 9 September 2014, p. 56). If so, what are the implications of this trend?

The answer to the committee's question is as follows:

No.

2. Has the Attorney-General's Department provided guidance to the states and territories through COAG processes or through another mechanism or forum? If not, are there plans to do so?

The High Court's *Momcilovic* decision has been considered by the Standing Council of Attorneys-General (SCAG) and the Standing Council on Law and Justice (SCLJ), and by justice agency officials through the National Justice CEOs forum (NJCEOs) and the National Criminal Law Reform Commission (NCLRC).

At the meeting of the Standing Council on Law and Justice in April 2012, Ministers asked the NCLRC to undertake work to review existing means for avoiding constitutional inconsistency between Commonwealth, State and Territory criminal laws and, if necessary, develop new proposals for avoiding such inconsistency.

In June 2013, following advice from the NCLRC, the NJCEOs agreed that this project required no further consideration on the basis that the risk of inconsistency was low.

3. Has any State or Territory Government sought advice from the Attorney-General's Department in relation to the Momcilovic judgement?

The Commonwealth Attorney-General's Department does not provide legal advice to State or Territory governments.

4. Does the Momcilovic decision require a national policy response to clarify any uncertainties for Commonwealth, State and Territory law enforcement agencies? Is the Attorney-General's Department undertaking any review in relation to the Momcilovic judgement?

No.

5. Does the Attorney-General's Department wish to make any additional comments with respect to the use of Commonwealth offence provisions by state and territory police forces?

No.

6. Has the Attorney-General's Department given consideration to:

a. including ASIC as an interception agency under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) or

Interception agencies are able to apply for an interception warrant to investigate serious offences (offences with a penalty of at least seven years' imprisonment). Given the highly intrusive nature of this power, interception agency status is restricted to Commonwealth and State and Territory law enforcement and anti-corruption bodies (currently the Australian Crime Commission, the Australian Security Intelligence Organisation, the Australian Commission for Law Enforcement Integrity and the Australian Federal Police). Restricted access to interception powers has been supported by successive Parliaments, including by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in its 2013 *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation.*

ASIC cannot apply for an interception warrant in its own right to gain access to real time content. However, an interception agency may disclose intercepted information to ASIC to further that interception agency's own investigation, including in the course of a joint investigation with ASIC. In such circumstances, any information obtained by ASIC during the investigation can only be used for the purposes of that joint investigation.

b. including ASIC as eligible to receive 'lawfully intercepted information', pursuant to s 68 of the TIA Act?

The TIA Act strictly regulates what agencies may do with information collected under an interception warrant and restricts the giving of interception information to particular agencies for the purposes set out in section 68 of the Act. ASIC is not specifically included in that section, which means that intercepted information cannot be communicated to ASIC for ASIC to use in its own investigations and prosecutions. However, as outlined above, ASIC can receive information from an interception agency as part of a joint investigation for the purposes of that joint investigation (pursuant to sections 67 and 73 of the Act).

The limitations imposed by the TIA Act on information sharing were considered by the PJCIS in its 2013 Report. The PJCIS recommended that the Attorney-General's Department review the information sharing provisions of the TIA Act to ensure protection of the security and privacy of intercepted information, and sharing of information where necessary to facilitate investigation of serious crimes or threats to national security (Recommendation 8).

The findings of the PJCIS are currently being considered by the Senate Legal and Constitutional Affairs References Committee as part of its inquiry into the proposed reform of the TIA Act. That Committee is scheduled to table its report on 18 March 2015

7. Is a review into the operation of the TIA Act under consideration?

In recent years the TIA Act has been reviewed several times. The 2013 Report of the PJCIS made 18 recommendations relating to the TIA Act. Currently, the Senate Legal and Constitutional Affairs Committee is undertaking a broad review of the TIA Act and the PJCIS' recommendations. The Government will respond to the findings of that Committee after it reports on 18 March 2015.

In addition, the PJCIS is undertaking a review of the proposed mandatory data retention scheme, which includes significant changes to the legislative scheme governing agencies' lawful access to non-content telecommunications data.

8. The Australian Bankers Association has advocated that banks be able to discuss with law enforcement the contents of search warrants, as opposed to handing over everything, including potentially unrelated material. Does the Attorney-General's Department have a response to this? (see: Committee Hansard, 9 September 2014, p. 5).

The Attorney-General's Department does not support the Australian Bankers' Association's proposal.

Any person or organisation that is party to a police investigation is required to comply with relevant laws. The Department does not support creating specific arrangements for banking institutions, as distinct from other organisations or individuals, during investigations of criminal matters. In order to effectively investigate suspected criminal behaviour, it is important that law enforcement should have timely access to all relevant information, irrespective of the nature of the organisation that is in control or possession of that information.

9. What is the Attorney-General's Department's view on the possibility of making taskforces like Operation Wickenby ongoing, to permanently enhance inter-agency co-operation?

This is a matter for Government.

10. Does the Attorney-General's Department have a view on the closure of remitters' bank accounts in Australia? (see: Committee Hansard, 9 September 2014, pp 27–35).

Australian banks' decisions to close remitters' accounts reflect their own, and in some instances their international partner banks' assessment, of the money laundering, terrorist financing and sanctions risks.

Australian financial institutions are required to assess the money laundering, terrorist financing and sanctions risks associated with the services they provide and implement appropriate measures to mitigate and manage those risks. The Department considers that the assessment of risk should not be arbitrary and should be conducted on a case by case basis. This position is confirmed in the statement issued by the Australian Transaction Reports and Analysis Centre (AUSTRAC) in November 2014. The statement can be found at the AUSTRAC website < www.austrac.gov.au >.

11. In evidence to the inquiry, Veda advocated that private sector financial service providers should be given access to the Document Verification System (DVS), 'We ask that the committee recommend the development of a policy framework to ensure that government agencies, including law enforcement agencies, can share suspected fraud data and have confidence in the private entities they share it with.' (see: Committee Hansard, 9 September 2014, p. 36). Does the Attorney-General's Department have a view on whether the DVS should be open to any user with a reasonable requirement to identity verification and the lowering of the per user access fees?

The Attorney-General's Department has proposed to States and Territories via the Law Crime and Community Safety Council that the DVS should be open to use by any organisation that:

- has a reasonable requirement to identify a person to conduct their business, and
- obtains that person's consent, consistent with the revisions to the *Privacy Act 1988* that came into effect in March 2014.

The Attorney-General's Department expects to implement the new access policy for all jurisdictions that have agreed to these arrangements in March 2015.

The Attorney-General's Department and State and Territory governments have also reviewed the process for applying for access to the DVS. The Department will implement a substantially simplified application process in March 2015. The per user access fee will be significantly reduced as a result.