



16 November, 2010

File:

Mr John Hawkins
Secretary
Senate Economics Legislation Committee
Parliament House
CANBERRA ACT 2600

Dear Mr Hawkins

CORPORATIONS AMENDMENT (NO 1) BILL 2010 — TREASURY RESPONSE TO QUESTIONS TAKEN ON NOTICE

I thank the Committee for providing Treasury the opportunity to appear before it in relation to its consideration of the Corporations Amendment (No 1) Bill 2010 (Bill). Treasury's responses to the questions taken on notice are below.

Penalty for a company not providing a copy of the register requested under subsection 173(3) of the *Corporations Act 2001* (Corporations Act)

A company is required to provide a copy of a register within 7 days of a request. Failure to comply with this provision is a strict liability offence, with a penalty of 10 penalty units (\$1100) or 3 months imprisonment or both [subsection 173(9A)].

Reporting requirements under the *Telecommunications (Interception and Access) Act 1979* (TIA Act)

The *Telecommunications (Interception and Access) Act 1979* (the TIA Act) maintains the integrity of the telecommunications interception regime by imposing a number of record-keeping and reporting obligations on interception agencies who utilise telecommunications interception for the investigation of serious offences defined in the TIA Act.

Statistical reporting

Section 94 of the TIA Act requires Commonwealth agencies to report to the Attorney-General (as the Minister responsible for the TIA Act), on an annual basis, in relation to exercising their powers to apply for interception warrants and other associated powers. Commonwealth agencies must provide a wide range of information, including:

- the number of applications for warrants they have made
- the number of warrants issued to them
- the offences in relation to which each warrant was issued, and
- the number of prosecutions and convictions arising from the use of intercepted information.

Division 2 of Chapter 2 of the TIA Act sets out in detail the range of information required which includes effectiveness reporting and information regarding the duration and costs of interception. These figures are combined into a report, which is subsequently tabled in Parliament by the Attorney-General.

Operational reporting

In addition to statistical reporting, section 81 of the TIA Act also requires Commonwealth agencies to provide a report to the Attorney-General in relation to each interception warrant issued on:

- the use made by the agency of information obtained by interceptions under the warrant
- the communication of such information to persons other than officers of the agency
- the number of arrests that have been, or are likely to be, made on the basis of such information, and
- an assessment of the usefulness of information obtained by interceptions under the warrant.

These reports must be provided to the Attorney-General within three months of the warrant ceasing to be in force.

The reporting requirements in the TIA Act are augmented by detailed record keeping requirements which are subject to the Commonwealth Ombudsman for Commonwealth interception agencies and the respective State Ombudsman for State agencies. All Ombudsman reports are provided to the Attorney-General.

Record keeping and reporting by the Attorney-General – General and Special Registers

Commonwealth agencies are required to provide to the Attorney-General a copy of each telecommunications interception warrant issued to that agency, and each instrument revoking such a warrant.

Section 81A of the TIA Act requires the Secretary of the Attorney-General's Department to maintain a General Register of Warrants which includes particulars of all telecommunication interceptions warrants. The particulars to be recorded are:

- the date of issue and period for which the warrant was to be in force
- the agency to which the warrant was issued and the Judge or nominated AAT member who issued the warrant
- the telecommunications service to which the warrant relates
- the name of the person specified in the warrant as the person using or likely to use the telecommunications service
- each serious offence in relation to which the Judge or nominated AAT member who issued the warrant was satisfied on the application for the warrant, and
- for named person warrants, the name of the person to whom the warrant relates and each telecommunications service that is specified in the warrant, or in relation to which interceptions authorised by the warrant have occurred.

The Secretary of the Attorney-General's Department must deliver the General Register of Warrants to the Attorney-General for inspection every three months. Interception agencies are notified once the Attorney-General has inspected the General Register to enable the destruction of restricted records.

Section 81C of the TIA Act requires the Secretary of the Attorney-General's Department to also maintain a Special Register of Warrants recording the details of telecommunications interception warrants which did not lead, directly or indirectly, to a prosecution within three months of the expiry of the warrant. The Secretary must deliver the Special Register to the Attorney-General for inspection every three months together with the General Register.

Offences currently listed in the TIA Act

When the TIA Act was enacted, it enabled the issuing of warrants for investigations relating to drug trafficking. Overtime, the TIA Act has been expanded to provide powers to a wider range of agencies, including State police forces and anti-corruption bodies. This has led to a corresponding expansion in the offences for which an agency can investigate with the assistance of telecommunications interception.

Section 5D of the TIA Act provides an exhaustive list of the offences in relation to which an agency can apply for a telecommunications interception warrant. An extract of section 5D is attached.

As a general rule, the TIA Act limits access to telecommunications interception to investigate offences which carry a penalty of at least seven years' imprisonment and encompassing conduct including:

- murder;
- kidnapping;
- importing and exporting border controlled drugs or border controlled plants;
- loss of a person's life;
- serious personal injury;
- serious property damage;
- arson;
- trafficking in prescribed substances;
- fraud;
- money Laundering;
- cartel offences;
- loss to the revenue of the Commonwealth, a State or the ACT; and
- bribery or corruption of or by an officer of the Commonwealth, a state or a territory.

Warrants are available for additional offences that do not meet the penalty threshold. These are generally offences which are committed within a telecommunications network (such as unlawful access to computers) as well as offences in matters which are particularly heinous (such as child pornography offences).

Use of information obtained under a telecommunications interception warrant for the prosecution of other offences

Section 63 of the TIA Act places a general prohibition on the use or disclosure of information that has been obtained by way of an interception (including whether an interception has even taken place). The TIA Act then lists specific exceptions to this prohibition.

Information can be disclosed to a different agency for a permitted purpose pursuant to section 67 or 68 of the TIA Act either to further the agency's current investigation or in relation to a separate investigation.

Section 67 of the TIA Act enables an interception agency (such as the AFP) to communicate the information for a permitted purpose in relation to the agency that applied for the warrant. A permitted purpose is exhaustively defined in section 5 of the TIA Act. It generally allows using and disclosing information to further the investigation and the prosecution of any offence which carries a maximum penalty of at least three years' imprisonment, or an offence which the TIA Act authorises an agency to apply for a warrant, as set out in section 5D of the TIA Act (see question number 3).

Any person that receives information (such as the ACCC in a joint investigation) can only use the information for the purposes for which it was received under section 73. This means that should the receiving agency cannot use the information for their own purposes or to further their own investigations.

Use of technologically neutral language for the formats in which a copy of the register is provided

The use of technologically neutral language for the formats of copies of a register is aimed at ensuring companies cannot frustrate legitimate uses of registers.

By specifying the formats in the *Corporations Regulations 2001*, rather than the *Corporations Act 2001*, there is scope to update the formats if required. Treasury is continuing to consult with stakeholders regarding the appropriate wording to be used in the regulations and notes the Committee's concerns that the language be technologically neutral.

Australian Government Investigation Standards

The Australian Government Investigations Standards (AGIS) provide best practice case handling standards. The standards are applicable for the investigation of fraud and other appropriate matters (for example, the investigation of offences against the Commonwealth). The guidelines set out standards for investigators and procedures for investigations, and draw attention to legislative obligations that should be complied with when investigating offences.

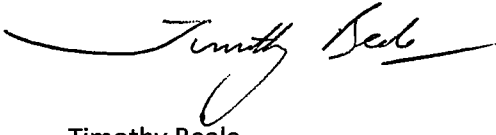
All Commonwealth agencies that are required to comply with the Commonwealth Fraud Control Guidelines must also comply with the minimum standards for investigations set out in AGIS. The Commonwealth Fraud Control Guidelines apply to all agencies covered by the *Financial Management and Accountability Act 1997* (the FMA Act) and bodies covered by the *Commonwealth Authorities and Companies Act 1997* that receive at least 50 per cent of funding for their operating costs from the Commonwealth.

The Financial Management and Accountability Regulations 1997 prescribe the Australian Securities and Investments Commission (ASIC) is prescribed as an FMA Act agency. As an FMA Act agency, the Commonwealth Fraud Control Guidelines apply to ASIC, and therefore the AGIS also apply to ASIC.

Any use of by ASIC of its powers, such as applications for and execution of search warrant would be conducted in compliance with these standards.

I trust that the foregoing answers the questions on notice arising from the Committee's recent hearings on the Bill.

Yours sincerely

A handwritten signature in black ink, appearing to read "Timothy Beale", with a long horizontal flourish extending to the left.

Timothy Beale
Manager
Governance and Insolvency Unit
Corporations & Financial Services Division

enc