CDPP
Australia's Federal Prosecution Service

Commonwealth Director
of Public Prosecutions

GPO Box 21
Melbourne VIC 3001
Level 16 460 Lonsdale Street
Melbourne VIC 3000
DX. 446
Telephone **03 9605 4333**
Facsimile 03 9670 4295
www.cdpp.gov.au

15 September 2015

Ms Karen Chester
Chair
Capability Review Panel
The Treasury
GPO Box 89
SYDNEY 2000

Via email: capabilitypanel@treasury.gov.au

Dear Ms Chester

RE: CAPABILITY REVIEW OF THE AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION

I refer to the meeting on 11 September 2015 held between yourself and other members of the Capability Review Panel with the Director Mr Bromwich SC and myself of this office, and to your request for me to forward some further written submissions as to some of the issues raised in that meeting.

Receipt by ASIC of lawfully intercepted telephone material

As stated in the meeting held on 11 September, ASIC is not an 'interception agency' as defined in the *Telecommunications (Interception and Access) Act 1979* ['TIA'] and as such cannot receive lawfully intercepted telephone intercept material ['TIs'] for the purposes of its own investigations.

An application for a warrant under Part 2-5 of the TIA Act can only be made by an 'interception agency'. In effect, that is defined in section 5(1) to mean:

- the Australian Federal Police (AFP);
- Australian Commission for Law Enforcement Integrity (ACLEI)
- the Australian Crime Commission (ACC); or
- an "eligible authority of a State" in respect of which a declaration under section 34 is in force.

For the purposes of Chapter 2 of the TIA, *'agency'* means an interception agency. *'Interception agency'* in turn is defined in s. 5(1) to mean:

(a) except for the purposes of section 6R, Part 2-6 or Chapter 5:
    (i) a Commonwealth agency; or
    (ii) an eligible authority of a State in relation to which a declaration under section 34 is in force; or

(b) for the purposes of Part 2-6:
    (i) a Commonwealth agency; or
    (ii) an eligible authority of a State; or

(c) for the purposes of section 6R and Chapter 5:
    (i) the Organisation; or
    (ii) a Commonwealth agency; or
    (iii) an eligible authority of a State in relation to which a declaration under section 34 is in force.

Commonwealth agency means:

(a) the Australian Federal Police; or
(aa) the Australian Commission for Law Enforcement Integrity; or
(b) the ACC.

Part 2-5 [ss. 34 – 61A] of the TIA provides for applications for warrants to authorise an agency to intercept communications. Part 2-6 [ss. 62 – 79A] provides for dealing with intercepted information. The most relevant provisions in relation to provision of intercepted information are ss. 67, s. 68 and 73. Pursuant to s. 67 (1) an officer or staff member of an agency may, for a permitted purpose, or permitted purposes, in relation to the agency, and for no other purpose, communicate to another person, make use of, or make a record of lawfully intercepted information other than foreign intelligence information, or interception warrant information.

'Permitted purpose' is defined in s. 5(1) to relevantly mean a purpose connected with an investigation by the agency of a prescribed offence. 'Prescribed offence' means a 'serious offence', as defined in s.5D as an offence punishable by a maximum of at least 7 years.

Pursuant to s. 68 the CEO of an interception agency may communicate lawfully intercepted material to specified other agencies. ASIC is not one of the specified agencies. Section 73 of the TIA limits the use of information provided in accordance with section 67 to use for the purpose or purposes for which it was communicated to the agency.

If an interception agency and ASIC form a joint task force, then the interception agency may share TI material with an officer from ASIC who is part of that joint task force, as pursuant to s. 67 of the TIA an officer who lawfully holds TI material has the power to communicate it to another person for a 'permitted purpose', being a purpose that includes a purpose connected with an investigation being conducted by that officer's agency in relation to a prescribed offence. In a joint task force situation,

where for example the AFP and ASIC are working together to investigate a prescribed offence, the AFP may be able to use section 67 to communicate TI material to officers from ASIC who are part of the joint task force.

The effect of sections 67 and 73 of the TIA is that an ASIC officer who receives TI material as part of a joint task force can only use that material in order to assist the interception agency (for instance the AFP) in the investigation that is being carried out by that agency. The ASIC officer cannot use the material to assist in any separate investigation being conducted by ASIC. Furthermore, as part of a joint task force, it is doubtful that ASIC can utilise its full suite of powers such as compulsory examinations pursuant to s.19 of the ASIC Act, as such power is dependent upon it being relevant to a matter ASIC is investigating or is to investigate.

ASIC is an 'enforcement agency', as defined in s. 5(1) of the TIA, as its functions include 'administering a law imposing a financial penalty', and thereby is able, pursuant to warrant issued under s. 116 of the TIA, to access stored communication data. However the definition of 'stored communication' excludes a communication that passes over a telecommunications system.

It is in the areas of market misconduct/manipulation, financial services fraud and insider trading offences, being offences with a maximum penalty of 10 years imprisonment [s.1041A–E, s.1043A in Part 7.10 of the *Corporations Act 2001*] that the significance of TI material is most acute. ASIC has primary responsibility for monitoring and investigation of such conduct, and those offences all fall within the definition of 'serious offence' in s. 5D of the TIA. But as ASIC is not an 'interception agency', it cannot obtain warrants to lawfully intercept telecommunications. Most significantly, ASIC cannot receive lawfully intercepted information from interception agencies for its own investigations, but only as part of a joint task force. The AFP and ACC can investigate alleged offences contrary to the *Corporations Act*, and may use lawfully intercepted TI, but they cannot commence a prosecution for an alleged breach of the *Corporations Act* without first obtaining Ministerial approval [s. 1315].

A recent example of such prosecution is that of Messrs Kamay & Hill for insider trading [and other] offences. This was a joint AFP and ASIC investigation into Australia's largest insider trading case, and resulted in significant custodial terms for both accused. The significance of TI evidence was demonstrated in that matter, albeit the primary evidence was evidence lawfully recorded by way of authorised surveillance device. It is fair to say that but for the lawfully recorded conversations there may not have been a prosecution. The importance of capturing the conversations of the accused at the time of the offending, being offending conduct that is typically covert and often coded or equivocal [e.g. SMS/text messages], rather than trying to investigate a matter some months or years post conduct, was critical to not only enabling the prosecution to prove the offences, but also to enabling the AFP to bring the conduct to an end via arrests, preventing further damage to the integrity of the market. Presumably it was also a significant factor in both accused entering pleas of guilty.

The 2010 amendments

During the course of our meeting I also referred to the amendments made in 2010 by the *Corporations Amendment (No. 1) Act 2010* that increased the penalties from 5 to 10 years for Part 7.10 offences. Those offences were expressly included in the definition of 'serious offence' in s.5D (5C) of the TIA for the specific purpose of enabling interception information to be obtained and used in investigations and prosecutions for those offences.

When first proposing the amendments, on 28 January 2010 the then Minister for Financial Services, Superannuation and Corporate Law, Chris Bowen stated via a media release[1]:

> *'As part of the proposals, ASIC will be able to access telecommunications interception material collected by the Australian Federal Police under a court issued warrant'.*

Soon thereafter, on 3 February 2010 the Minister released a proposals paper, and on 20 May 2010 released an Exposure Draft of the Bill. The draft Bill inserted s. 5D(5C) into the TIA, including market offences as 'serious offences' in the TIA. Submissions to the Governance and Insolvency Unit, Corporations and Financial Services Division, Treasury, were to be made by 10 June 2010. In a media release dated 20 May 2010[2], the Minister stated:

> *'ASIC has been hamstrung in its ability to prove intentional misconduct without access to the sort of direct evidence that can be compelling, such as incriminating statements made in telephone conversations, emails or text messages'...*
>
> *'These changes will provide ASIC with access to the same sort of evidence already available to the Australian Competition and Consumer Commission, while putting in place appropriate safeguards, such as requiring any interception be conducted by the AFP under a judge issued warrant'.*

I note that the Chartered Secretaries of Australia submission to the Unit dated 10 June 2010 stated:

> *'CSA is of the view that the provision of telephone interception warrants in relation to the offences of insider trading and market manipulation is appropriate. CSA's view is that the authorities should be provided with the powers they need to investigate and successfully prosecute the offence of insider trading and market manipulation. CSA notes that the nature of insider trading and market manipulation is such that it may be very difficult to prove beyond reasonable doubt the existence of such conduct without evidence obtained through telephone interception warrants. CSA contends that the use of telephone interception warrants for the investigation of insider trading and market manipulation should be*

[1] Ministers.treasury.gov.au – media release no. 008 of 2010 'Greater powers to the corporate regulator to pursue market misconduct'.

[2] Ministers.treasury.gov.au – media release no. 059 of 2010 'Government releases draft legislation cracking down on insider trading and other market offences'.

supported for the same public policy reasons as their use in the investigation of money laundering and cybercrime'.

In the Second Reading Speech on 29 September 2010[3] the Minister stated:

> *'Insider trading and market manipulation can distort Australia's financial markets and cause serious harm to their fair and efficient functioning. These markets function best when information is widely dispersed and investors have confidence in their integrity.*
>
> *It is essential that the penalties reflect the serious impact that breaches of these provisions have on financial markets ...*
>
> *The bill also proposes to include the insider trading and market misconduct provisions in part 7.10 of the Corporations Act in the list of serious offences in section 5D of the* [TIA Act].
>
> *Insider trading and other market offences are difficult to investigate, as these offences by their very nature involve complex networks of people, technological sophistication and avoidance of paper and traceable communications. In addition, the transactions often occur in real time, meaning that telephone conversations are often the only evidence of the offence.*
>
> *This bill enables interception agencies, such as the Australian Federal Police, to obtain direct evidence of these offences—such as the content of conversations—rather than simply relying on circumstantial evidence, such as the mere existence of suspicious telephone calls'.*

The Explanatory Memorandum for the Bill states:

> *4.6 - The Bill will amend the TIA Act to include the insider trading offences and those in Part 7.10 of the Corporations Act as serious offences for the purpose of section 5D of the TIA Act. [Schedule 1, Item 21]*
>
> *4.7 - This will enable an interception agency to apply for a telecommunications interception warrant in the course of investigations into these offences, including investigations assisted by ASIC.*

It would appear that initially it was understood by the then Minister that the proposed amendments would enable ASIC to access/receive TI material obtained by an interception agency, albeit that is not reflected in the Exposure Draft released on 20 May 2010, nor in the final drafting of the legislation which did not permit that in relation to an investigation by ASIC. I am unaware of any reason for this apparent change in drafting and policy. Treasury may have more information in that regard.

The inability of ASIC to receive TI material may be contrasted to the position under the *Surveillance Devices Act 2004* (Cth). Pursuant to that Act the AFP and other 'law enforcement agencies' [which

[3] Hansard, House of Representatives, 29 September 2010 pp. 112-113.

definition does not include ASIC], can lawfully listen to and record private conversations. Pursuant to ss.45(5) and (7) of the SD Act 'protected information' can be provided to and used by ASIC for the purpose of its own investigation and/or prosecution of a 'relevant offence', the definition of which includes any Commonwealth offence punishable by a maximum term of imprisonment of 3 years or more.

Obviously the broadening of the ASIC's powers to receive and use TI material for its own investigations [and prosecution by CDPP] raises some sensitive policy issues, bearing in mind the intrusive nature of TI material. Such concerns could be ameliorated by limiting the power to receive and use TI material to Part 7.10 offences, such offences being currently within the definition of 'serious offence' under the TIA.

Provision of compulsory examination material to CDPP

Prior to the recent decision of the NSW Court of Criminal Appeal in *R v OC [2015] NSWCCA 212*, there was doubt on the capacity of ASIC to provide to the CDPP a copy of examination material obtained against a person pursuant to s. 19 of the ASIC Act. The CDPP view is that the ASIC Act evinces a clear legislative intention to enable such provision, and the Court of Criminal Appeal agreed with that view. I note that the respondent to the Director's appeal has now applied for special leave to appeal to the High Court.

Statistics re referrals

You also requested some details of matters referred and prosecuted. Upon receipt of a brief of evidence, the CDPP opens a brief assessment phase on its database, and is able to produce reports from the database according to phase [e.g. brief assessment phase, summary phase, committal phase, trial phase].

In the period 1 January 2010 to 31 August 2015, for those matters in which a brief of evidence was referred by ASIC, and therefore a brief assessment phase opened in the CDPP database:

- A prosecution was commenced in 230 matters
- There was deemed to be insufficient evidence in relation to 94 matters
- Prosecution was considered inappropriate in 46 matters.

Please note that the brief assessment phase does not include those matters commenced via arrest where the CDPP had not previously received a brief of evidence. Those matters are opened in the summary or committal phase. Note though that for most ASIC referrals that are commenced via arrest the CDPP still receives a brief of evidence in advance which the CDPP assesses in accordance with the Prosecution Policy of the Commonwealth, and if satisfied there is a reasonable prospect of conviction and that prosecution is in the public interest, it is then a matter for ASIC whether to commence via arrest or via summons. The vast majority of referrals from ASIC to CDPP would result in a brief assessment phase being opened, including those matters that proceed via arrest. Proceedings commenced via arrest in relation to an ASIC matter, in which the CDPP had not been previously provided with a brief of evidence, are very rare.

If you require any further information please contact me on 03 96054476 or via shane.kirne@cdpp.gov.au. Please note that I will be on leave 21 September to 2 October 2015.

Yours faithfully

Shane Kirne
Deputy Director
Commercial, Financial & Corruption