Australian Government

ASIC Enforcement Review

Positions and Consultation Paper 5
ASIC's Access to Telecommunications Intercept Material
20 July 2017

ISBN 978-1-925504-54-5

Manager
Communications
The Treasury
Langton Crescent
Parkes ACT 2600

Email: **medialiaison@treasury.gov.au**

CONTENTS

1. EXECUTIVE SUMMARY

(i) The *Telecommunications (Interception and Access) Act 1979* (TIA Act) regulates access to telecommunications interception (live stream of the content of communications), telecommunications data (including subscriber details, call time and location details) and stored communications (historical text messages, voicemails and emails).

(ii) The TIA Act prohibits the interception of and unlawful access to communications without the knowledge of the parties to the communication. It then sets out a regime that enables agencies to access various forms of telecommunication information in prescribed circumstances and depending on the agency's status. This regime is summarised in Annexure A.

(iii) Designated 'interception agencies' can seek warrants to intercept telecommunications (TI warrant) for the purpose of investigating specific offences that are defined as a 'serious offence' in the TIA Act. Once a TI warrant has been executed, the TIA Act prohibits the use, communication and giving in evidence of lawfully intercepted information (TI material) subject to a number of exceptions.

(iv) Among other things, interception agencies may communicate TI material to specified agencies (recipient agency) if the material appears to relate to a matter that could be investigated by the recipient agency. The recipient agency may generally use the TI material for investigations and prosecutions of 'relevant offences' within its jurisdiction.

(v) ASIC is a criminal law enforcement agency under the TIA Act and can presently access telecommunications data and apply for warrants authorising access to stored communications in specified circumstances. ASIC is not an interception agency or a recipient agency under the TIA Act.

(vi) At the same time the definition of 'serious offence' in the TIA Act includes offences against provisions of the *Corporations Act 2001* (Corporations Act) including insider trading[1], market manipulation[2] and financial services fraud.[3] ASIC has specific statutory responsibility for conducting investigations and prosecutions of these offences. In addition, the definition of serious offence in the TIA Act includes other fraud offences that are commonly investigated and prosecuted by ASIC, including serious fraud.

(vii) As a result, ASIC as the agency with specific expertise and an express and primary statutory mandate to investigate serious Corporations Act offences cannot obtain or receive TI material to conduct investigations and prosecutions. Where an interception agency uncovers TI material relating to serious Corporations Act offences or other serious corporate crime, the present telecommunications interception regime prevents that agency from sharing the evidence with ASIC, except for the specific purpose of that agency's own investigation. This means that ASIC's ability to usefully conduct cooperative investigations with other interception agencies (such as the Australian Federal Police) in appropriate cases is limited.

(viii) The ASIC Enforcement Review Taskforce has been established by the Government to assess the suitability of the regulatory tools available to ASIC and whether there is a need to

1 Corporations Act, s1043A.

2 Corporations Act, ss1041A — 1041D

3 Corporations Act, ss1041E — 1041G

strengthen ASIC's toolkit.[4] The Taskforce's Terms of Reference include the following:

'The adequacy of ASIC's information gathering powers and whether there is a need to amend legislation to enable ASIC to utilise the fruits of telephone interception warrants … for market misconduct or other serious offences'.

(ix) The Taskforce has conducted preliminary analysis of the issues relating to the TIA Act regime outlined above and has developed the following preliminary position:

Position 1: ASIC should be able to receive TI material to investigate and prosecute serious offences.

(x) The Taskforce considers, on a preliminary basis, that ASIC should be able to receive lawfully intercepted TI material for the purposes of investigating and prosecuting offences, within its jurisdiction, that are defined under the TIA Act as 'serious offences', including the serious Corporations Act offences. The use and disclosure framework in the TIA Act is complex and there may be a number of ways to enable ASIC to receive and use TI material lawfully obtained by other agencies for the purpose of its own investigations and prosecutions of serious offences. The obvious option would be to make ASIC a recipient agency under section 68 of the TIA Act. However, if the Taskforce's policy intent outlined above could be achieved by other means, those could be considered.

(xi) In adopting this position, the Taskforce recognises that the telecommunication intercept powers intrude on the privacy of individuals. Accordingly, any legislative expansion of the powers needs to be proportionate to the seriousness of the misconduct sought to be addressed and ensure that there are adequate safeguards to protect against unjustified intrusion into personal privacy.

(xii) The Taskforce has developed this position on a preliminary basis, and now seeks industry and community feedback prior to reaching its final conclusions and preparing recommendations to Government.

(xiii) The background and reasons for the Taskforce's adoption of the position set out above is described below.

4 For more information about the ASIC Enforcement Review Taskforce see the Taskforce website (http://www.treasury.gov.au/ConsultationsandReviews/Reviews/2016/ASIC-Enforcement-Review).

2. BACKGROUND

2.1 THE TELECOMMUNICATIONS INTERCEPTION AND ACCESS REGIME

1. The *Telecommunications (Interception and Access) Act 1979* (TIA Act) regulates access to:

    1.1. telecommunications interception — live stream of the content of communications carried over a telecommunications service, for example, real-time listening of telephone calls;

    1.2. telecommunications data — including subscriber details and details of telecommunications such as call time and location but not actual content; and

    1.3. stored communications– including historical text messages, voicemails and emails.

2. The TIA Act prohibits the interception of and unlawful access to communications without the knowledge of the parties to the communication.[5] It then sets out a regime that enables agencies to access various forms of telecommunication information in prescribed circumstances and depending on the agency's status as an interception agency, criminal law enforcement agency or enforcement agency. This regime is summarised in Annexure A.

3. The staggered levels of access by agencies and the differing thresholds for access to communications are based on perceptions about the relative privacy-intrusiveness of particular kinds of communications. For example, covert access to text-based communications has been considered less intrusive than real-time listening, because, unlike a telephone call, text-based communications offer an opportunity for 'second thoughts' prior to transmission. Stored communications can be accessed with a warrant by criminal law enforcement agencies, for the investigation of a serious contravention.

4. Designated 'interception agencies' can seek warrants to intercept telecommunications (TI warrant) for the purpose of investigating serious offences defined in section 5D of the TIA Act. Interception agencies include the Australian Federal Police (AFP), Australian Commission for Law Enforcement Integrity (ACLEI) and Australian Crime Commission, now called the Australian Criminal Intelligence Commission (ACIC).[6] These are all agencies whose exclusive area of operation is law enforcement.[7] ASIC is not an interception agency for the purposes of the TIA Act.

---

5 See TIA Act ss. 7 and 108. In relation to telecommunication data see ss 276, 277 and 278 of the *Telecommunication Act 1997* and ss. 178, 178A, 179 and 180 of the TIA Act.

6 An eligible authority of a State may be declared an interception agency in certain circumstances (see section 5, 34 and 35 of the TIA Act).

7 In 2007, the Parliamentary Joint Committee on the Australian Crime Commission, in an inquiry into the future impact of serious and organised crime on Australian society, considered telecommunications interception to be an 'invasive power' and recommended that the 'potential gravity of the exercise of such powers should be properly restricted to those agencies whose exclusive area of operation is law enforcement.'

5. Interception agencies are subject to more comprehensive oversight and accountability frameworks than criminal law enforcement and enforcement agencies and must:

   5.1. provide regular reports on the effectiveness of their interception warrants;

   5.2. tender warrants to the Attorney-General to enable ministerial oversight through a 'warrant register';

   5.3. maintain detailed records of any conduct under a warrant to facilitate biannual inspections by the Commonwealth Ombudsman; and

   5.4. include comprehensive information of their interception activities in annual reports.

6. The TIA Act permits interception agencies to apply to an eligible Judge or nominated member of the Administrative Appeals Tribunal for a TI warrant.[8] A TI warrant will only be granted where the applicant can demonstrate that it would be likely to assist in connection with the investigation of a 'serious offence', and satisfy other statutory criteria, including having regard to 'how much the privacy of any person or persons would be likely to be interfered with by intercepting' the relevant telecommunications.[9]

7. Once an interception warrant has been executed, the information an interception agency receives is subject to strict controls. Section 63 of the TIA Act prohibits the use, communication and giving in evidence of lawfully intercepted information obtained under a warrant (TI material). Sections 67, 68 and 74 of the TIA Act provide exceptions to these prohibitions.

8. Interception agencies can generally use material obtained pursuant to TI warrants for the purpose of investigating a 'prescribed offence', which includes (among other things) a 'serious offence' or other offences punishable by imprisonment for a period of at least three years.[10] The TI material is generally admissible in prosecutions for such offences.[11]

9. Interception agencies may also communicate lawfully obtained TI material to an agency specified in section 68 of the TIA Act (recipient agency) if the material appears to (among other things) relate to a matter that could be investigated by the recipient agency. In this case the recipient agency may generally use the TI material for (among other things) investigations and prosecutions for 'relevant offences' within its jurisdiction.

8 TIA Act, s5 and s39. As stated above the current Commonwealth interception agencies are: the Australian Federal Police, the Australian Commission for Law Enforcement Integrity and the Australian Criminal Intelligence Commission: s5.

9 TIA Act, s46.

10 TIA Act, s67, s5 (definitions of 'permitted purpose', 'prescribed offence' and 'relevant offence') and s6L.

11 TIA Act, s74, s75A, s5B and s5 (definitions of 'prescribed offence').

2.2 SERIOUS MARKET AND FINANCIAL SERVICES OFFENCES IN THE TIA ACT

10. A 'serious offence' is defined in s5D of the TIA Act. This definition expressly includes offences against the following provisions of the *Corporations Act 2001* (Corporations Act):[12]

    10.1. insider trading (s1043A of the Corporations Act);

    10.2. market manipulation (ss1041A—1041D of the Corporations Act); and

    10.3. financial services fraud (s1041E—s1041G of the Corporations Act).

    (serious CA offences)

11. Each of the serious CA offences are punishable:

    11.1. in the case of an individual, by imprisonment for up to 10 years and/or a maximum fine of the greater of 4,500 penalty units (currently $945,000)[13] or three times the value of the benefit that was obtained by reason of the offence;[14] and

    11.2. in the case of a body corporate, by a maximum fine of the greatest of 45,000 penalty units (currently $9.45 million), three times the value of the benefit that was obtained by reason of the offence or 10 per cent of the body corporate's annual turnover at the time of the offence.[15]

12. ASIC is, among its other functions, a criminal law enforcement agency with primary statutory responsibility for the investigation and prosecution of serious offences prescribed in the Corporations Act,[16] including the serious CA offences.[17]

13. In addition to investigating and prosecuting serious CA offences, ASIC's enforcement functions include investigating and prosecuting other criminal offences (Commonwealth, State or Territory) where the conduct involves corporations, managed investment schemes or certain types of financial fraud.[18] The definition of serious offence in s5D of the TIA Act extends to (among other things) other fraud offences that are commonly investigated and prosecuted by ASIC, including serious fraud.[19]

---

12 TIA Act, s5D(5C).

13 As at 1 July 2017 a penalty unit is $210, *Crimes Amendment (Penalty Unit) Act 2017.*

14 Corporations Act, s1311 and Sch 3, item 310.

15 Corporations Act, s1311 and Sch 3, item 310.

16 *Australian Securities and Investments Commission Act 2001* (**ASIC Act**), s1(2)(g), s13 and s49(2). ASIC (and its immediate predecessor, the Australian Securities Commission) has been exercising important criminal law enforcement functions since 1991 and before this there was a very long tradition, spanning 150 years, of comparable specialist authorities undertaking criminal investigations and prosecutions in relation to corporate crime in Australia: see, for example, sections LVII to LX of the *Companies Statute* 1864 (Vic).

17 All of these offences are contained in Part 7.10 of the Corporations Act, which is headed 'Markets Misconduct and Other Prohibited Conduct relating to Financial Products and Financial Services'.

18 ASIC Act, s13(1)(b).

19 TIA Act, s5D(2)(a) and (b)(v).

2.3 SURVEILLANCE MATERIAL

14. Under the *Surveillance Devices Act 2004* (Cth) (SD Act) certain Commonwealth law enforcement agencies can apply for a surveillance devices warrant to use listening devices (and other types of surveillance devices) to lawfully listen to and record private conversations, for example by planting listening/recording devices in a particular room or car to capture conversations that take place at that specific location. The only Commonwealth law enforcement officers who may apply for warrants under the SD Act are officers of the AFP, the ACIC and the ACLEI.

15. The SD Act is limited in its scope to regulating the use of listening devices (and other types of surveillance devices) by the restricted Commonwealth law enforcement agencies mentioned above, or State/Territory police forces, investigating Commonwealth offences (or State/Territory offences with a federal aspect).

16. Accordingly, officers of other Commonwealth agencies who also investigate criminal offences, such as ASIC, the Australian Customs and Border Protection Service and the Department of Human Services (Centrelink), are not subject to the provisions of the SD Act. The use of listening devices by these officers will be governed by relevant State and Territory laws.

17. However, the SD Act permits information obtained pursuant to a surveillance devices warrant to be used, recorded, communicated and published to another agency if it is necessary to do so for purposes including the investigation of an offence (Commonwealth or State offences with a federal aspect) that is punishable by a maximum term of imprisonment of 3 years or more.[20] The relevant investigation can be one that is being conducted by the other agency.

2.4. ASIC'S CURRENT ACCESS TO TI AND SURVEILLANCE MATERIAL

18. As a criminal law enforcement agency under the TIA Act ASIC can presently access telecommunications data if its disclosure is reasonably necessary for enforcement of the criminal law, enforcement of a law imposing a pecuniary penalty or protection of the public revenue[21] and apply for warrants authorising access to stored communications for the purpose of investigating a serious contravention or other offences.[22]

19. Any subsequent use of telecommunications data or stored communications obtained by ASIC is strictly restricted by the legislative and procedural safeguards, in addition to oversight regimes.[23]

20. ASIC is currently neither an interception agency nor a recipient agency under the TIA Act.[24] Accordingly, ASIC can neither apply for TI warrants for the purpose of investigating offences

20 s45(5) of the SD Act.

21 TIA Act, s178 and s179.

22 TIA Act, s5E and s116.

23 TIA Act, Part 3-4, Part 3-5 and Part 3-6 with respect to stored communications and Part 4-1 Division 5 and Division 6 and Part 4-2 with respect to telecommunications data.

24 TIA Act, s5 and s68.

within its statutory responsibility nor receive TI material lawfully obtained by other agencies for the purpose of investigating such offences or other 'relevant offences'.

21. However, material captured pursuant to a surveillance devices warrant under the SD Act (for example private conversations recorded through a device planted in a particular room or car) can be shared with ASIC for use in investigations and prosecutions, including serious CA offences.[25]

22. There are difficulties and limitations associated with the use of listening devices, including that they can be more difficult and dangerous to use, and more intrusive and indiscriminate in their operation, than telecommunications interceptions[26] and are also generally less effective[27]. The current position is therefore somewhat of a paradox: ASIC can access information that is obtained with greater invasion of privacy and less discrimination, but cannot access intercepted information.

25 SD Act, s45(5) and s45(7).

26 For example, law enforcement officers have to covertly enter a suspect's house or car to plant a listening device and it will then indiscriminately record all conversations by any persons, not merely those involving the suspect, in the particular house or car.

27 For example, listening devices will only capture conversations at the specific location where the device is situated — if the suspect uses his or her phone at a different location the telephone conversation will not be captured at all and even if the suspect uses his or her phone at the relevant location only one side of the conversation is likely to be captured.

3. INVESTIGATING AND PROSECUTING THE SERIOUS CA OFFENCES

3.1 THE CORPORATIONS AMENDMENT (NO. 1) ACT 2010

23. The *Corporations Amendment (No. 1) Act 2010* introduced the serious CA offences to the definition of 'serious offence' in section 5D of the TIA Act. The serious CA offences, and in particular the markets offences, were considered appropriate for interception because they are:

> '… difficult to investigate … as [they] 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.'[28]

24. The media release announcing the proposed amendment in 2010 stated:

> …
>
> 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 …
>
> The *Telecommunications (Interception and Access) Act 1979* (the TIA Act) currently limits the offences for which interception can be used as an investigative tool. Interception may only be conducted under a warrant obtained by an interception agency in relation to the investigation of a serious offence.
>
> It is proposed that the law will be amended so that a serious offence for these purposes includes market and insider trading offences investigated by ASIC.
>
> A telecommunications interception agency, such as the AFP, would execute the warrant, then ASIC and the agency would work together on the investigation.
>
> This will enable ASIC to obtain direct evidence of inside information, such as the content of conversations, rather than simply relying on circumstantial evidence, such as the mere existence of suspect telephone calls.'[29]

25. It appears that the objective of the 2010 amendments was to enable an interception agency, like the AFP, to apply for a warrant to intercept communications in the investigation of these offences. Interception agencies would then be able to pass lawfully intercepted information to ASIC for the purpose of furthering an investigation to which ASIC was a party. This is confirmed by the Explanatory Memorandum which states:

---

28 Replacement Explanatory Memorandum, *Corporations Amendment (No. 1) Bill 2010,* p. 21

29 Minister for Financial Services, Superannuation and Corporate Law, Media Release, 28 January 2010 (emphasis added), available at: http://ministers.treasury.gov.au/listdocs.aspx?doctype=0&PageID=003&min=ceba.

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.[30]

3.2 MULTIPLE AGENCY INVESTIGATIONS — PRACTICAL AND LEGAL ISSUES

26. ASIC's role in any investigation involving TI material is necessarily limited as:

    26.1. ASIC is not a recipient agency able to receive or use TI material for the purpose of its own investigation; and

    26.2. the provisions in the TIA Act relating to the use and disclosure of TI material, in effect, only permit that material to be shared with specific ASIC officers who are assisting the interception agency in an investigation that is being carried out by that agency.

27. An interception agency can only seek and obtain a TI warrant for the purpose of its own investigation[31] and officers of an interception agency can only lawfully use and communicate TI material for the purpose of their own agency's investigation.[32] An ASIC officer who receives TI material can only use that material in order to assist the interception agency in the investigation being carried out by that agency. The ASIC officer cannot use the TI material to assist any separate or related investigation being conducted by ASIC.

28. As a result of these issues, in practice ASIC officers are seconded to the relevant interception agency to assist in the conduct of an investigation by that agency. This can create management and administrative difficulties and result in inefficiencies and delays, which can in turn prejudice the investigation.

29. At the same time, complexities can be created for the Commonwealth Director of Public Prosecutions (CDPP) where a course of conduct leads to multiple investigations and potential prosecutions by different agencies, which may include ASIC and an interception agency relying on TI material. Employees of the CDPP may be privy to TI material but must not disclose that material or information derived from that material to ASIC when communicating with ASIC regarding the matter it is pursuing.

---

30 Corporations Amendment (No.1) Bill 2010 Explanatory Memorandum p21.

31 TIA Act, ss46(1)(d) and 46A(1)(d).

32 TIA Act ss 63, 67, 73 and 105.

3.3 THE RESPONSIBLE AGENCY CANNOT RECEIVE RELEVANT EVIDENCE

30. Parliament has recognised that TI warrants ought to be available for the investigation of the serious CA offences and other serious offences commonly investigated by ASIC (for example, serious fraud), and that lawfully obtained TI material ought to be available for investigating and prosecuting 'serious offences' and other 'relevant offences'.

31. Investigations and prosecutions of these offences are notoriously difficult, resource-intensive and time-consuming.[33] For the purpose of carrying out these investigations and prosecutions, ASIC (among other things):

    31.1. has unique powers for gathering information and evidence and obtaining assistance that are not available to any other agency (and can only be exercised for the purpose of an investigation by ASIC rather than another agency);[34]

    31.2. has specialised staff, resources and experience not possessed by any other agency; and

    31.3. is the only agency in Australia able to directly obtain information and assistance from other international securities commissions throughout the world.[35]

32. As an interception agency, the AFP can seek TI warrants and obtain and use TI material for the purpose of investigating serious offences. While it is open to the AFP to investigate Corporations Act offences, it rarely does so due to competing law enforcement priorities and ASIC's express jurisdiction in this area. Further, the AFP cannot commence a prosecution for Corporations Act offences without specific Ministerial approval.[36] In contrast, ASIC is the only agency with specific statutory responsibility for investigating and prosecuting Corporations Act offences, including the serious CA offences, and the only agency with a statutory entitlement to initiate prosecutions for such offences.[37]

33. As a result, ASIC as the agency with specific expertise and an express and primary statutory mandate to investigate the serious CA offences cannot obtain and receive TI material. In addition, where the AFP (or any other interception agency) uncovers TI material relating to serious CA offences or other serious corporate crime, the present telecommunications interception regime prevents that agency from sharing the evidence with ASIC.

---

33 This has been widely recognised by courts: see, eg, *R v Curtis (No 3)* [2016] NSWSC 866 at [52]; *Kamay v R* [2015] VSCA 296 at [51]; *CDPP v Hill* [2015] VSC 86 at [48] & [92]; *Khoo v R* [2013] NSWCCA 323 at [22] & [97]-[100]; *Hartman v R* (2011) 87 ACSR 52 at [96]; *R v Glynatsis* [2013] NSWCCA 131 at [39]; *R v O'Brien* [2011] NSWSC 1553 at [36] & [45]; *R v Bateson* [2011] NSWSC 643 at [31]; *R v Rivkin* (2003) 198 ALR 400 at [44]; *R v Hannes* [2002] NSWSC 1182 at [90]; *R v Hannes* [2000] NSWCCA 503 at [394].

34 Including powers to: conduct compulsory examinations of witnesses and suspects (s19 of the ASIC Act); compel the production of documents and records (s28—s34 of the ASIC Act); and compel persons to provide 'reasonable assistance' in relation to investigations and prosecutions (s19 and s49 of the ASIC Act).

35 Through being a signatory to the International Organization of Securities Commissions ('IOSCO') *Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information*.

36 Corporations Act, s1315(1)(c).

37 Corporations Act, s1315(1), and ASIC Act, s49(2).

34. ASIC understands that from time to time interception agencies conducting their own investigations have lawfully obtained TI material relating to suspected serious CA offences and may have wished to provide that evidence to ASIC but have been unable to do so. The prohibitions in the TIA Act on divulging TI material mean that it is not possible to determine how often this may occur.[38] ASIC believes that in at least some cases the relevant agency has declined to investigate those offences themselves because of jurisdictional limitations and/or competing priorities.

35. At least five other relevant matters have come to public attention. In each case:

    35.1. the suspected offences included insider trading;

    35.2. the interception agency ultimately investigated and (with Ministerial approval) prosecuted the suspected offences due to the inability of ASIC to receive or use the interception information for the purpose of an ASIC investigation;

    35.3. ASIC provided assistance to the interception agency, but ASIC's ability to assist was severely limited because it could not receive or use TI evidence to conduct its own investigation or exercise its own unique powers;

    35.4. the interception agency's investigation and prosecution was drawn out, spanning ten years on average; and

    35.5. the accused was acquitted.[39]

3.4 TI MATERIAL PROVIDES IMPORTANT EVIDENCE

36. ASIC considers that there have been matters where ASIC has identified suspected serious CA offences committed through the use of telecommunications, but has been unable to gather sufficient evidence to prosecute. The following case study provides an example where access to TI warrants and/or TI material would have significantly assisted the investigation.

38 See TIA Act, s46(1)(d), s46A(1)(d), s63, s67, s73 and s105.

39 See, eg, 'Insider trading allegations plague the nephew of Governor Ken Michael', The Australian, 13 January 2009: http://www.theaustralian.com.au/news/nation/governors-nephew-charged/story-e6frg6pf-1111118546512; 'West Australian insider trading case dropped after 10 years', The Australian, 26 August 2011: http://www.theaustralian.com.au/business/legal-affairs/west-australian-insider-trading-case-dropped-after-10-years/story-e6frg97x-1226122421169; 'Skimpies king cleared of insider trading', The West Australian, 1 April 2010: http://au.news.yahoo.com/thewest/a/-/wa/7010232/skimpies-king-cleared-of-insider-trading/; *R v Mansfield & Kizon* [2011] WASCA 132; *Kizon & Mansfield v R* [2011] HCATrans 331. The acquittal of Messrs Kizon and Mansfield was set aside and a new trial was ordered, but it too resulted in acquittals: 'John Kizon and associate Nigel Mansfield found not guilty of insider trading' (13 March 2014): http://www.perthnow.com.au/news/western-australia/john-kizon-and-associate-nigel-mansfield-found-not-guilty-of-insider-trading/story-fnhocxo3-1226854137192; 'Insider Trading charges against former Premier Brian Burke dropped' (18 February 2014): http://www.abc.net.au/news/2014-02-18/burke-charges-dropped/5267090.

Case study 1: Insider trading investigation

In 2009 ASIC investigated the largest suspected insider trading ring detected in Australia to date. The suspects were well-connected businesspeople who appeared to be trading on information obtained from corporate advisors about pending takeovers. ASIC estimates that the traders made profits in excess of $40 million over a period of two years. During the investigation, it was identified that the traders acquired large positions in a listed entity, worth over $60 million, as a likely result of access to inside information. The traders then sold these positions after a proposed takeover of the entity was announced. Despite using its search warrant and compulsory examination powers, ASIC was unable to obtain sufficient evidence to prosecute.

37. The CDPP supports ASIC's view that TI material can be significant in the prosecution of the serious CA offences and can determine whether or not there is sufficient evidence to prosecute. Often this conduct is sophisticated and covert. As a result capturing conversations of the suspected offenders at the time of or proximate to the offending can provide crucial evidence that may not come to light through investigations focused on gathering documentary evidence after the conduct has occurred.

Case study 2: Insider trading investigation

ASIC investigated suspected insider trading in a target company in advance of a takeover announcement by a group of individuals, one of whom had links to the bidding company. ASIC identified the suspicious trades on the day of the takeover announcement as the trading by the group represented a significant part of the trading volume in the target company leading up to the takeover announcement and the individuals had only previously engaged in small-value share trades. Telecommunication records showed a significant number of calls between members of the group both prior to and subsequent to the takeover announcement. While text communications obtained during the execution of search warrants were to a degree circumstantially incriminating, there was no direct evidence to prove the suspected insiders possessed the relevant information before the takeover announcement. Interception of telecommunications between members of the group may have provided direct or further circumstantial evidence of possession of inside information by individuals within the group.

38. A number of international jurisdictions also recognise the importance of TI material for the investigation of offences equivalent to the serious CA offences in their jurisdictions. The US Department of Justice (**DOJ**) has similar criminal investigation and prosecution functions to ASIC, including relating to insider trading and market manipulation.[40] The DOJ can obtain and use TI material (referred to as 'wiretap' evidence) and has successfully prosecuted insider trading and market manipulation matters using this type evidence, including securing high profile convictions against Raj Rajaratnam, founder of one of the biggest hedge funds in the world, and Rajat Gupta, former Chief Executive of McKinsey & Co.[41]

40 The Securities and Exchange Commission (**SEC**), which is similar to ASIC in some other respects, differs from ASIC because it does not conduct criminal investigations and prosecutions.

41 See, for example, http://www.scribd.com/collections/2980389/The-Galleon-Trial-Transcripts-of-Wiretapped-Calls; http://online.wsj.com/article/SB10001424052748704590704576091851297336450.html.

39. In 2015 Preet Bharara, US Attorney for the Southern District of New York, stated:

> ' … because illegal insider trading appears so prevalent and because it is so difficult to prove — we remain committed to using every lawful investigative tool available to investigate and prosecute insider trading offenses, including court-authorized wiretaps, which have provided valuable evidence in insider trading cases where communication is an essential element of the crime.'[42]

40. The legislative regime for the interception of telecommunications in the United Kingdom (**UK**) differs from that in Australia in a number of respects, including the following:

    40.1. TI warrants are issued by the Secretary of State;[43]

    40.2. TI warrants are available for the relatively broad purpose (among others) of 'preventing or detecting serious crime'[44] (rather than investigations by specified interception agencies of specified 'serious offences');

    40.3. while there are restrictions on the purpose for which TI material can be used and communicated (for example, for the purpose of investigating a relevant offence), there is no additional limitation on which particular agencies are able to receive and use TI material;[45] and

    40.4. TI material is generally not admissible in any legal proceedings,[46] (whereas in Australia it is generally admissible in prosecutions for relevant offences).

41. The two agencies in the UK with primary responsibility for investigating and/or prosecuting the UK equivalents of the serious CA offences are the Financial Conduct Authority (**FCA**), which specialises in financial and securities enforcement, and the Serious Fraud Office (**SFO**), which is responsible for investigating and prosecuting serious or complex fraud offences.[47]

42. While neither of these agencies is able to apply for a TI warrant,[48] they can request other agencies (for example, the Metropolitan Police or Serious Organised Crime Agency) to seek TI warrants for the purpose of their investigations into 'serious crime' and they can lawfully receive and use TI material obtained by those other agencies for the purpose of their own investigations into 'serious crime' (although in the UK TI evidence is generally not admissible in any legal proceedings).[49]

---

42 https://www.justice.gov/usao/priority-areas/financial-fraud/securities-fraud

43 *Regulation of Investigatory Powers Act 2000* (UK), s.5(1).

44 *Regulation of Investigatory Powers Act 2000* (UK), s.5(3)(b). The term 'serious crime' is defined in s.81(2) & (3) as conduct involving one or more offences that: (a) could reasonably be expected to attract a sentence of imprisonment for three years or more; and (b) involves the use of violence, results in substantial financial gain or was committed by a large number of persons in pursuit of a common gain.

45 *Regulation of Investigatory Powers Act 2000,* s 15.

46 *Regulation of Investigatory Powers Act 2000*, s17—18.

47 *Criminal Justice Act 1987* (UK), s 1.

48 *Regulation of Investigatory Powers Act 2000* (UK), s 6.

49 Regulation of Investigatory Powers Act 2000, s17—18.

43. In recent times, ASIC has observed rapid changes in the methods in which individuals that are the subject of investigations are communicating. Communications which were previously being conducted through emails, SMS messages and over phone lines are now being conducted over internet-based messaging and communication platforms such as Snapchat, WeChat and WhatsApp. Such platforms provide the ability for individuals to communicate through text-based messaging and also through voice/video communications using Voice Over Internet Protocol (VOIP). In the case of text-based communications over such platforms, the platform application may store for a period a copy of the message on the device used to communicate, depending on how the application preferences are set. In relation to VOIP communications, the platform application may, similar to text-based communications, store a copy of the message or simply store a log of VOIP calls for a period. Such communications however are not apparent from telecommunications carrier records.

44. The issues arising from ASIC's inability to obtain or access intercepts of voice communications will carry through and be compounded as communication through internet-based messaging and communication platforms becomes increasingly common. Interception powers under the TIA Act in its existing form would allow access to VOIP calls and potentially other internet-based forms of communication. Further, as the TIA Act evolves over time in response to new forms of communication, ASIC would have the ability to access those new forms of evidence.

45. At the same time communication through these alternative platforms is frequently encrypted or conducted through a secure network. This makes interception difficult and leads to an increase in the volume of data to analyse reducing the utility and benefit from those interceptions. In addition, providers of internet based communications are often based overseas, which creates jurisdictional complications associated with enforcing obligations imposed by the TIA Act.

Position 1: ASIC should be able to receive TI material to investigate and prosecute serious offences

46. The Taskforce adopts as a preliminary position that ASIC should be able to receive lawfully intercepted TI material for the purposes of investigating and prosecuting offences, within its jurisdiction, that are defined under the TIA Act as 'serious offences', including the serious CA offences. The use and disclosure framework in the TIA Act is complex and there may be a number of ways to enable ASIC to receive and use TI material lawfully obtained by other agencies for the purpose of its own investigations and prosecutions of serious offences. The obvious option would be to make ASIC a recipient agency under section 68 of the TIA Act. However, if the Taskforce's policy intent as outlined above could be achieved by other means, those could be considered.

47. The Taskforce considers that this reform would:

    47.1. reflect ASIC's current status as a criminal law enforcement agency that has primary responsibility for investigating criminal offences that are already expressly defined as 'serious offences' in the TIA Act and are difficult to prove;

    47.2. enhance ASIC's ability to successfully investigate and prosecute serious offences and thereby achieve its legislative objectives;

    47.3. allow ASIC and other agencies, in particular the AFP, to conduct effective cooperative or parallel investigations and share evidence relating to serious criminal wrongdoing with aspects within each agency's principle remit (for example, foreign bribery); and

    47.4. avoid the circumstance in which an interception agency is in possession of evidence of serious corporate offences but is unable to share that information with the corporate regulator.

48. In adopting this position the Taskforce recognises that the telecommunication intercept powers intrude on the privacy of individuals. Accordingly, any legislative expansion of the powers needs to be proportionate to the seriousness of the misconduct sought to be addressed and ensure that there are adequate safeguards to protect against unjustified intrusion into personal privacy.

49. While this proposal involves a degree of expansion to the scope of telecommunication intercept powers, the Taskforce considers that it would be appropriate to address the issues identified in this paper. The proposal would not expand the range of offences for which TI warrants could be sought under the TIA Act, the range of evidence that could be obtained pursuant to a TI warrant or broaden the admissibility of TI material. It will only permit ASIC to receive and use information that has already been lawfully intercepted by other interception agencies where that information is or may be relevant to a serious offence that ASIC may investigate, which offences are already recognised by Parliament to be sufficiently seriousness to warrant the invocation of telecommunication intercept powers. In addition, there would be no dilution to the existing safeguards contained in the TIA Act. When in receipt of TI material ASIC would be subject to the strict limitations, restrictions, reporting and record-keeping requirements that currently apply.

50. Another, more expansive option would be to include ASIC within the definition of 'interception agency' in the TIA Act so that it can seek a TI warrant from an eligible Judge or AAT Member for the purpose of investigating serious CA offences, and other 'serious offences' within its investigative jurisdiction, and then obtain and use TI evidence for the purpose of its own relevant investigations and prosecutions. This would also allow ASIC to receive TI

evidence obtained by other interception agencies where it relates to Corporations Act offences.[50]

51. While this could significantly enhance ASIC's ability to investigate and prosecute the serious CA offences and may be consistent with ASIC's existing ability to seek other types of warrants from judicial officers, such as search warrants and warrants to access stored communications it would involve a significant departure from the existing regime that restricts the exercise of telecommunications intercept powers to agencies whose exclusive area of operation is law enforcement.

52. This will likely increase the number of telecommunication interceptions that are obtained and consequently the amount of data that is captured through this invasive power, particularly given the increased reliance on internet based platforms discussed above. This would have a corresponding impact on the privacy of individuals who may not only be suspected of serious crimes, but those with whom suspected individuals communicate, who may not be subject of an investigation.

53. ASIC would also need to develop a new capability which will involve capital costs and be resource intensive. ASIC would need to establish the necessary infrastructure and specialist skills to maintain an interception system and meet more comprehensive oversight and accountability frameworks. Alternatively, it could request (possibly on a user pays basis) other interception agencies to execute TI warrants on its behalf but this will still have resource implications for ASIC and the other agency.

54. For the reasons stated above, the Taskforce does not consider that ASIC should be made an interception agency.

Questions

1. Should ASIC be a recipient agency so that it can receive telecommunications intercept material lawfully obtained by interception agencies and use that material for the purpose of investigating serious Corporations Act offences and other 'serious' or 'relevant' offences?

2. If ASIC is made a recipient agency, are any additional reforms appropriate to address any negative consequences of this change?

50 See TIA Act, s68(b)(ii).

ANNEXURE A

SUMMARY OF THE REGIME FOR ACCESS TO COMMUNICATIONS IN THE TIA ACT

Material	Description	Purpose for access	How obtained	Agencies
Telecommunications interception	Live stream of the content of communications carried over a telecommunications service, e.g. real-time listening of telephone calls.	Investigating a serious offence, as defined in section 5D of the TIA Act	Warrant[51]	• Interception agencies Includes: • Australian Federal Police • Australian Commission for Law Enforcement Integrity • Australian Crime Commission, now the Australian Criminal Intelligence Commission • An 'eligible authority of a State' in respect of which a declaration under s34 is in force.[52]
Stored communications	Content of historical communications, e.g. text-based communications like SMS or email	Investigating a serious contravention as defined in s5E of the TIA Act. Including offences with at least a maximum penalty of three years in prison or maximum pecuniary penalty of at least 180 penalty units for individuals or otherwise 900 penalty units.	Warrant[53]	• **Interception agencies** • **Criminal law-enforcement agencies** Includes, among others, the: • AFP • Police Force of a State • ACLEI • ACIC • ASIC • ACCC.[54]
Telecommunications data	The 'metadata' of communications, e.g. the subscriber information or duration of a phone call.	Enforcement of the criminal law, pecuniary penalties and the protection of public revenue.	Accessed under authorisation by an authorised officer of an enforcement agency[55]	• **Interception agencies** • **Criminal law-enforcement agencies** • **Enforcement agencies**[56]

51 Part 2-5 of the TIA Act.
52 Section 5(1) of the TIA Act.
53 Part 3-3 of the TIA Act.
54 Sections 5(1) and 110A of the TIA Act.
55 Sections 178, 178A and 179 of the TIA Act..
56 Defined in section 176A of the TIA Act.

ANNEXURE B

ASIC ENFORCEMENT REVIEW TASKFORCE TERMS OF REFERENCE

The Taskforce will review the enforcement regime of the Australian Securities and Investments Commission (ASIC), to assess the suitability of the existing regulatory tools available to it to perform its functions adequately.

- The review will include an examination of legislation dealing with corporations, financial services, credit and insurance as to:

- The adequacy of civil and criminal penalties for serious contraventions relating to the financial system (including corporate fraud);

- The need for alternative enforcement mechanisms, including the use of infringement notices in relation to less serious contraventions, and the possibility of utilising peer disciplinary review panels (akin to the existing Markets Disciplinary Panel) in relation to financial services and credit businesses generally;

- The adequacy of existing penalties for serious contraventions, including disgorgement of profits;

- The adequacy of enforcement related financial services and credit licensing powers;

- The adequacy of ASIC's power to ban offenders from occupying company offices following the commission of, or involvement in, serious contraventions where appropriate;

- The adequacy of ASIC's information gathering powers and whether there is a need to amend legislation to enable ASIC to utilise the fruits of telephone interception warrants or to grant the equivalent of Federal Crimes Act search warrant powers under ASIC's enabling legislation for market misconduct or other serious offences;

- The adequacy of ASIC's powers in respect of licensing of financial services and credit providers, including the threshold for granting or refusing to grant a licence, the circumstances in which ASIC may vary, suspend, or cancel licenses; and its coercive powers (including whether there is a need for ASIC to have a power to direct licensees to take, or refrain from taking, particular action);

1. The adequacy of the frameworks for notifying ASIC of breaches of law, including the triggers for the obligation to notify; the time in which notification is required to be made; and whether the obligation to notify breaches should be expanded to a general obligation (currently confined under the Corporations Act to auditors, liquidators, and licensees, and noting that obligations to report offences exist under other Federal or State statutes); and

2. Any other matters, which arise during the course of the Taskforce's review of the above, which appear necessary to address any deficiencies in ASIC's regulatory toolset.

Upon completion of the Review, the Taskforce will identify any gaps in ASIC's powers and make recommendations to the Government which it considers necessary to strengthen any of ASIC's regulatory tools and as to the policy options available that:

3. address gaps or deficiencies identified in a way that allows more effective enforcement of the regulatory regime;

4. foster consumer confidence in the financial system and enhance ASIC's ability to prevent harm effectively;

5. do not impose undue regulatory burden on business, and promote engagement and cooperation between ASIC and its regulated population;

6. promote a competitive and stable financial system that contributes to Australia's productivity growth; and

7. relate to other matters that fall within this Terms of Reference.

Further information on the ASIC Enforcement Review taskforce is available at our website:

http://www.treasury.gov.au/ConsultationsandReviews/Reviews/2016/ASIC-Enforcement-Review.