Law Council
OF AUSTRALIA

ASIC's Access to Telecommunications Intercept Material

ASIC Enforcement Review Taskforce

23 August 2017

Telephone +61 2 6246 3788 • *Fax* +61 2 6248 0639
Email mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

Table of Contents

About the Law Council of Australia 3
Acknowledgement 4
Executive Summary 5
Departure from intent of legislation 6
The need for a review of telecommunications intercept information sharing provisions 7
A principled framework for determining access 9
Guidance for agencies 10
Other options 10

About the Law Council of Australia

The Law Council of Australia exists to represent the legal profession at the national level, to speak on behalf of its Constituent Bodies on national issues, and to promote the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world.

The Law Council was established in 1933, and represents 16 Australian State and Territory law societies and bar associations and the Law Firms Australia, which are known collectively as the Council's Constituent Bodies. The Law Council's Constituent Bodies are:

- Australian Capital Territory Bar Association
- Australian Capital Territory Law Society
- Bar Association of Queensland Inc
- Law Institute of Victoria
- Law Society of New South Wales
- Law Society of South Australia
- Law Society of Tasmania
- Law Society Northern Territory
- Law Society of Western Australia
- New South Wales Bar Association
- Northern Territory Bar Association
- Queensland Law Society
- South Australian Bar Association
- Tasmanian Bar
- Law Firms Australia
- The Victorian Bar Inc
- Western Australian Bar Association

Through this representation, the Law Council effectively acts on behalf of more than 60,000 lawyers across Australia.

The Law Council is governed by a board of 23 Directors – one from each of the constituent bodies and six elected Executive members. The Directors meet quarterly to set objectives, policy and priorities for the Law Council. Between the meetings of Directors, policies and governance responsibility for the Law Council is exercised by the elected Executive members, led by the President who normally serves a 12 month term. The Council's six Executive members are nominated and elected by the board of Directors.

Members of the 2017 Executive as at 1 January 2017 are:

- Ms Fiona McLeod SC, President
- Mr Morry Bailes, President-Elect
- Mr Arthur Moses SC, Treasurer
- Ms Pauline Wright, Executive Member
- Mr Konrad de Kerloy, Executive Member
- Mr Geoff Bowyer, Executive Member

The Secretariat serves the Law Council nationally and is based in Canberra.

Acknowledgement

The Law Council is grateful for the assistance of its National Criminal Law Committee and the Law Society of New South Wales in the preparation of this submission.

Executive Summary

1. The Law Council is grateful for the opportunity to provide a submission to the Australian Securities and Investment Commission (**ASIC**) Enforcement Review Taskforce (**the Taskforce**) Positions and Consultation Paper 5, *ASIC's Access to Telecommunications Intercept (**TI**) Material* (**the Consultation Paper**).

2. The Consultation Paper outlines reforms aimed at enhancing ASIC's access to TI material for the investigation and prosecution of serious offences and thereby assisting ASIC in achieving its legislative objectives.[1] ASIC currently has access to telecommunications data and stored communications under the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**).[2] The principal question raised by Consultation Paper is whether ASIC should be a 'recipient agency' which can receive TI material lawfully obtained by interception agencies and use that material for the purpose of investigating serious *Corporations Act 2001* (Cth) (**the Corporations Act**) offences and other 'serious' or 'relevant' offences.

3. The term 'recipient agency' is not currently used in the TIA Act, although the Law Council understands that it is intended to encompass agencies in section 68 of the TIA Act. Section 68 generally enables the chief officer of an interception agency to communicate to prescribed agencies lawfully intercepted information that was originally obtained by the originating agency or interception warrant information if the information relates, or appears to, relate to a matter that may give rise to an investigation by the prescribed agency. Currently, 'recipient agencies' include for example agencies such as core law enforcement and anti-corruption bodies or foreign countrijes with the consent of the Attorney-General.

4. Effective co-operation and appropriately defined information sharing between agencies is critical given the national and global nature of many serious and organised crime and national security investigations. However, information sharing in combating crime and security risks must always be balanced with protecting the right to privacy.

5. Telecommunication interception powers necessarily intrude on the privacy of individuals. Any legislative expansion of the powers needs to be demonstrated to be necessary and proportionate to the seriousness of the misconduct sought to be addressed.

6. The Law Council's primary recommendation is that there be an independent review, or as a minimum, a review by the Attorney-General's Department (**the Department**), of the operation and effectiveness of the information sharing provisions in the TIA Act. One of the objectives of the review should be to establish a principled framework for determining which agencies should be able to receive, use or disclose TI material for the purpose of their own investigations. ASIC's access to TI material should be considered as part of the broader information sharing provisions review.

[1] ASIC Enforcement Review, 'Positions and Consultation Paper 5: ASIC's Access to Telecommunications Intercept Material', 20 July 2017, [47.2].
[2] *Telecommunications (Interception and Access) Act 1979* (Cth), s 110A(1)(ea).

Departure from intent of legislation

7. Subsection 5D(5C) of the TIA Act sets out the serious Corporations Act offences for which an interception agency may apply for a telecommunications interception warrant. In 2010 when subsection 5D(5C) was inserted into the TIA Act it was done so on the basis that:

> *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 only evidence of the offence.*[3]

8. The Explanatory Memorandum also noted that:

> *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****.*[4] [emphasis added]

9. During the course of the Parliamentary scrutiny process ASIC told the Senate Economics Committee in its evidence that:

> *… it does not expect the new telecommunications intercept powers to be frequently used. Ms Gibson noted that the magistrate would have to be satisfied that it would assist the investigation. The investigator – the AFP – would need evidence of a 'pattern of successful trading across a succession of stocks by a potential trader and would then be able to see a person building a position in a stock'. Ms Gibson recalled only 'three or four instances' in her three years working at ASIC where there was a suspected ring of insider traders.*[5]

10. The Treasury also outlined the process for telecommunications interception:

> *In the normal course of events we would expect ASIC to conduct its normal investigations, using its normal powers, to come across a circumstance where it believes a TI warrant is justified. Because it cannot apply itself, it would have to go to an intercept agency and convince the agency to apply resources to the investigation. So it would actually have to convince that TI agency, just on the information that it has already gathered, that there is sufficient evidence to justify that step and also that the offences are allegedly occurring are sufficiently serious enough for it to prioritise its own work and to actually start an investigation. Of course, that agency, once it was convinced, would then have to go to court and would have to convince the court that there was sufficient evidence and it was sufficiently serious to justify the issue of a warrant.*[6]

11. The TIA Act itself prevents ASIC from applying for an interception warrant and limits its access to such material to where an interception agency may disclose intercepted material to further that interception agency's own investigation, including a joint

---

[3] Explanatory Memorandum to the Corporations Amendment (No 1) Bill 2010 [4.4].
[4] Ibid [4.7].
[5] Senate Standing Committee on Economics, 'Report on Provisions of the *Corporations Amendment (no. 1) Bill 2010*', Department of the Senate, 17 November 2010, available at http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Completed_inquiries/2010-13/corpsamendment2010/report/index.
[6] Ibid.

investigation with ASIC.[7] Any information obtained by ASIC during the course of the investigation can only be used for the purposes of that joint investigation.[8]

12. This reflects an understanding that telecommunication intercepts are a significant intrusion into the privacy of individuals and recognises the need to strictly limit the number of agencies who can access information in that way. While the Act has been amended to include serious offences under the Corporations Act within the range of offences for which an interception agency may apply for a warrant, it is quite clear that Parliament did not intend that access to telecommunication intercept information in respect of those offences should be expanded in the manner proposed in the Consultation Paper. The Law Council considers that the Taskforce's recommendation to amend the TIA Act to enable ASIC to receive TI material should be understood as a significant departure from the intent of the current legislative access framework.

13. In such circumstances, the case for ASIC receiving, using and disclosing TI material beyond these joint investigations and particularly for an unclear set of 'other serious and relevant offences' does not currently appear to have been demonstrated. It is not clear why ASIC should receive TI material for offences that are allegedly occurring that are not, in the Treasury's words, 'sufficiently serious enough' for a core criminal law enforcement agency such as the Australian Federal Police (**AFP**) to investigate. In this context, it is also important to note that, unlike ASIC, the AFP cannot commence a prosecution for Corporations Act offences without specific Ministerial approval.[9]

14. It is does not follow that because ASIC is a 'criminal law enforcement agency' for the purposes of the TIA Act (and hence able to access the 'less sensitive' telecommunications data and sorted communications warrants) it should be able to receive the more serious telecommunication intercept information. Nor does it follow that because ASIC may consider that it has limited search abilities when compared with *Crimes Act 1914* (Cth) powers for the AFP it should have access to TI material. The ability to receive TI material would arguably be a tool that any agency would like to have to assist in their ability to investigate and prosecute offences. However, agencies have been limited in recognition of the serious privacy intrusion of the information. ASIC is not exclusively a criminal law enforcement agency and it may not be governed in a similar way to other Commonwealth law enforcement bodies or subject to the same oversight as those currently able to receive such information. The Law Council considers it would be appropriate for the Taskforce to give this further consideration.

The need for a review of telecommunications intercept information sharing provisions

15. The Taskforce's current inquiry must be seen in the context of the need for a comprehensive revision of the TIA Act, including its information sharing provisions. Recommendation 8 of the 2013 the Parliamentary Joint Committee on Intelligence and Security's (**PJCIS**) *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (**the PJCIS 2013 Report**) was that the Department review the information sharing provisions in the TIA Act to ensure:

    - *protection of the security and privacy of intercepted information; and*

[7] *Telecommunications (Interception and Access) Act 1979* (Cth), s 67.
[8] Ibid.
[9] *Corporations Act 2001* (Cth), s1315(1)(c).

- *sharing of information where necessary to facilitate investigation of serious crime or threats to national security.*[10]

16. This recommendation was made after considering a concern expressed by the Department that the complex and prescriptive nature of the existing information sharing framework represents a significant barrier to the effective use of lawfully obtained information within agencies, and to meaningful cooperation between agencies.[11]

17. The Government response to this recommendation was to support it in part.[12] It noted that the Department 'will review the information sharing provisions of the [TIA] Act'.[13] It also indicated that:

> *… the Government intends to develop a simplified regime that appropriately protects the privacy and security of lawfully accessed information while facilitating the effective use and sharing of such information for legitimate law enforcement and national security purposes.*[14]

18. The Law Council is not aware of any public review occurring on the information sharing provisions relating to TI material by the Department following the PJCIS's 2013 Report.

19. In 2015 the Senate Legal and Constitutional Affairs Committee conducted an inquiry into the *Comprehensive revision of the TIA Act*. However, the review did not examine appropriate information sharing provisions between agencies, including agencies which ought to be considered as 'recipient agencies'.[15]

20. The Law Council considers that such a review must occur prior to determining whether particular agencies ought to have expanded access to TI material through information sharing provisions.

21. The TIA Act does not expressly set out the objectives of the legislation. However, the PJCIS has formerly recommended the inclusion of an objectives clause within the TIA Act, which:

> *… expresses the dual objectives of the legislation – to protect the privacy of communications; to enable interception and access to communications in order to investigate serious crime and threats to national security; and accords with the privacy principles contained in the Privacy Act 1988 (Cth).*[16]

22. A broader review of the information sharing provisions is needed to determine the principles which should apply when seeking to balance these objectives, including when determining which agencies should be considered 'recipient agencies'.

---

[10] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (2013) Recommendation 8.
[11] Ibid [2.79].
[12] Government Response to Parliamentary Joint Committee on Intelligence and Security Report of the Inquiry into Potential Reforms in National Security Legislation, House of Representatives Committees, 1 July 2015 available at http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/reports.htm.
[13] Ibid.
[14] Ibid.
[15] Senate Legal and Constitutional Affairs Committee, *Report of the Inquiry into a Comprehensive Revision of the Telecommunications (Interception and Access) Act 1979* (2015).
[16] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (2013) Recommendation 1.

23. The Law Council appreciates the Taskforce's attempts to minimise undue incursions on privacy by its suggestion that ASIC continue to not to be considered as an 'interception agency' for the purposes of the TIA Act. Given the highly intrusive nature and gravity of this power, interception agencies are rightly limited to core Commonwealth and State and Territory law enforcement and anti-corruption bodies.

24. However, the suggestion that ASIC be considered a 'recipient agency' appears premature in the absence of a public independent (or Departmental) review of the information sharing provisions to determine appropriate thresholds which should apply for recipient agencies.

25. The TIA Act is administered by the Attorney-General who has an understanding of the legislation as a whole. In this respect, absent an independent review of the TIA Act's operation and effectiveness, the Attorney-General's Department is well-placed to conduct a public review to determine any need for reform in this area.

26. The risk with considering a particular agency's access to TI material without the development of a principled approach is that there may be an erosion of public confidence in the institutions and the ability of the Australian Government and/or Parliament to appropriately uphold privacy protections. This may be particularly critical in an environment where Australia's core law enforcement and security agencies are requesting greater access to individual data (e.g. through decryption methodologies).

27. In this context, making ASIC a 'recipient agency' under the TIA Act would be a significant shift in the operation of the legislation. Such an amendment may create a precedent for similar provisions in relation to other agencies that have typically not been able to receive TI material under the TIA Act. This would expand the impact of the TIA Act on individual privacy. Further consideration needs to be given to whether the adverse impact of such wider provisions on individual privacy is proportionate, considering the benefit in making the information available to agencies such as ASIC. A broader review of the information sharing provisions is needed to allow further consideration to the effect of any such a significant shifts in the operation of the TIA Act.

A principled framework for determining access

28. As noted above, the information sharing provisions of the TIA Act should balance the dual objectives of the TIA Act. There may be a range of factors to be appropriately considered in determining whether a particular agency should be considered a 'recipient agency' for the purposes of the TIA Act. These may include for example:

    - The agency's role as a law enforcement or integrity body;
    - The agency's role for the responsibility of investigating and prosecuting serious offences as defined in section 5D of the TIA Act;
    - The availability of equivalent or similar levels of accountability, oversight and reporting obligations as interception agencies in terms of ensuring both the security and privacy protections of the data; and
    - The availability of less privacy intrusive options for investigating and prosecuting the section 5D of the TIA Act offences.

29. Principles will also need to be developed by the information sharing review to determine the scope of access to, use and disclosure of TI material by recipient agencies. For example, it might be appropriate for agencies to be able to receive information for the purpose of investigating serious offences under section 5D of the TIA Act for which they have a primary statutory function. Australian Privacy Principle 6 is instructive for determining use and disclosure principles that should apply.

30. The Consultation Paper is not clear as to the proposed scope of information that ASIC would be able to receive, use or disclose as a 'recipient agency'. It raises the question of whether ASIC should 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"'.[17] While the serious Corporations Act offences are outlined in subsection 5D(5C) of the TIA Act, it is less clear what the other 'serious' or 'relevant' offences may encompass. The Consultation Paper notes that recipient agencies may generally use the TI material for investigations and prosecutions of 'relevant offences' within its jurisdiction.[18] This appears to suggest that 'relevant offences' may include any offences that fall within ASIC's jurisdiction. The definition of 'relevant offence' in subsection 5(1) of the TIA Act currently refers to the offences for which the chief officer of an agency can communicate information obtained by the agency to an eligible authority under section 68 of the TIA Act.

31. Given the privacy implications of telecommunications intercepts, the Law Council has serious concerns about any proposal to extend powers originally established for investigation of 'serious offences' to a broader range of less serious 'relevant offences'.

32. The range of the proposed offences must be clearly set out in the TIA Act.

33. Any amendment should also make it clear that intercepted information can only be used for the purpose of investigating criminal offences and not for any civil penalty or other civil action.

Guidance for agencies

34. Under section 68 of the TIA Act it is at the discretion of a Chief Officer of an agency who may communicate lawfully intercepted material to a 'recipient agency'. It would be important for the interception agencies to have clear guidance as to the offences in respect of which recipient agencies can receive that information.

Other options

35. The Consultation Paper appears to have given very limited consideration to other options to address the need for ASIC to have further information gathering powers to allow it to fulfill its functions in respect of the Corporations Act. Given that the current recommendation would represent a significant departure from the way in which the TIA Act currently operates, the Law Council considers that there would be merit to giving further consideration to other options. It may be useful for the Taskforce to review the current practice in other jurisdictions and consider the extent to which such practices are effective, bearing in mind the impacts on individual privacy.

---

[17] ASIC Enforcement Review, 'Positions and Consultation Paper 5: ASIC's Access to Telecommunications Intercept Material', 20 July 2017, 19.
[18] Ibid, 4.