ASIC
Australian Securities &
Investments Commission

Review of the mandatory data retention regime proscribed by Part 5-1A of the Telecommunications (Interception and Access) Act 1979: Submission by ASIC

June 2019

Introduction

1. ASIC welcomes the opportunity to contribute to the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) review of the mandatory data retention regime proscribed by Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**).

2. Telecommunications data is essential to the effective performance of ASIC's law enforcement functions and is a critical investigative tool utilised by ASIC for the investigation of serious offences against the *Corporations Act 2001* (Cth) (**Corporations Act**).

3. The types of white-collar crime investigated by ASIC are both notoriously difficult to prove and capable of causing immense harm to Australia's financial system. This harm includes damage to the integrity of Australia's financial markets, and devastation to individual victims who risk losing their houses and life savings.

4. ASIC is responsible for the investigation and prosecution of criminal offences in a range of Commonwealth statutes, including the following "serious offences" in Part 7.10 of Corporations Act that are punishable by imprisonment for up to 15 years:

    (i) insider trading (s 1043A);

    (ii) market manipulation (ss 1041A to 1041D); and

    (iii) financial services fraud (ss 1041E to 1041G), such as fraudulent investment schemes (including Ponzi schemes), cold calling 'boiler room' investment frauds and superannuation fraud.

5. Between the commencement of the metadata retention regime in October 2015 and June 2019, ASIC, in collaboration with the Commonwealth Director of Public Prosecutions (**CDPP**), secured criminal convictions against 72 persons for indictable offences, including "prescribed offences" and "serious offences" as defined in ss 5(1) and 5D of the TIA Act.

6. ASIC has contributed case studies and other information for the portfolio submission authored by the Department of Home Affairs (**DHA**). ASIC supports the views expressed by the DHA in their portfolio submission.

7. This submission will address items 1, 2, 3, 4 and 6 of the Terms of Reference for the review. As requested by the PJCIS, ASIC has also included a consolidated summary of the records it is required to keep under section 187N(3) of the TIA Act.

Continued Effectiveness of the Scheme

8. ASIC considers that the overall design of the scheme remains effective in achieving an appropriate balance between the protection of privacy and the need for law enforcement agencies to access critical information to aid in the investigation of serious offences.

9. ASIC also believes the robust and independent oversight mechanisms within the regime will ensure that this balance is maintained into the future.

10. However, it must be noted that ASIC continues to be confronted with advancements in the use of technology that are not covered by the provisions of the TIA Act and the mandatory data retention regime. While ASIC's investigative techniques have evolved to keep pace with the technological advancements employed by those contravening the law, the datasets that are required to be retained by the TIA Act remain limited.

11. For example, ASIC has seen a recent decrease in the number of authorisations for IP addresses due to the use of Virtual Private Networks (**VPNs**) administered by overseas Internet Service Providers (**ISPs**) or Virtual Private Server Providers (**VPSs**) that are not subject to the TIA Act. The data in the following table demonstrates that when ASIC accounts for IP address requests from overseas providers our overall requests for this type of data has significantly increased in line with the decrease in authorisations to domestic ISP providers under the TIA Act.

	TIA Act Authorisations for IP Addresses	Requests to International Providers
2015-2016	59	0
2016-2017	54	0
2017-2018	27	13*

*this figure includes data from July 2017 – December 2018

12. Further, ASIC has also noticed some domestic telecommunications providers appear to be leasing their numbers to overseas Direct Inward Dialling (**DID**) providers, which allows persons from a foreign jurisdiction to call from what appears to be an Australian number. From our experience, the Australian provider does not retain this subscriber information and directs ASIC to the offshore reseller. As the offshore reseller is not subject to the TIA Act it can be difficult to obtain this information.

13. ASIC has also noticed the increasing use of encrypted and internet-based communication methods that fall outside the scope of the TIA Act. For

example, in two recent market manipulation and insider trading investigations, ASIC obtained search warrants which authorised the seizure of mobile telephone devices. Upon review of the content of these devices it was discovered that the relevant communications relating to the suspected offending were sent via an encrypted internet-based messaging application. In at least one instance, the content of the communication suggested that such applications were used specifically in an attempt to evade detection by law enforcement agencies.

14. Although the scope and use of technology continues to change the metadata retention regime remains a vital investigative tool for the offending that ASIC is tasked with investigating.

Appropriateness of the Dataset and Retention Period

15. ASIC considers that the existing retention period under the TIA Act is appropriate and submits that it should be maintained. To assist the PJCIS review, the following table contains the number of authorisations obtained by ASIC since the regime commenced, and the age of the data that has been obtained:

	2015-2016	2016-2017	2017-2018	Total since commencement
Undated data	1082	1385	1471	3938
0-3 months	107	149	108	364
3-6 months	64	27	93	184
6-9 months	27	18	87	132
9-12 months	16	21	21	58
12-15 months	6	15	7	28
15-18 months	11	16	16	43
18-21 months	20	3	12	35
21-24 months	14	14	38	66
24-36 months	13	15	15	43
+36 months	23	38	30	91
Total	1383	1701	1898	4982

16. ASIC notes that the data obtained which is specified in the table as 'undated' relates to subscriber information and information held in the Integrated Public Number Database (**IPND**).

17. Apart from undated data, access to 0-3 month data is the most commonly authorised by ASIC. Access to this data is most commonly sought for investigations into suspected insider trading in contravention of section 1043A of the Corporations Act. For example, of the 107 authorisations for 0-3 month data in 2015-16, 54% were for investigations into suspected insider trading. Similarly, of the 149 authorisations for 0-3 month data in

2016-17, 70% were for investigations into suspected insider trading. Most of these authorisations were for Call Charge Records (**CCR**) or Reverse Call Charge Records (**RCCR**).

18. Access to telecommunications data that is older than 12 months is often crucial for ASIC to obtain successful criminal outcomes. As outlined above, ASIC is responsible for investigating complex financial and corporate offences that may not be uncovered for years after the relevant conduct. Once a suspected contravention is detected, telecommunications data allows ASIC to identify, and eliminate, relevant lines of inquiry and sources of admissible evidence.

19. ASIC has provided a number of relevant examples that appear in the DHA portfolio submission to the PJCIS, including:

- a 2015 investigation into suspected market manipulation in which telecommunications data ranging between 12 to 24 months in age enabled ASIC to identify that 43 accounts with a number of stockbroking firms that were dominating the market for a listed company were connected to the same person; and
- a recent investigation in which telecommunications data that was 20 months old enabled ASIC to disprove a claim that the accused had authority to vote on behalf of approximately 600 people in the election for the director of a credit union. The accused ultimately plead guilty to an offence under section 274A of the *Crimes Act 1958* (Vic).

20. These examples demonstrate the important role that retained telecommunications data that is older than 12 months can play in investigations undertaken by ASIC.

Costs

21. ASIC broadly supports the 'no profit-no loss' basis for which telecommunications providers seek to recover the costs of complying with the metadata retention regime from agencies.

22. However, ASIC holds similar concerns to those expressed in the portfolio submission by DHA that the costs charged by some service providers are unclear, inconsistent and lack transparency. It has been ASIC's experience that it is often difficult to understand and reconcile the significant discrepancies between some service providers for access to comparable datasets.

23. ASIC supports the recommendation by the DHA for a review of the charging and request frameworks between agencies and providers.

Oversight

24. ASIC strongly supports the oversight mechanisms that have been built into the metadata retention regime. In particular, ASIC considers that the annual inspections by the Commonwealth Ombudsman and reporting obligations under the regime are appropriate, proportionate and robust.

25. ASIC is of the view that similar annual inspections on the compliance of telecommunications providers with the metadata retention regime could improve overall oversight and compliance with the regime.

26. Since the introduction of the retention regime ASIC has not authorised or actioned a journalist information warrant. ASIC considers that the additional controls for obtaining a journalist information warrant under the regime are appropriate and proportionate.

Complaints

27. To ASIC's knowledge it has not received, or been the subject of, any complaints regarding the use or access of telecommunications data under the TIA Act.

ASIC's Records

28. As requested by the PJCIS, the following tables contain the data that is required to be reported annually under sections 186(1)(e) to (k) of the TIA Act. The table provided at paragraph 15 above contains the total number of authorisations made each year since the introduction of the regime and the age of the data that has been accessed by ASIC. The table at paragraph 15 therefore covers ASIC's reporting requirements under subsections 186(1)(a), (b), (c) and (f) the TIA Act.

29. Please note that the figures provided for 2015-2016 in all tables that appear in this submission only relate to authorisations made since the commencement of the metadata retention regime in October 2015. All other figures relate to the relevant financial year in which the authorisations were made.

30. Pursuant to section 186(1)(e) of the TIA Act the offences where authorisations were made by ASIC for historical and prospective data are as follows:

	2015-2016	2016-2017	2017-2018
Abduction, harassment and other offences against the person	2	1	0

Conspire/aid/abet serious offence	6	17	12
Cybercrime and telecommunications offences	0	0	161
Fraud, deception and related offences	589	649	756
Miscellaneous offences	933	1230	1320
Offences against justice procedures, government security and government operations	19	10	22
Robbery, extortion and related offences	2	1	0
Other offences relating to the enforcement of a law imposing a pecuniary penalty	0	1	0
Theft and related offences	0	6	3

31. Please note that ASIC may obtain a single authorisation for telecommunications data under section 178 and 179 of the TIA Act for multiple offences.

32. Pursuant to subsection 186(1)(g) and (h) of the TIA Act, the total number of authorisations relating to retained data that included information of the kind referred to in items 1 to 6 of the table in subsection 187AA(1) of the Act are as follows:

	2015-2016	2016-2017	2017-2018
Total number of authorisations relating to retained data which includes information in item 1 ss187AA(1)	1096	1441	1574
Total number of authorisations relating to retained data which includes information in items 2-6 ss187AA(1)	287	260	341

33. As ASIC outlined above, our agency has not applied for a journalist information warrant since the commencement of the regime and therefore have no reportable figures for the purposes of subsections 186(1)(i) and (j) of the TIA Act.