ASIC

Australian Securities & Investments Commission

Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014: Submission by ASIC

January 2015

ASIC's submission

1 ASIC welcomes the opportunity to contribute to the Parliamentary Joint Committee on Intelligence and Security's inquiry into the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill* 2014 (**TIA Bill**).

2 The TIA Bill proposes to amend the *Telecommunications (Interception and Access) Act* 1979 (Cth) (**TIA Act**) by: (i) introducing a mandatory minimum retention period for prescribed telecommunications data; and (ii) restricting the agencies who have the ability to access telecommunications data and stored communications to specified "criminal law enforcement agencies". ASIC, which currently has the ability to access both types of material for certain law enforcement purposes, is excluded from the proposed definition of "criminal law enforcement agency", even though it has major criminal law enforcement functions and obligations. Accordingly, ASIC's existing powers in this field will be removed if the TIA Bill is enacted in its current form.

3 In light of the general importance of telecommunications data to effective law enforcement, ASIC fully supports the mandatory retention proposals in the TIA Bill. This reform does not involve conferring new powers on law enforcement agencies, but rather seeking to ensure that crucial existing powers retain their utility and are not eroded because of profit-driven changes in commercial practices.

4 In light of the essential nature of telecommunications data and stored communications to effective performance of ASIC's law enforcement functions, ASIC does not support the TIA Bill's proposed removal or weakening of its existing powers to access such material.

5 Our submission, which focuses on the second aforementioned aspect of the TIA Bill, provides information on ASIC's:

(a) status and role as a major criminal law enforcement agency;

(b) existing powers under the TIA Act;

(c) need to access telecommunications data;

(d) need to access stored communications;

(e) robust internal procedures, safeguards and oversights to protect privacy; and

(f) views about the desirability of having to rely on the possibility of a future Ministerial declaration in order to retain its existing powers under the TIA Act.

6 We would be happy to provide further, more specific, information where the Committee considers it would assist the inquiry.

ASIC as a major criminal law enforcement agency

7 ASIC is, among other things, a major criminal law enforcement agency. The types of white collar crime investigated and prosecuted 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.

8 This significant risk is expected to increase into the future given the ever-growing pool of superannuation investments and large number of Australians expecting to retire from active work in the next 20 years.

9 ASIC's express criminal law enforcement functions and obligations extend to the investigation and prosecution of "prescribed offences" and "serious offences", as defined in sections 5(1) and 5D of the TIA Act. For example:

- ASIC is responsible for the investigation and prosecution of criminal offences in a range of Commonwealth statutes,[1] including the following "serious offences" in Part 7.10 of *Corporations Act* 2001 (Cth) (**Corporations Act)** that are punishable by imprisonment for up to 10 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; and
- ASIC is also empowered to, and regularly does, investigate and prosecute other criminal offences (Commonwealth, State or Territory) where the conduct involves corporations, managed investment schemes or certain types of financial fraud,[2] including the following "serious offences":

[1] See, eg, ss 1(2)(g), 13 & 49(2) of the *Australian Securities and Investments Commission Act* 2001 (Cth) (ASIC Act); s 1315 of the Corporations Act; and ss 247 and 274 of the *National Consumer Credit Protection Act* 2009 (Cth) (NCCP Act). While all criminal prosecutions arising out of ASIC investigations are commenced by ASIC and are based on briefs of evidence prepared by ASIC, prosecutions for indictable offences are generally continued by the Commonwealth Director of Public Prosecutions (CDPP).

[2] See, eg, s 13(1)(b) of the ASIC Act. Prosecutions for State or Territory offences are commenced by ASIC or its officers in accordance with the law in each jurisdiction governing the commencement of prosecutions.

(i) general fraud offences under State legislation punishable by a maximum term of imprisonment of 7 years or more. [3]

10 ASIC is the only agency with specific statutory responsibility for investigating and prosecuting criminal offences in the Corporations Act. ASIC is also the only agency with a standing statutory entitlement to commence prosecutions for offences in the Corporations Act.[4]

11 ASIC regularly exercises these criminal law enforcement functions and obligations. For example, between 1 July 2009 to 30 June 2014:

- ASIC, in collaboration with the Commonwealth Director of Public Prosecutions (**CDPP**), secured criminal convictions against 129 persons for indictable offences, including "prescribed offences" and "serious offences" as defined in ss 5(1) and 5D of the TIA Act, and achieved sentences of imprisonment against 68 persons;[5] and
- ASIC, through the conduct of its own prosecutions, secured criminal convictions against 2,404 other persons for less serious summary offences, an average of 481 persons convicted a year.

12 On 24 June 2013 the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) handed down its report entitled *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*. In its report the PJCIS did not recommend removing or reducing ASIC's

[3] ASIC is also responsible for the investigation and civil prosecution of contraventions of a range of federal laws imposing substantial pecuniary penalties. Examples of civil penalty cases successfully brought by ASIC include: *ASIC v GE Capital Finance Australia* [2014] FCA 701 (penalties totalling $1.5 million); *ASIC v Newcrest Mining Ltd* [2014] FCA 698 (penalties totalling $1.2 million); *Idylic Solutions Pty Ltd, Re; ASIC v Hobbs* (2013) 93 ACSR 421 (penalties totalling $670,000); *ASIC v Macdonald (No 12)* (2009) 259 ALR 116 (James Hardie case) (penalties totalling $670,000); *ASIC v Vines* (2006) 58 ACSR 298 (penalties totalling $640,000); *ASIC v Vizard* (2005) 54 ACSR 394 (penalties totalling $390,000); *ASIC v Loiterton* (2004) 50 ACSR 693 (penalties totalling $805,000); *ASIC v Adler* [2002] NSWSC 483 (HIH case) (penalties totalling $900,000).

[4] Pursuant to s 1315 of the Corporations Act and s 49(2) of the ASIC Act.

[5] Some examples of recent criminal cases successfully pursued by ASIC include: *R v Johnson* [2014] VSC 175 (imprisonment for 6 years and 6 months, with a non-parole period of 3 years and 6 months); *R v Veitch*, NSW District Ct, 26 June 2014 (imprisonment for 6 years and 2 months, with a non-parole period of 4 years); *R v Maile*, QLD District Ct, 20 June 2014 (imprisonment for 4 years and 3 months, with a non-parole period of 16 months); *R v Williams*, QLD District Ct, 20 June 2014 (HIH investigation) (imprisonment for 4 years and 3 months, with a non-parole period of 16 months); *R v Kur*, WA District Ct, 21 February 2013 (imprisonment for 4 years, with a non-parole period of 2 years); *R v Evans*, NSW District Ct, 7 May 2013 (imprisonment for 5 years, with a non-parole period of 3 years and 9 months); *R v Weerappah*, VIC County Ct, 6 August 2013 (imprisonment for 4 years, with a non-parole period of 2 years); *Banovec v R* [2012] NSWCCA 137 (imprisonment for 7 years, with a non-parole period of 4 years and 9 months); *R v Hoy* [2011] VSC 95 (imprisonment for 13 years and 9 months, with a non-parole period of 9 years); *Koch v R* [2011] VSCA 435 (imprisonment for 13 years and 2 months, with a non-parole period of 10 years, reduced on appeal to imprisonment for 9 years and 10 months, with a non-parole period of 7 years and 6 months); *R v Finnigan*, NSW District Ct, 18 December 2011 (imprisonment for 10 years, with a non-parole period of 6 years); R v *Dale*, QLD District Ct, 25 November 2011 (imprisonment for 7 years and 6 months, with a non-parole period of 3 years and 2 months. The sentence was upheld on appeal: *R v Dale* [2012] QCA 303); *R v Jovicic*, QLD District Ct, 1 September 2011 (imprisonment for 7 years, with a non-parole period of 2 years and 4 months); *R v* Kennedy, QLD District Ct, 8 November 2011 (imprisonment for 6 years, with a non-parole period of 2 years); *R v De Silva* [2011] NSWSC 243 (imprisonment for 2 years and 6 months, with a non-parole period of 18 months); *R v Bangaru*, NSW District Ct, 17 December 2010 (imprisonment for 8 years and 6 months, with a non-parole period of 6 years and 4 months); *R v Hartman* [2010] NSWSC 1422 (imprisonment for 4 years and 6 months, with a non-parole period of 3 years).

existing powers under the TIA Act to access telecommunications data or stored communications. Rather, the PJC wrote the following (at pp.25-26):

> *2.54 The Committee is satisfied that access to telecommunications data for serious crime and threats to security is justified. Access for agencies not enforcing the criminal law or investigating security threats should be subject to further review.*
>
> ***Recommendation 5***
>
> ***The Committee recommends that the Attorney-General's Department review the threshold for access to telecommunications data. This review should focus on reducing the number of agencies able to access telecommunications data by using gravity of conduct which may be investigated utilising telecommunications data as the threshold on which access is allowed.***

13 This conclusion and recommendation does not justify the proposed removal of ASIC's existing powers to access telecommunications data given that ASIC is responsible for enforcing the criminal law, including investigating and prosecuting "serious offences" as defined in the TIA Act.

14 Neither the Explanatory Memorandum nor the second reading speech relating to the TIA Bill elaborates on the criteria that were adopted in determining which agencies should be included within the definition of "criminal law-enforcement agency", but in the second reading speech the Minister for Communications stated:

> *[T]he bill will strictly limit, and indeed reduce, the range of enforcement agencies permitted to access telecommunications metadata without a warrant.*
>
> *The bill will allow what we might call 'traditional' law enforcement agencies, such as the police, Customs, crime commissions and anticorruption bodies, to access this information.*

15 In light of ASIC's explicit, extensive and longstanding[6] criminal law enforcement functions, there does not appear to be logical reason for its exclusion from the primary definition in the Bill of a "criminal law-enforcement agency". In particular, ASIC is not aware of any specific submission or suggestion to the effect that it has either misused its existing powers under the TIA or should have them removed.

[6] 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, eg, sections LVII to LX of the *Companies Statute* 1864 (Vic).

ASIC's existing powers under the TIA Act

16 ASIC is currently an "enforcement agency", as defined in s 5(1) of the TIA Act.[7] Consequently:

- authorised ASIC officers are able to receive *telecommunications data* if it is reasonably necessary for enforcement of the criminal law or a law imposing a pecuniary penalty; and
- ASIC has the ability to seek a warrant from an independent judicial officer authorising ASIC to access stored communications for the purpose of investigating a "serious contravention", as defined in s 5E of the TIA Act.

17 Any subsequent use of telecommunications data or stored communications obtained by ASIC is strictly restricted by a number of legislative and procedural safeguards, in addition to oversight regimes. These are outlined later in the submission.

18 An important consideration in any assessment of the necessity of ASIC having the ability to access telecommunications data and stored communications is the fact that many of the offences it investigates and prosecutes, including all of the offences in Part 7.10 of the Corporations Act, are actually constituted by communications or otherwise generally require proof of communications for a successful conviction. For example:

- the insider trading offence in s 1043A(1) ordinarily requires proof that inside information was communicated to the accused;
- the insider trading offence in s 1043A(2) specifically criminalises the "communication" of inside information;
- the market manipulation offences in ss 1041A to 1041C ordinarily require proof of communications, such as placing orders for the offending trades by telephone or over the internet, and the identity of the persons who made them;
- the market manipulation offence in s 1041D specifically criminalises the "circulation or dissemination" of offending "statements or information";
- the offence in s 1041E (false or misleading statements) specifically criminalises the "making" or "dissemination" of offending statements or information;
- the offence in s 1041F (inducing persons to deal) criminalises the "making" or "publishing" of offending statements or information; and

[7] ASIC falls within paragraph (n)(i) of the definition of "enforcement agency" in s 5(1) of the TIA Act because ASIC's functions include, among other things, "administering a law imposing a pecuniary penalty".

- the offence in s 1041G criminalises engaging in "dishonest conduct" in the course of carrying on a financial service business, which commonly involves communications of false or misleading information.

19 The central importance of telecommunications evidence and the need for ASIC to obtain such evidence in relation to investigations of these market-related offences was specifically recognised by the then Minister for Financial Services, Superannuation and Corporate Law when introducing reforms to the TIA Act in 2010.[8]

20 One particular type of serious criminal activity investigated by ASIC that involves communications is "cold calling" investment frauds, which can be prosecuted as a serious fraud offence against State Acts or as a financial services fraud offence against the Corporations Act. These frauds involve individuals being unexpectedly called and subjected to intense pressure into buying investments on the premise of high returns (sometimes as high as 300 per cent in just 15 days), but the returns are often completely fictitious and the investments a sham or worthless.

21 An example of cold calling frauds involved ASIC's investigation between September 2009 and April 2013 of 17 cases of investment fraud causing over $8 million in losses to Australian investors. In these investigations, ASIC used telecommunications data as a crucial form of intelligence. The Australian Crime Commission estimated that between January 2007 and April 2012 more than 2,600 Australians lost over $113 million to investment frauds, but it is believed there is a high level of under-reporting and the extent is far greater.[9]

22 Investigations and prosecutions for Corporations Act offences are notoriously difficult, resource-intensive and time-consuming. Effective performance of ASIC's law enforcement functions can only be achieved if we have adequate powers to obtain information and evidence about suspected contraventions of the laws we administer. Given the increasing role of telecommunications in the delivery of financial services in Australia, including carrying out trades on Australia's markets, ASIC anticipates that its need to obtain telecommunications data and stored communications will correspondingly increase over time.

---

[8] Minister for Financial Services, Superannuation and Corporate Law, Speech, 2 March 2010, available at: http://ministers.treasury.gov.au/listdocs.aspx?doctype=1&PageID=005&min=ceba. Also see Minister for Financial Services, Superannuation and Corporate Law, Media Release, 28 January 2010, available at: http://ministers.treasury.gov.au/listdocs.aspx?doctype=0&PageID=003&min=ceba.

[9] Australian Crime Commission, *Serious and organised investment frauds*, *https://www.crimecommission.gov.au/publications/intelligence-products/crime-profile-fact-sheets/serious-and-organised-investment-frauds*.

Access to telecommunications data

23 In its current form, the TIA Bill restricts access to telecommunications data to "criminal-law-enforcement agencies", a term that currently excludes ASIC.

24 In order to adequately perform its important law enforcement functions ASIC requires the ability to obtain cogent proof of telecommunications involving suspected offenders. ASIC agrees with the following assessment in the Explanatory Memorandum to the TIA Bill at pp. 5-6:

> *Telecommunications data is increasingly important to Australia's law enforcement and national security agencies, allowing agencies to determine how and with whom a person has been communicating.*
>
> *Access to telecommunications data has proven to be a critical tool for security and enforcement law agencies, providing both intelligence and evidence when identifying and prosecuting offenders. Telecommunications data provides agencies with an irrefutable method of tracing all communications from end-to-end. It can also be used to demonstrate an association between two or more people, prove that two or more people communicated at a particular time (such as before the commission of an offence), or exclude a person from further inquiry. The attrition of data will have a deleterious impact on law enforcement agencies' intelligence and evidence gathering capabilities.*

ASIC's use of telecommunications data

25 Pursuant to sections 178 and 179 of the TIA Act, ASIC currently accesses and uses telecommunications data for the purpose of a large proportion of its investigations into suspected criminal offences and civil penalty contraventions. For example, in 2013/14 ASIC staff exercised their authority to access telecommunications data for the purpose of criminal investigations on 1,771 occasions and civil penalty investigations on 110 occasions. Telecommunications data is particularly essential for investigations into suspected insider trading. Over the past two years (November 2012 to November 2014) ASIC has utilised telecommunications data in 81.4% of such investigations.

26 ASIC's extensive use of telecommunications data reflects its vital importance. ASIC concurs with the conclusion of Anthony Blunn that "*access to telecommunications data is, and for the foreseeable future will remain, fundamental to effective security and law enforcement*".[10] One of the main uses of telecommunications data was accurately identified at

[10] Blunn, *Report of the Review of the Regulation of Access to Communications* (August 2005), p.5.

p.14 of the Attorney-General's Department's Discussion Paper to the Committee's prior inquiry relating to telecommunications reform:

> *Telecommunications data is commonly the first source of important lead information for further investigations and often provides a unique and comprehensive insight into the behaviour of persons of interest.*[11]

27 As this observation illustrates, telecommunications data is often an elemental source of information and intelligence at early stages of an investigation. It is frequently used to either initially identify suspected offending and offenders or verify preliminary suspicions. Without such data many offences and offenders would never be detected or investigations would be prematurely discontinued due to lack of evidence. Telecommunications data is particularly crucial in establishing sufficient grounds to obtain various types of warrants authorising more intrusive investigatory measures, such as search warrants or (for interception agencies) telecommunications interception warrants.

28 On 28 November 2014 ASIC Commissioner Greg Tanzer told the Parliamentary Joint Committee on Corporations and Financial Services:

> *The point that the Chairman [of ASIC] made in his Bloomberg speech is: the access to that data is absolutely essential for the discharge of our law enforcement responsibilities, particularly with respect to insider trading and market manipulation, superannuation fraud and the like. We had made the point, indeed publicly, that, for example, the actions that we took in Trio were facilitated by access to that information, and the actions that were recently taken in relation to some insider trading involving a National Australia Bank employee and an ABS employee also were facilitated by - more than facilitated by - access to that information.*

29 In addition, telecommunications data is an essential *ongoing* source of both intelligence and evidence during ASIC investigations and in subsequent proceedings. In particular, it is often crucial for the purpose of seeking to prove the existence and nature of potentially relevant communications and/or relationships, especially in the absence of evidence of the content of those telecommunications. Telecommunications data is also an essential tool in identifying which individuals should be excluded from ongoing investigation.

30 The following examples demonstrate ASIC's need to access telecommunications data for the effective performance of its law enforcement functions.

[11] Attorney-General's Department, Discussion Paper, *Equipping Australia against emerging and evolving threats* (July 2012) p.14.

Example 1: Insider trading

Between August 2013 and May 2014, Lukas Kamay, an employee of the National Australia Bank (NAB), received market-sensitive information from Christopher Hill, an employee of the Australian Bureau of Statistics (ABS), before its official release by the ABS. Mr Kamay then used this information to trade in foreign exchange derivative products, resulting in profits of approximately $7 million.

Telecommunications data received by ASIC identified communications between phone numbers registered to Mr Kamay and Mr Hill in September 2013, establishing a critical connection between the two men. Call charge records also indicated that the two men ceased communications just prior to the suspected offences, which supported ASIC and the Australian Federal Police (**AFP**) suspicion that the men were attempting to avoid detection by law enforcement agencies.

On 9 May 2014, following a period of surveillance, the AFP and ASIC executed eight search warrants in Melbourne and Canberra and arrested Mr Kamay and Mr Hill. A brief of evidence was then prepared and forwarded to the defence which contained a substantial amount of incriminating telecommunications data. On 16 September 2014, Mr Kamay and Mr Hill pleaded guilty to a range of insider trading, identity fraud and abuse of public office charges.

Example 2: Market Manipulation

Between 16 May 2006 and 2 November 2006 Dr Mervyn Jacobson was involved in manipulating the share price of ASX-listed company Genetic Technologies Ltd (GTG) to create an artificial price for GTG to manage and reduce margin calls on margins totalling approximately $12 million. Dr Jacobson regularly communicated instructions to trade in GTG shares to Rocco Musumeci, a trainee client adviser, by phone. Dr Jacobson also regularly communicated information about the conspiracy to manipulate the price of GTG shares with co-offenders Geoffrey Newing and Tamara Newing by phone.

Telecommunications data established the persons responsible for sending and receiving communications and the date and times these communications were made. The telecommunications data provided evidence of phone communication between offenders at key times surrounding suspicious trading activity.

In November 2014, after an eight week jury trial in the Supreme Court of Victoria, Dr Jacobson was found guilty of 35 charges in relation to the market manipulation of the share price of GTG shares. Evidence of telecommunications data was a crucial part of the prosecution case against Dr Jacobson. He was subsequently sentenced to a total term of two years and eight months imprisonment, with 12 months to serve before being released on a recognisance release order to be of good behaviour for 20 months.

Four other convictions in relation to this market manipulation syndicate also relied on similar evidence of telecommunications data.

Example 3: Insider trading

In March 2014, three men were convicted on insider trading charges following an ASIC investigation.

Chris Jordinson, a former CEO of UCL Resources Limited (UCL), received confidential, price-sensitive information that UCL was going to receive a takeover offer from its major shareholder. Mr Jordinson communicated the inside information to his nephew, Joe Turner, and encouraged him to acquire UCL shares.

Mr Turner then communicated the inside information to a friend, Jonathan Breen, and provided him with money and instructions to acquire UCL shares. Mr Breen committed insider trading offences when he acquired 107,463 UCL shares on behalf of Mr Turner and himself.

All three men were convicted and sentenced for their roles in this insider trading syndicate.

Telecommunications data established that Mr Jordinson and Mr Breen communicated with Mr Turner at relevant times. In particular, the telecommunications data demonstrated that certain mobile handsets held by the three men (identified by their mobile phone's unique IMEI numbers) may contain SMS messages that may provide evidence of the suspected offences. ASIC then issued notices to the three men under the ASIC Act to compel them to produce those mobile phones. Subsequent inspection of the phones revealed that the three men had sent and received SMS messages containing and referring to the insider information.

When confronted with the compelling evidence recovered from their mobile handsets, the three men pleaded guilty to insider trading offences.

Mr Jordinson received a sentence of imprisonment for two years, fully suspended on the condition he enter into a two year good behaviour bond. Turner and Breen were convicted and ordered to be of good behaviour for two years.

All illegal profits were recovered under the *Proceeds of Crime Act 2002* (Cth).

Example 4: Obtaining financial advantage by deception

Between January 2004 and September 2007 Craig Dangar was engaged by SMSF Consultants Pty Ltd (SMSF) to provide technical superannuation advice to trustees of self-managed superannuation funds. SMSF is a company related to an accounting practice operated by a chartered accountant, Paul Atkins.

One of the companies that Mr Dangar advised clients to invest in was Morris Finance Ltd (Morris), an unlisted public company. Mr Dangar was a director of Morris and had an interest in 24.5% of the Morris shares (49,500 shares), neither of which were disclosed to clients that he recommended invest in Morris.

> Between September and November 2006, Mr Dangar advised two clients of SMSF to purchase a portion of the shares of Morris that he owned. In providing his recommendation, Mr Dangar deceived the two clients by misrepresenting the true owner of the shares and by also stating to one of the clients that the shares would experience capital growth.
>
> Mr Dangar pleaded guilty to obtaining a total financial advantage of $250,000 by deception. On 13 February 2013 Mr Dangar was sentenced in the District Court of NSW to a suspended sentence of 18 months imprisonment.
>
> The use of telecommunications data was required to prove the times and dates that Mr Dangar contacted victims by phone to advise them to purchase Morris shares. In addition, due to his extensive travel between states, ASIC needed to ascertain Mr Dangar's location at the time of each call as it determined which state offence had been contravened. Call charge records providing location information assisted in this jurisdictional issue.

31 If ASIC is not included within the definition of "criminal law-enforcement agency" and loses its ability to access telecommunications data it will frequently be unable to effectively investigate these types of cases.

Access to stored communications

32 In its current form, the TIA Bill removes ASIC's existing ability to seek independently issued warrants to access stored communications (e.g. the content of SMS messages and emails). While obtaining a warrant for access to stored communications is difficult, resource intensive and time-consuming, ASIC does seek access to this material in those particular cases in which it appears that there may still exist relevant stored communications and ASIC is able to meet the relatively high threshold for obtaining a warrant.

33 In these cases, ASIC considers this evidence and intelligence can be crucial to the ongoing success of the investigation. Stored communications are a proven valuable source of intelligence to ASIC and constitute crucial evidence for proving serious offences which ASIC is primarily responsible for investigating and prosecuting. Between 1 July 2008 and 30 June 2013 ASIC sought and obtained 19 such warrants.[12] As the following examples illustrate, stored communications can be extremely valuable.

[12] ASIC does not frequently apply for warrants to access stored communications as ASIC is unable to issue ongoing preservation notices. Accordingly, as some telecommunication service providers delete stored communications within short periods of time (sometimes as little as 24 hours) ASIC is required to issue a separate historical preservation notice each day prior to the issuing of the stored communications warrant. This is a resource-intensive task to ensure the preservation of stored communications, such as SMS messages.

Example 5: Dishonest conduct

Trio Capital Limited was formerly the trustee of five superannuation entities and the responsible entity for 25 managed investment schemes, including Astarra Strategic Fund (ASF). The ASF was a fund of hedge funds which had reported assets of $125 million.

Shawn Richard, former investment manager of ASF, dishonestly used ASF funds to make fraudulent investments for which he received in excess of $6.4 million in undisclosed payments. Most of the assets invested were subsequently lost.

During its investigation, ASIC obtained a stored communications warrant in relation to private email addresses suspected to be used covertly by Mr Richard to communicate with other persons involved in the misconduct. The emails were crucial evidence of a dishonest scheme in which funds from ASF were used to purchase shares in small US companies at inflated prices. When Mr Richard became aware that ASIC had obtained these emails, it began a process which led to his guilty plea in December 2010.

In August 2011, Mr Richard was sentenced to 3 years and 9 months imprisonment, with a non-parole period of 2 years and 6 months, for dishonest conduct in carrying on a financial services business.

Example 6: Insider trading

In July 2011, while in possession of information that his employer, Hanlong Mining Limited, was going to announce takeover bids for ASX-listed companies Bannerman Resources Limited (Bannerman) and Sundance Resources Limited (Sundance), Bo Shi 'Calvin' Zhu procured his mother-in-law and a private company, Wingatta Pty Ltd (Wingatta), to acquire financial products relating to Bannerman and Sundance. Wingatta was the trading vehicle for a syndicate of four employees of Hanlong, including Mr Zhu.

On 11 August 2011, during a covert investigation, ASIC applied for a stored communications warrant to retrieve SMS messages relating to phone numbers used by Mr Zhu and other suspects. The recovered messages indicated that Mr Zhu had provided instructions for the disbursement of the trading profits from an account in the name of Wingatta to four offshore accounts controlled by the four members of the insider trading syndicate.

This crucial evidence supported ASIC's suspicions that Mr Zhu was an active participant in the suspected misconduct and assisted ASIC's decision to apply for search warrants for Mr Zhu's residence and other related addresses.

Following ASIC’s investigation, Mr Zhu agreed to plead guilty to insider trading offences and provide evidence against the other members of the syndicate. On 15 February 2013, Mr Zhu was sentenced for insider trading offences to 2 years and 3 months jail, with a non-parole period of 15 months.

ASIC's robust internal procedures

34 Any use of telecommunications data or stored communications obtained by ASIC is strictly restricted by:

- obligations imposed on ASIC under the TIA Act;
- ASIC's obligation to comply with the *Australian Privacy Principles*, which arises because ASIC is an "APP entity" within the meaning of s 6(1) of the *Privacy Act* 1988 (Cth) (**Privacy Act**); and
- section 127 of the ASIC Act, which imposes an additional obligation upon ASIC to protect the confidentiality of such information.

35 ASIC also maintains strict internal procedures to protect privacy and ensure we meet all of our obligations when exercising our powers.

TIA Act obligations

36 The TIA Act limits ASIC's use of telecommunications data and stored communications. In particular, such information can only be used for the purpose of enforcing criminal laws or laws imposing pecuniary penalties (as opposed to broader regulatory purposes). In addition, ASIC must keep, and allow inspection by the Commonwealth Ombudsman, records relating to stored communications.

37 The Commonwealth Ombudsman conducts an annual inspection of ASIC's compliance with the stored communications access provisions of the TIA Act. The Ombudsman's inspection criteria includes an assessment of:

- the destruction of stored communications;
- record keeping;
- compliance with the TIA Act when applying for each warrant;
- compliance with the TIA Act when providing and revoking perseveration notices;
- adherence to any conditions or restrictions placed on any warrants;
- compliance with the requirement for lawfully accessed information to only be communicated to authorised officers; and
- the validity of ASIC's execution of each warrant.

38 Since the Commonwealth Ombudsman's first report in 2008-09, the Ombudsman has found that ASIC has complied with these legislative provisions each year.

39 The TIA Act also requires ASIC to provide information to the Attorney-General's Department on our use of stored communications powers. The Attorney-General's Department uses this information for the TIA Act Annual Report.

Privacy Act and Australian Privacy Principles

40 ASIC is an APP entity and must implement procedures that will ensure ASIC's compliance with the Australian Privacy Principles.

41 ASIC must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of our functions or activities under the legislation we administer.

42 The Privacy Commissioner has the power to apply to the Federal Court to impose civil penalties on entities that engage in serious or repeated breaches of the Australian Privacy Principles.

43 We take steps to protect the personal information we hold against loss, unauthorised access, use, modification or disclosure, and against other misuse. These steps include password protection and access privileges for accessing our IT systems, securing paper files in locked cabinets and physical access restrictions.

44 When no longer required, personal information is destroyed in a secure manner after it has met the destruction date identified in a records authority issued by the National Archives of Australia.

Confidentiality and the ASIC Act

45 Section 127(1) of the ASIC Act requires ASIC to take reasonable measures to prevent unauthorised use and disclosure of information it receives in confidence in connection with its statutory functions. This information includes telecommunications data and stored communications obtained under the TIA Act.

Internal procedures

46 ASIC's robust internal procedures and safeguards ensure our powers are properly exercised. These include:

- strict guidelines for approving telecommunications data requests, including mandatory sign-off by an Executive Level lawyer, Information Resource Centre Log Approver and Authorised Officer (as defined in the TIA Act);

- policies relating to when ASIC can access stored communications and how to obtain approval, apply and execute a stored communications warrant;
- policies relating to when ASIC can access telecommunications data and how to obtain approval and issue a request for telecommunications data;
- policies setting out ASIC's obligations concerning revocation of stored communications warrants, destruction of accessed information and record-keeping;
- oversight by Senior Executives within ASIC's Chief Legal Office, who are generally responsible for recommending or approving applications for stored communications warrants, and a designated Executive Level Stored Communications Warrant Compliance Officer, who is responsible for ensuring overall compliance with the TIA Act; and
- mandatory memoranda to the Chairman of ASIC, requesting the destruction of stored communications records, which must be destroyed forthwith if the Chairman of ASIC is satisfied that those records are not likely to be required for a purpose referred to in s 139(2) of the TIA Act. This duty cannot be delegated to another ASIC officer.

Ministerial declaration

47 The TIA Bill contains provision for the Minister to declare that other agencies are "criminal law-enforcement agencies", having regard to various factors, and to impose conditions in relation to the extent to which such agencies can access telecommunications data and stored communications.

48 It is possible that if ASIC applied to the Minister to be included in such a declaration it would meet the criteria set out in the TIA Bill. However, there is no certainty that the Minister would make a declaration. If a declaration were made, ASIC considers that it would be a sub-optimal outcome because:

- as the making of a declaration would be a challengeable decision, it would result in some legal uncertainty about the nature and extent of ASIC's powers in this field, which would reduce the efficiency of ASIC's investigations and prosecutions and may encourage legal challenges by alleged offenders;
- such a declaration may be limited by subject matter or be subject to a sunset provision, or be otherwise subject to restrictive or onerous

conditions not applicable to analogous agencies included within the statutory definition; and

- even if a declaration were made by the current Minister at the time the Bill became operational that was not limited by subject matter or time, such a declaration would not bind a future Minister and might be revoked or otherwise varied (the Minister could revoke the declaration at any time under proposed subsection 110A(8)).

49 As a result, having to rely on a Ministerial declaration may result in reduced confidence in Australia's financial system and damage to members of the community who have invested their savings in Australia's markets, arising from possible perceptions that ASIC is not adequately empowered to effectively perform its law enforcement functions.

Conclusion

50 ASIC understands and accepts the concerns that have been expressed about privacy of individuals in light of potential misuse of this information. However, ASIC submits that there is a legitimate law enforcement need justifying ASIC's access to this information and that there are appropriate safeguards in place to prevent its misuse. The alternative, of removing the power of ASIC to access this information, would significantly impair ASIC's ability to perform its law enforcement role and expose the Australian financial market and victims of crimes investigated by ASIC to unacceptable risks. In our view, the better course would be to enable ASIC to retain its existing ability under the TIA Act to access both telecommunications data and (via warrant) stored communications. Making ASIC's power contingent upon a Ministerial declaration introduces legal uncertainty that does not appear to be justified in light of the explicit and extensive nature of ASIC's criminal law enforcement functions and obligations.