Senate Economics Legislation Committee

ANSWERS TO QUESTIONS ON NOTICE

Treasury Portfolio

Additional Estimates

2014 - 2015

Department/Agency: ASIC
Question: AET 131-141
Topic: ASIC gutted by new data retention regime
Reference: Written - 6 March 2015
Senator: Dastyari, Sam

Question:

With reference to: ASIC gutted by new data retention regime, The Sydney Morning Herald, 12 November 2014.

Questions
131. On 12 November 2014 a news article was published saying ASIC had been left off the list of agencies proposed to be able to access retained telecommunications data. Can you please give us some insight into how ASIC uses telecommunications data?
132. What are the volumes of data are accessed by ASIC?
133. What type of information is accessed?
134. Has this information been critical in successful prosecutions of breaches of the law?
135. How many cases?
136. Are there some examples you could give?
137. How would it impact ASICs operations if it were not able to access this data?
138. Is it fair to say that some of ASICs prosecutions would not have been possible if access to this data was it available?
139. What representations did ASIC make to the Government about being included on the list of approved agencies?
140. Is it still the case that ASIC is not on the list?
141. Did the Government indicate it would reconsider placing ASIC on the list of approved agencies?

Answer:

131. ***On 12 November 2014 a news article was published saying ASIC had been left off the list of agencies proposed to be able to access retained telecommunications data. Can you please give us some insight into how ASIC uses telecommunications data?***

Pursuant to sections 178 and 179 of the *Telecommunications (Interception and Access) Act (Cth)* 1979 (**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. Telecommunications data is a critical tool for ASIC providing both intelligence and evidence to identify and prosecute offenders. Telecommunications data can be used to identify, or provide evidence of, networks among persons of interest and can prove that two or more people communicated at a particular time, such as before the commission of an offence.

Telecommunications data is also used by ASIC to identify individuals who should be excluded from any ongoing investigation.

ASIC uses this data in a range of matters, such as bribery, false or misleading statements to the market, insider trading, market misconduct and fraud.

Further, many of the offences ASIC investigates and prosecutes, including all of the offences in Part 7.10 of the *Corporations Act 2001* (Cth), 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
- 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.

132. ***What are the volumes of data are accessed by ASIC?***

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.

133. ***What type of information is accessed?***

The types of telecommunication data ASIC commonly receives when ASIC officers exercise their authority to access such data include: subscriber information (for example, the name and address of the telecommunications account holder), call record information for the period (for example, the outgoing call phone number, incoming call phone number, the date, time and duration of the call), SMS record information (the outgoing SMS phone number, the incoming SMS phone number, the date and time of the SMS). The location for the originating or receiving call or SMS may be included, being the base station name.

134. ***Has this information been critical in successful prosecutions of breaches of the law?***

Telecommunications data is often a key 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 may not have been detected or investigations could have been prematurely discontinued due to lack of evidence. Telecommunications data is, and has been, particularly crucial in establishing sufficient grounds to obtain various types of warrants authorising more intrusive investigatory measures, such as search warrants. In these ways, ASIC considers telecommunications data has been critical in the successful investigation, and subsequent prosecutions, for breaches of the law.

135. ***How many cases?***

Given the nature of investigations and litigations and the multitude of factors which contribute to a successful prosecution, it would be inappropriate for ASIC to specifically identify the number of prosecutions which would have been unsuccessful without access to telecommunications data. However, ASIC has provided examples of successful prosecutions which have utilised telecommunications data below (see answer to question 136).

136. ***Are there some examples you could give?***

Telecommunications evidence has been used in over 80% of our insider trading investigations, including in the Lucas Kamay and Christopher Hill insider trading, public abuse and money laundering prosecution.

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. 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.

On 17 March 2015, Mr Kamay was sentenced to seven years and three months imprisonment, with a minimum term of four and a half years. Mr Hill was jailed for three years and three months with a minimum term of two years.

There are a number of additional examples outlined in ASIC's submissions to the Parliamentary Joint Committee on Intelligence and Security's inquiry into the

Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (**TIA Bill**) (**PJCIS inquiry**).

137. ***How would it impact ASIC's operations if it were not able to access this data?***

In light of the essential nature of telecommunications data to the effective performance of ASIC's law enforcement functions, ASIC's criminal law enforcement operations would be significantly impacted if ASIC did not have access to telecommunications data. Investigations and prosecutions for *Corporations Act 2001* (Cth) 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 will correspondingly increase over time.

138. ***Is it fair to say that some of ASIC's prosecutions would not have been possible if access to this data was it [sic] available?***

As telecommunications data is frequently used by ASIC to either initially identify suspected offending and offenders or verify preliminary suspicions, ASIC considers that if the data was not available many offences and offenders may not have been detected or investigations could have been prematurely discontinued due to lack of evidence.

139. ***What representations did ASIC make to the Government about being included on the list of approved agencies?***

ASIC submitted a public submission and a supplementary confidential submission to the PJCIS inquiry raising concerns that ASIC was not included in the list as a criminal-law enforcement agency. The public submission provided information on ASIC's status and role as a major criminal law enforcement agency; existing powers under the TIA Act; need to access telecommunications data; need to access stored communications; robust internal procedures, safeguards and oversights to protect privacy; and 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. The confidential submission provided information on ASIC's experiences with telecommunications services providers' short or varying retention periods of telecommunications data.

140. ***Is it still the case that ASIC is not on the list?***

The Government supported the Parliamentary Joint Committee on Intelligence and Security's recommendation that ASIC (and the Australian Competition and Consumer Commission) be included as criminal law enforcement agencies under proposed section 110A of the TIA Act.

The Government stated that it "recognises the law enforcement related functions of these agencies and will amend the TIA Bill to specifically list these agencies as criminal law-enforcement agencies in the TIA Act. "

The TIA Bill passed both Houses on 26 March 2015, which included ASIC as a criminal law enforcement agency.

141. ***Did the Government indicate it would reconsider placing ASIC on the list of approved agencies?***

See answer to question 140.