Senate Standing Committee on Economics

ANSWERS TO QUESTIONS ON NOTICE

Treasury Portfolio

Budget Estimates

4 – 6 June 2013

Question: BET 10

Topic: **Content Blocking**

Hansard Page: **Tuesday 4 June 2013, Page 91-92**

Senator LUDLAM asked:

Senator LUDLAM: I want to very briefly change the subject. I will come back to content blocking. Can I confirm that ASIC supports the retention of telecommunication data and also content? I note that Commissioner Tanzer, at the hearing of the joint committee on 27 September in Sydney, was pretty forthright about ASIC's inability to access lawfully intercepted information. This relates to the data retention proposals that were forwarded by the Attorney-General to the joint committee. Could you confirm for us that it is ASIC' view that a data retention scheme would be good for the work of the agency?
Mr Kell: I do not think we have changed our view from what Commissioner Tanzer said on that occasion. I do not have before me exactly what he said.
Senator LUDLAM: For what length of time do you believe telecommunication data should be retained?
Mr Kell: We would have to take some of those issues on notice.
Mr Price: If data retention were introduced, I think it would be subject to an appropriate consultation process about length of time and so forth.
Senator LUDLAM: Yes. I am interested to know what ASIC would bring to the table. It would certainly need a degree more consultation than it has had thus far, but what is the position of ASIC? That is what I am interested in while we have you here.
Mr Price: That is a hypothetical question, I think.
Senator LUDLAM: No, not at all. It is real and present. Your commissioner has been telling the committee what ASIC's policy is. I am just trying to draw you out on some details that were not canvassed. For what length of time do you believe data retention should be implemented? For what forms of data—whether it is just the traffic data or the telecommunication's data or also content? Do you support the Attorney-General's view that it should be rolled across the entire population of the country, including, obviously, everyone sitting in this room?
Mr Kell: I think it would be better for us to take those questions on notice. We are happy to provide a response.
Senator LUDLAM: And the purpose of that, as to whether or not it would actually improve your record of successfully prosecuting people? Perhaps we could go to the cause or why.
Mr Kell: Yes.

Answer:

ASIC strongly supports a mandatory minimum retention period for telecommunications data and stored communications. At present there is no minimum retention period and telecommunications carriers retain communications for varying periods. For example, one carrier might retain stored communications for 24 hours after they are made or received, while another retains them for 14 days, and another for up to 90 days.

Senate Standing Committee on Economics

ANSWERS TO QUESTIONS ON NOTICE

Treasury Portfolio

Budget Estimates

4 – 6 June 2013

For serious corporate fraud offences and fraudulent investment schemes (such as Ponzi schemes and superannuation fraud) there may be a gap of some years between the transmission of telecommunications data which we could later use in detection and investigation of the offences and as evidence. Even in markets offences, there may be a long lag between commission and detection of the offence. Recently we obtained stored communications from seized computers and mobile phones that dated back over 5 years before the investigation commenced. That telecommunications evidence was instrumental in obtaining a guilty plea in relation to the insider trading case involving Hanlong Mining. Had that evidence not been available through that route then we would have needed to access it under the Telecommunications (Interception and Access) Act. For completeness, serious criminal offences are not affected by a statute of limitations.

We regularly use our existing powers under the TIA Act to obtain telecommunications data and stored communications. Our experience has been that, for those forms of telecommunications data that we are able to access under the TIA Act, access to these forms of evidence is cost-effective, timely, low-risk and extremely successful for obtaining intelligence and evidence. For instance, stored communications evidence was crucial in recently securing convictions against a pivotal offender in the collapse of Trio Capital, which was recently described as the largest superannuation fraud in Australian history.