



GOVERNMENT TO SEEK BOOST TO ASIO POWERS

ASIO to get increased powers under new legislation to be introduced within a fortnight. Rohan Pearce Computerworld) on 25 June, 2014

Read more articles on Cyber security at: <http://abalinx.com/abcyberlinx/>

Attorney-General George Brandis has indicated that the federal government will seek to boost the powers of national security agencies such as ASIO. The changes potentially include recommendations from a committee of the previous parliament that advocated changes to the ASIO Act to "enable the disruption of a target computer for the purposes of executing a computer access warrant." The attorney-general today told the Senate that the government "has decided to give effect to important recommendations of the report of the Parliamentary Joint Committee on Intelligence and Security in its report into potential reforms to Australia's national security legislation."

"In particular, I will be introducing legislation in the next sitting fortnight to give effect to the recommendations in chapter four of that report," the attorney-general said. "Those are the series of recommendations which deal with the powers of Australia's national security agencies. That legislation has been developed in recent weeks and, as I say, I will be introducing it in the next sitting fortnight." The Parliamentary Joint Committee on Intelligence and Security in June last year issued the report on changes to national security legislation. Recommendations in section four of the report include updating the Australian Security Intelligence Organisation Act 1979 to address difficulties "that can arise in executing ASIO's computer access warrants".

The ASIO Act "should be amended so that the prohibition on disrupting computers does not apply to activities that would be necessary to execute the warrant," the committee's report stated. Legislation "currently restricts ASIO from doing anything under a computer access warrant that adds, deletes or alters data or interferes with, interrupts, or obstructs the lawful use of the target computer by other persons." "This prohibition operates regardless of how minor or inconsequential the interference, interruption or obstruction may be," the report stated.

Another recommendation in section four of the report is that legislation should be amended so that ASIO can "access third party computers and communications in transit to access a target computer under a computer access warrant". In a separate section of its report the committee considered whether a mandatory data retention scheme should be introduced, but declined to take a firm position on the issue. "This is ultimately a decision for Government," the report stated. "If the Government is persuaded that a mandatory data retention regime should proceed, the Committee recommends that the

Government publish an exposure draft of any legislation and refer it to the Parliamentary Joint Committee on Intelligence and Security for examination."

Asked on Monday about data retention and so-called metadata, Prime Minister Tony Abbott told a press conference that "it's important to ensure that our police and our security services have the means at their disposal to ensure that our community is safe," and that the government "will do whatever is reasonably necessary to secure the safety of our community." The Telecommunication (Interception and Access) Act 1979, changes to which were also canvassed by the committee, is currently the subject of an inquiry instigated by Greens Senator Scott Ludlam.

http://www.computerworld.com.au/article/548508/government_seek_boost_asio_powers/?utm_medium=www.computerworld.com.au&utm_source=article_body_related_article



EFA TAKES WAIT-AND-SEE APPROACH TO ASIO CHANGES

Attorney-General George Brandis has said he will seek to increase the powers available to Australian intelligence agencies

Rohan Pearce (Computerworld) on 27 June, 2014

Online civil liberties group Electronic Frontiers Australia will wait until Senator George Brandis unveils his raft of changes to the *Australian Security Intelligence Organisation Act 1979* before passing judgement on them, but EFA executive officer Jon Lawrence says he is hopeful that the Attorney-General's proposals will not be "too extreme". Lawrence said the organisation is concerned about extensions to ASIO's surveillance powers, "especially anything that is not specifically targeted or that can be undertaken without a warrant".

"We're also very concerned that the current situation in Syria and Iraq may be used to rush changes through without the opportunity for a sober, objective debate on the balance between security and civil liberties," Lawrence said. Brandis announced earlier this week that he would seek to give increased powers to intelligence agencies including ASIO based on a report (PDF) issued by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) during the last parliament. Brandis told the Senate that he would be "introducing legislation in the next sitting fortnight to give effect to the recommendations in chapter four of that report".

"I think there are a few things in [section four] that we're not terribly happy with, but it wouldn't, for example, include any proposal for data retention or anything like that," Lawrence said. The potential introduction of a mandatory data retention regime for telcos was covered in section five of the report. There was a "diversity of views" within the PJCIS

on the issue of a data retention regime, the report states. "This is ultimately a decision for Government," the report concluded.

A *Daily Telegraph* report that was published two days before Brandis' announcement and revealed the AG's intention to boost ASIO's powers said that a data retention regime would be introduced as separate legislation later in the year. Lawrence said that although data retention is "definitely on the agenda" he doesn't expect it to be included in the first tranche of legislation introduced by Brandis.

"At the end of the day, our primary overriding concern is to do with untargeted mass surveillance and stuff that can be done without proper oversight in terms of warrants and so forth," the EFA spokesperson said. "If they're going after legitimate targets and it's quite specific and they've got some sort of warrant approval, then in the greater scheme of things that's less of a concern for us than mass, all-economising potential surveillance that data retention, for example, involves."

However, he added that some elements in section four were potentially concerning for civil liberties advocates. These include recommendations that ASIO be allowed to "disrupt" computer systems as well as access third-party "computers and communications in transit to access a target computer under a computer access warrant". "The devil of course will be in the detail" of the legislation introduced by the government, Lawrence said. The EFA executive officer said the organisation is very concerned about the abolition of the Independent National Security Legislation Monitor.

The Senate Legal and Constitutional Affairs Legislation Committee is currently conducting an inquiry into the *Independent National Security Legislation Monitor Repeal Bill 2014*. The inquiry was due to report on 2 June; however the Senate has extended the committee's deadline to 19 August.

http://www.computerworld.com.au/article/548710/efa_takes_wait-and-see_approach_asio_changes/



GUIDE CAUTIONS FEDERAL AGENCIES ON RESPONSIBLE USE OF DATA

Rohan Pearce (Computerworld) on 27 June, 2014 15:31

AGIMO issues draft guide on using data analytics. The Australian Government Information Management Office has issued a draft guide for public sector organisations looking to deploy data analytics.

The draft guide (PDF) "is intended as an appendix of the *APS Better Practice Guide for Big Data* and, should be read in this context", AGIMO assistant secretary, Marc Vickers, wrote in a blog entry. The *APS Better Practice Guide for Big Data* was issued in April. "Because big data projects often use information about individuals and, almost always, decisions and actions resulting from these findings may affect individuals, public sector agencies need to ensure that they maintain trust and operate within acceptable bounds as they increase their use of new technologies such as data analytics," cautions the draft *Guide to Responsible Data Analytics*.

Agencies must ensure that projects involving analytics projects are "in the general interest of the community"; must "identify and apply relevant ethical guidelines"; comply with the "values of the administrative law system; have an open data approach in the absence of privacy concern; adhere to relevant privacy and security principles; and that ensure "scope of assurance programs include management and use of data". Agencies must also investigate any data breaches or oversights.

The big data guide issued in April identified big data as "an opportunity to address complex, high volume and high speed problems that have previously been beyond the capability of traditional methods" "This includes finding new solutions for enhanced evidence based policy research, improved service delivery and increased efficiency," it stated. "Agencies need to identify the opportunities brought by big data and assess their alignment with strategic objectives and future business operating models. Agencies also need to articulate the pathway for developing a capability to take advantage of the opportunities."

http://www.computerworld.com.au/article/548726/analytics_guide_cautions_federal_agencies_responsible_use_data/?utm_medium=www.computerworld.com.au&utm_source=article_body_related_article