For Official Use Only

QTB13/32

SURVEILLANCE ALLEGATIONS - PRISM

What effect does the National Security Agency's PRISM program have on the privacy of Australians? Do Australian agencies use PRISM to circumvent Australian law?

Talking points

MATERIAL ON THIS PAGE HAS BEEN DELETED UNDER SECTION 7(2A)(b) OF THE FOI ACT - UNLESS OTHERWISE INDICATED

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Contact:	S47F(1)	Phone:	S47F(1)	Adviser:	S47F(1)
Division:	NSLPD	Dep Sec:	Tony Sheahan		
Date Updated:	27 June 2013				

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

If asked whether the Australian Signals Directorate or another intelligence agency, directly or indirectly, obtained access to strategic components of the National Broadband Network in order to facilitate surveillance or monitoring on Australians?

- No. Interception and access to telecommunications in Australia is undertaken strictly in accordance with the law.
- The NBN is the largest nation-building project in Australian history and it will become the backbone of our information infrastructure.
- As a strategic and significant Government investment, we have a responsibility to do our utmost to protect the NBN's integrity.
- The Australian Government treats protection of the NBN - as a significant piece of infrastructure - with the utmost importance.

Contact: S47F(1) Phone: S47F(1) Adviser: S47F(1)
Division: NSLPD Dep Sec: Tony Sheahan
Date Updated: 27 June 2013

Background

Policy commitments and key facts

The communication interception activities of all national security and law enforcement agencies are conducted under the *Telecommunications (Interception and Access) Act 1979*.

The US Director of National Intelligence publicly clarified that the PRISM program is an internal government computer system used to facilitate the US Government's lawful collection of foreign intelligence information from electronic communication service providers under warrants issued by the Foreign Intelligence Surveillance Court, as authorized by the US Foreign Intelligence Surveillance Act.

Questions from Senator Xenophon 26 June 2013

Senator Xenophon asked the following question in the Senate on 26 June 2013.
Whether the Australian Signals Directorate or another intelligence agency, directly or indirectly, obtained access to strategic components of the National Broadband Network in order to facilitate surveillance or monitoring on Australians?

Australian Greens' reaction

Senator Ludlam, the Australian Greens communications spokesperson wrote that Australia's intelligence agencies are "actively complicit in the United States' surveillance of Australian citizens". Senator Ludlam added: "The Australian Government was aware of the spying, and collaborating to circumvent due process through receipt of vast amounts of surveillance material from the United States".

Senator Ludlam has placed the following seven questions on notice to you in the Senate:

(1) Is the Australian Government or any of its law enforcement agencies aware that the United States (US) National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) are utilising a back-door program called PRISM to tap directly into the central servers of US Internet companies to source meta and content data information without warrants.
(2) Has information obtained using PRISM without warrant by the FBI or NSA about Australian citizens—including audio and video chats, photographs, e-mails, documents, and connection logs or other material—been shared with Australian law enforcement or intelligence agencies.
(3) Does the Australian Government believe it is appropriate that the US intelligence agencies appear to be engaged in warrantless real-time surveillance of the entire online population.
(4) Are the communications and information held by Australian Government, law enforcement and intelligence agencies also collected or is there an agreement to prevent the use of PRISM or other back door programs.
(5) Given the use of Microsoft programs at Parliament House and electorate offices, are the communications of Australian Federal Members of Parliament protected from or vulnerable to the PRISM program.
(6) How do the Australian Privacy Principles apply to Australian customers of Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple.
(7) Has the Australian Government ever offered immunity from legal proceedings to companies that open their servers to data-intercepting efforts by Australian intelligence organisations.

Contact:	S47F(1)	Phone:	S47F(1)	Adviser:	S47F(1)
Division:	NSLPD	Dep Sec:	Tony Sheahan		
Date Updated:	27 June 2013				

Senator Ludlam has also indicated that he will move an Order for the production of documents in the Senate to cause disclosure from the Government on these issues.

Media Reporting

[redacted]

Extensive media reporting continued between 8 and 14 June 2013.

Contact:	S47F(1)	Phone:	S47F(1)	Adviser:	S47F(1)
Division:	NSLPD	Dep Sec:	Tony Sheahan		
Date Updated:	27 June 2013				

FOR OFFICIAL USE ONLY

Australian Government
Attorney-General's Department

Sub No: AG-SB2013/1251
File No: 13/9005

Date submitted to Office by AGD: 10 JUL 2013
Min No:

ATTORNEY-GENERAL AND MINISTER FOR EMERGENCY MANAGEMENT

Proposed Answers to Senator Ludlam QoNs – PRISM

Deadline: 10 July 2013 to enable tabling of these answers in the Senate within the required timeframe.

Key Issues: Senator Ludlam has asked seven questions of you regarding Australia's involvement in the United States National Security Agency's PRISM program, the legality of US activities under US law as well as the potential impact on Australian Parliamentarians and application of the *Privacy Act 1988*.

2. **AGD Analysis:** S33(a)(iii)

Financial Implications: Nil.

Material deleted under s 7(2A)(b) of the FOI Act

Sensitivities and Communications Plan:

Recommendation: I recommend that you approve these answers for tabling in the Senate.

Approved / Not Approved / Discuss

.....
Attorney-General
Minister for Emergency Management
18 / 7 /2013

AGD Clearance

Geoff McDonald, Acting Deputy Secretary, National Security and Criminal Justice Group, 6141 2900
Date Cleared: 10/07/2013

Action Officer: S47F(1) **h:** 02 S47F(1) Date sent for approval by AO: 03/07/2013
Branch Head: Acting Assistant Secretary, TSLB, 6141 S47F(1)

Background

3. There has been extensive international and domestic media reporting since 7 June 2013 about allegations of mass surveillance by the United States' National Security Agency following leaks by Edward Snowden.

S33(a)(iii)

5. The US Director of National Intelligence publicly clarified that the PRISM program is an internal government computer system used to facilitate the US Government's lawful collection of foreign intelligence information from electronic communication service providers under warrants issued by the FISC, as authorised by the US Foreign Intelligence Surveillance Act.

6. Senator Ludlam, has previously written that Australia's intelligence agencies are "actively complicit in the United States' surveillance of Australian citizens". Senator Ludlam added: "The Australian Government was aware of the spying, and collaborating to circumvent due process through receipt of vast amounts of surveillance material from the United States".

7. An article in *The Canberra Times* on 7 June 2013 quoted Mr Jon Lawrence, spokesman for online users' lobby group *Electronic Frontiers Australia* stating, "it was likely that Australians' data was caught up in the NSA surveillance program, because many Australians had signed up for online accounts on US-based servers. Given the close working relationship between US and Australian intelligence agencies, there's also no reason not to suspect that the NSA has been sharing information gathered about Australians with Australian intelligence agencies."

8. The communication interception activities of all national security and law enforcement agencies are conducted under the *Telecommunications (Interception and Access) Act 1979*. The TIA Act also protects the privacy of all communications in Australia by prohibiting

Relevance to Election Commitments/Government Policy

9. The Australian Government is considering a suite of reforms and legislative amendments to the laws governing intelligence-gathering powers included in the *Telecommunications (Interception and Access) Act 1979*, the ASIO Act and the *Intelligence Services Act 2001*.

S33(a)(iii)

Consultation

10. Internal— Business and Information Law Branch provided the answer to the question about the application of the Privacy Act's Australian Privacy Principles to the collection of personal information by US-based companies such as Microsoft, Google and Facebook.

11. External— the Australian Signals Directorate, ASIO, AFP and the Department of Broadband, Communications and the Digital Economy have been consulted on the development the submission.

Sensitivities and Communication Plan Material deleted under s 7(2A)(b) of the FOI Act

ATTACHMENTS:

13. **Attachment A**: Answers to Senator Ludlam's Questions on Notice for tabling in the Senate.

SENATE QUESTION

QUESTION NUMBER: 3003

Senator Ludlam asked the Minister representing the Attorney-General, upon notice, on 11 June 2013

(1) Is the Australian Government or any of its law enforcement agencies aware that the United States (US) National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) are utilising a back-door program called PRISM to tap directly into the central servers of US Internet companies to source meta and content data information without warrants.

(2) Has information obtained using PRISM without warrant by the FBI or NSA about Australian citizens—including audio and video chats, photographs, e-mails, documents, and connection logs or other material—been shared with Australian law enforcement or intelligence agencies.

(3) Does the Australian Government believe it is appropriate that the US intelligence agencies appear to be engaged in warrantless real-time surveillance of the entire online population.

(4) Are the communications and information held by Australian Government, law enforcement and intelligence agencies also collected or is there an agreement to prevent the use of PRISM or other back door programs.

5) Given the use of Microsoft programs at Parliament House and electorate offices, are the communications of Australian Federal Members of Parliament protected from or vulnerable to the PRISM program.

(6) How do the Australian Privacy Principles apply to Australian customers of Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple.

(7) Has the Australian Government ever offered immunity from legal proceedings to companies that open their servers to data-intercepting efforts by Australian intelligence organisations.

Senator Ludwig– The Attorney-General has provided the following answer to the honourable senator's question:

(1) The Australian Government does not comment on the law enforcement or intelligence capabilities of other countries.

However, I can refer to statements made by President Obama and the United States Director of National Intelligence that United States intelligence agencies operate within the law, are subject to strict congressional and judicial oversight and that access to telecommunications information was authorised by a warrant issued by the United States Foreign Intelligence Surveillance Court.

(2) As indicated in my response to question on notice 3003 (1) above, the Australian Government understands that information obtained by United States agencies was authorised by a warrant issued by the United States Foreign Surveillance Court.

Australia's intelligence agencies operate under a strong legal framework to protect Australians at all times, including when dealing with information from outside Australia.

Intelligence Services Act 2001 agencies, such as the Australian Signals Directorate, are required by law to obtain specific authorisation either from the Minister for Defence or the Minister for Foreign Affairs to produce intelligence on an Australian.

For matters relating to threats to security, the Attorney-General must also support the approval. All such activities are independently examined by the Inspector-General of Intelligence and Security to ensure that authorisations are conducted in accordance with the law. Any information obtained by our agencies from the US is subject to these protections.

(3) As indicated in my response to questions on notice 3003 (1) and (2) above, the Australian Government understands that information obtained by United States agencies was authorised by a warrant issued by the United States Foreign Surveillance Court.

(4) Any access to communications in Australia must be in accordance with the provisions of the Telecommunications (Interception and Access) Act 1979.

The legal and oversight arrangements of all Australian Government agencies should assure all Australians that the privacy of their communications are appropriately protected.

(5) The communications of Federal Members of Parliament are protected by law, just as the communications of all Australians are protected by law.

In Australia, the privacy of communications is protected by the Telecommunications (Interception and Access) Act 1979 (the Interception Act). The Interception Act prohibits the listening to, copying or recording of a communication as it passes over an Australian telecommunications system.

(6) The Government's position is that entities carrying on business in Australia or an external territory should be subject to Australian laws. This includes the Privacy Act 1988, which contains the Australian Privacy Principles (APPs).

Importantly, the fact that an entity that carries on a business in Australia is located overseas or otherwise has no physical presence in Australia should not provide a basis for that entity to avoid its legal obligations and responsibilities to individuals in Australia. An individual in Australia should benefit from the protection provided to their personal information by the Privacy Act and the APPs, and entities should be accountable and responsible to individuals for providing the appropriate protection for that personal information.

Some entities that provide online services may have a physical presence in Australia and will be considered to be 'carrying on a business in Australia'. However, it is also the case that an entity can carry on a business in Australia without having a physical presence in Australia. This issue is addressed by section 5B of the Privacy Act 1988, which deals with the extra-territorial operation of the Privacy Act, and subsection 5B(3) in particular.

The Explanatory Memorandum for the Privacy Amendment (Enhancing Privacy Protection) Act 2012 makes clear that, under paragraph 5B(3)(c) of the Privacy Act, the collection of personal information 'in Australia or an external territory' includes the collection of personal information from an individual who is physically within the borders of Australia or an external territory, by an overseas entity (see page 218).

(7) All communication interception activities carried out by Australian agencies are conducted in strict accordance with Australian law.

Under subsection 313(5) of the Telecommunications Act 1997, a carrier or carriage service provider is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith while rendering lawful assistance to law enforcement and national security agencies, as required by section 313 of the Act, for example, through enabling the execution of interception warrants issued under the TIA Act.