

Sub No:  
File No: 10/1516-04

**ATTORNEY-GENERAL**

**Proposal for a mandatory data retention regime in Australia**

**Deadline: 16 June 2010.** [Redacted] S34(3), S47C(1)


**Key Issues:** [Redacted] S34(3), S47C(1)

**AGD Analysis:** [Redacted] S34(3), S47C(1)

**Financial Implications:** [Redacted] S34(3), S47C(1)

**Recommendation:** I recommend that you [Redacted] S34(3), S47C(1)

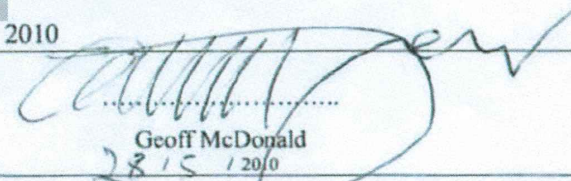
Approved / Not Approved / Discuss

  
.....  
Catherine Smith  
Assistant Secretary, Telecommunications and  
Surveillance Law Branch

.....  
Attorney-General

28/5/2010

/ / 2010

Cleared by:  .....

Geoff McDonald  
28/5/2010

.....  
Roger Wilkins AO  
/ / 2010

**Background**

2. Telecommunications data is information about a communication such as the date, time, duration, and location of a call or internet session, or subscriber details about the parties to a communication or account. It does not include the actual content of a communication. The importance of data to agencies is growing as Internet based communications, encryption and pre-paid technology becomes more prevalent.

3. The ability to lawfully access telecommunications data held by a carrier or carriage service providers (C/CSP) is a vital tool for agencies to fight and solve crime and protect national security. It enables investigators to identify and build a picture of a suspect, provides vital clues to solve life threatening situations such as child abductions, and creates evidence for alibis and prosecutions. It is critical for national security agencies to counter the terrorist threat, defeat cyber espionage and ensure border integrity and security.

4. There are also ever increasing levels of technology enabled cyber crimes such as child exploitation, online fraud, internet banking crimes and identity fraud that can only be investigated via access to historical Internet-based telecommunications data. From an investigative standpoint, telecommunications data is becoming a primary tool and in some investigations is becoming of equal or greater benefit than the content of communications, particularly as the encryption of the content of a communication is becoming increasingly prevalent and represents a major challenge for agencies.

5. Industry has advised Government that they are moving towards business and billing models which will reduce the collection of telecommunications data. S37(2)(b), S47(1)(b), S47C(1)

[Redacted]

6. Accordingly, destruction practices and developments in technology are resulting in telecommunications data not being available when disclosure is required by enforcement or national security agencies.

7. S34(3), S47C(1)

[Redacted]

8. S34(3), S47C(1)

[Redacted]

9. S34(3), S47C(1)

[Redacted]

10. S34(3), S47C(1)

[Redacted]

S34(3), S47C(1)

11. S34(3), S47C(1)

12. S34(3), S47C(1)

### Consultation

13. The Telecommunications and Surveillance Law Branch has consulted with the Freedom of Information (FoI) Section of the Cabinet and Ministerial Coordination Branch on the privacy aspects of the proposal.

14. The proposal has also been developed in consultation with the Department of Broadband, Communications and the Digital Economy, the Department of the Prime Minister and Cabinet, the Australian Security Intelligence Organisation, the Australian Federal Police, all State and Territory law enforcement agencies, the Australian Competition and Consumer Commission, the Australian Crime Commission, the Australian Customs and Border Protection Service, the Australian Securities and Investments Commission, and the Office of the Privacy Commissioner.

15. S34(3), S47C(1)

### Sensitivities and Media Implications

16. S47C(1)