



Australian Government  
Attorney-General's Department

Security and Critical  
Infrastructure Division

Sub No: 1112  
File No: 08/1219

25 MAR 2008

**Attorney-General**

**Development of a proposals for a mandatory data retention scheme**

**Deadline:** Nil

**Issue:** New and emerging telecommunications technologies have the potential to cause significant challenges to the investigative abilities of Australian national security and law enforcement agencies. A potential solution being considered by the Department is the introduction of a mandatory data retention regime.

**Action required:** That you note the challenges being faced by Australian agencies in relation to the availability of data and approve the Department's progression of the proposal.

**Recommendation**

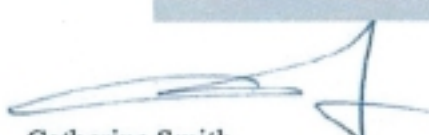
I recommend that you:

- (i) Approve the development by the Department, in consultation with other relevant Australian Government agencies, of a model for a mandatory data retention scheme.

Approved / Not Approved / Discuss

S47C(1)

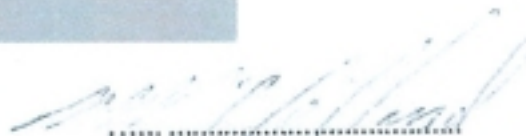
Signed by

  
Catherine Smith  
Assistant Secretary  
Telephone: S47F(1)

25 March 2008

**Action officer:**

S47F(1)  
Principal Legal Officer  
Telephone: S47F(1)

  
Attorney-General

19/3/2008

## Background

1. This submission relates to telecommunications data: that is, information about the **process** of a communication, as distinct from its **content**. This includes information about the identity of the sending and receiving parties ('A and B parties'), when a communication started and stopped, and the type of communication (i.e. a phone call, a web-browser session, or a file transfer).
2. Access to telecommunications data for law enforcement purposes is regulated by the *Telecommunications (Interception and Access) Act 1979* (the TIA Act). Chapter 4 of the TIA Act permits agencies to authorise the disclosure of telecommunications data where it is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty, or the protection of the public revenue. Chapter 4 contains separate provisions enabling access for national security purposes.

S37(2)(b), S47C(1)

### *The importance of telecommunications data*

4. Telecommunications traffic data and related information is currently kept by carriers for billing and other business purposes and has proven to be an important tool for law enforcement and national security agencies, providing both intelligence and evidence for use when identifying and prosecuting offenders.

5. S37(2)(b), S47C(1)

It can be used to prove an association between two or more people, prove that two or more people communicated at a particular time (such as before the commission of an alleged offence), or prove that a person was, or was not, in a particular location at a particular time.

S37(2)(b), S47C(1)

S37(2)(b), S47C(1)

7. The UK experience has also shown that the availability of this information can be of great benefit in providing exculpatory evidence, allowing police to rule out a person from an investigation, and to Coroners in determining the circumstances leading up to death.

S37(2)(b), S47C(1)

*Why a mandatory data retention scheme is necessary*

10. With an evolutionary trend in the telecommunications industry towards Internet Protocol (IP) based services and volume based charging models, there is the likelihood that the traditional business reasons for creating or retaining this information may cease. This concern is not isolated to Australia; data retention is a significant topic internationally.

11. In response, agencies have proposed that new requirements be introduced to ensure that the telecommunications data currently retained continues to be available for law enforcement and national security purposes.

12. The European Union is currently implementing its data retention regulation directive, in response to the rapid adoption of new technologies. It is timely for Australia to also consider how the needs of agencies can be met without unduly impacting on the telecommunications industry.

**Issues**

*What kind/type of data would need to be retained?*

13. Information would fall into two general categories: subscriber information and traffic data.

14. Agencies would require carriers to retain sufficient subscriber information so they could:
- identify the subscriber to a telecommunications service, and associated subscriber detail information, based on the service identifier, and
  - identify all services and equipment identifiers associated with a subscriber, based on a subscriber name and/or other subscriber detail information.
15. Agencies would require carriers to retain sufficient traffic information so they could:
- trace a communication S37(2)(b), S47C(1) [REDACTED]
  - ascertain the details of the communication, including:
    - the type of service used to communicate
    - the time, date and duration of the communication
    - [REDACTED]
    - the communications device(s) used, and
    - the location of the communication device(s) (whether fixed, nomadic or mobile).

*How long would the data need to be retained?*

S37(2)(b), S47C(1)

17. There is no consistent international approach for data retention for law enforcement purposes. Some countries have explicit requirements, while others do not. The most consistent approach is provided by the European Union (EU). The EU directive requires member states to introduce legislation to require specific data to be retained for law enforcement purposes for a period of at least six months but no more than two years. After this period, the data is required to be destroyed, if the carrier has no further business case requiring its retention.

*What are the likely costs?*

18. Generally, the types of costs associated with the proposal can be summarised as follows:

Collection

S37(2)(b), S47C(1)

S37(2)(b), S47C(1)

20. This is not assessed to be a large issue in relation to fixed and mobile telephony, since industry seem to already collect most of the relevant data sets for billing purposes or could do so relatively easily.

S37(2)(b), S47C(1)

S37(2)(b), S47C(1)

*Who would pay?*

25. Under current rules, carriers are reimbursed by agencies for providing assistance on a 'no-cost/no-profit' basis.

S37(2)(b), S47C(1)

*What are the likely impacts?*

27. In considering this proposal, several possible impacts must be considered.

Law enforcement and security agencies

28. As described above, reliable access to telecommunications data is essential to effective investigations. Due to changing technology, a failure to provide some legislative requirement to collect and store this data is likely to see the steady erosion of investigative capabilities which may have serious implications for the capacity of both law enforcement and national security agencies to perform their tasks.

Privacy

29. The systematic collection of telecommunications data has privacy implications, although perhaps not as significant as may first appear, since much of the information is already collected and stored by carriers.

S37(2)(b), S47C(1)

Any mandatory data retention scheme risks being seen as increasing the threat to privacy.

30. It should be stressed that the proposal does not involve keeping records of the content of communications—only the fact that the communication occurred.

Industry, innovation and changing technology

31. The central concern of the telecommunications industry is that the proposal would require them to collect and, depending on the model adopted, either store or transmit large quantities of data for which there is no business use, all of which incurs costs. To the extent that these costs are

imposed on industry, it would raise business costs for companies operating in Australia, reducing profitability and/or raising the prices of telecommunications services on consumers.

**Comment**

S47C(1)



**Consultation—internal**

34. First Assistant Secretary, Security and Critical Infrastructure Division; Deputy Secretary, National Security and Criminal Justice Group,

**Consultation—external**

35. None on this submission. However, as noted above, the requirement for data retention has been discussed in detail at officer level with Australian law enforcement agencies. These discussions have indicated strong agency support for the Department taking the lead in developing a mandatory data retention scheme.

**Media Implications**

36. None at this stage. However, should the data retention proposal proceed to public discussion, it is likely to attract considerable interest from the media and from privacy advocates. The Department will ensure that these issues are addressed in more detail at the relevant time.

**Resource Implications**

37. None at this stage.