GUIDE TO ENFORCEMENT AGENCY STATUS

1. From 13 October 2015 any agencies wanting ongoing access to historical telecommunications data must be listed as an 'enforcement agency', unless already listed as a 'criminal law enforcement agency' in section 110A of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015.*

2. The Attorney-General's Department is seeking advice from agencies that consider they require direct access to telecommunications data to fulfil their functions.

3. This guide is designed to assist organisations seeking to be included as an enforcement agency. It is not intended as legal advice or determinative of legal rights or obligations.

Changes introduced by the Data Retention Act

4. Prior to passage of the Data Retention Act, any authority or body with functions involving enforcing the criminal law, enforcing a law imposing a pecuniary penalty or a law protecting the public revenue was deemed to be an 'enforcement agency'. Those authorities and bodies could authorise access to historical telecommunications data.

5. The law has now changed to ensure that access to historical telecommunications data is limited to agencies with a clear operational need and appropriate privacy safeguards.

6. Section 110A of the Act lists specific *criminal law enforcement agencies* that are also deemed to be enforcement agencies.

7. Section 176A of the Data Retention Act provides that the Attorney-General may declare a body or authority to be an enforcement agency if satisfied on reasonable grounds that its functions include:

   (a) enforcement of the criminal law; or

   (b) administering a law imposing a pecuniary penalty; or

   (c) administering a law relating to the protection of the public revenue.

8. When doing so, the Attorney-General must have regard to:

   (a) whether the ability to access data under authorisations would be reasonably likely to assist the authority or body in performing those functions

   (b) whether the authority or body is required to comply with the Australian Privacy Principles, an equivalent binding scheme or has agreed in writing to do so

   (c) whether the authority or body proposes to adopt processes and practices that would ensure its compliance with the obligations of an enforcement agency, and

(d) whether the declaration would be in the public interest.

Next steps

9. If your organisation has in interest in enforcement agency status, you will need to write to the Attorney-General's Department by **12 June 2015**. Emails to ESPB@ag.gov.au are preferred.

10. While there is no prescribed form, all requests should be in writing. The information you provide should be accurate, credible and relevant.

11. You will need to provide sufficient detail in your request to address each of the factors in section 176A of the Data Retention Act.

12. Your request should also:

    (a) include references to the legislation underpinning relevant powers exercised by your organisation

    (b) demonstrate why your organisation cannot perform its functions using alternative information sources (i.e. without access to telecommunications data)

    (c) include evidence and examples of past use of historical telecommunications data, and

    (d) include details of a nominated contact officer.

13. The Attorney-General's Department will contact your organisation's nominated officer to confirm receipt of your request.

14. Any organisations not listed in the legislation as 'criminal law enforcement agencies' or temporarily declared to be an enforcement agency may wish to engage with law enforcement about being able to continue to be able to access this data for its investigative or operational purposes.

Guidance on the factors in section 176A of the Data Retention Act

What is a 'body' or 'authority'

15. A *body* is any identifiable group of persons (whether a body corporate or not). An *authority* is an organisation (generally public or quasi-public) that controls a subject matter area, zone or certain activities. This can include Commonwealth, State and Territory Departments, local government bodies, statutory authorities or quasi-government organisations

When will an organisation have a function of 'administering a law'?

16. 'Administering a law' may involve managing processes associated with its application or having charge of, or being involved in, its execution.

17. An organisation will generally have a 'function' of 'administering a law' where a body or authority is:

    (a) responsible for carrying legislation into effect (implementing a law or series of laws or provisions under a statute)

    (b) involved in activities supporting the ongoing application of legislation or key aspects of legislation, or

    (c) monitoring and ensuring compliance with the administrative requirements associated with the application of a law.

18. Examples include:

    (a) ensuring that obligations imposed by the legislation are performed by officials within the organisation or by members of the public, and

    (b) setting up and operating any associated administrative processes and mechanisms for ensuring the objects of the legislation are carried out. For example, a Commonwealth Department described in the Administrative Arrangement Order as the Department responsible for administering a statute would have the function of administering that statute.

19. Administering a law may also include where a body's sole function in respect of a law is to investigate possible breaches.

What is meant by 'enforcement of the criminal law'?

What is meant by 'enforcement'?

20. 'Enforcement' can extend not only to the apprehension of persons who commit an offence, but also to activities directed at investigating whether an offence has been committed (i.e. detection/investigative activities). It includes:

    (a) the process of investigating crime and prosecuting criminals, or

    (b) gathering intelligence about crime to support the investigating and prosecuting functions of law enforcement agencies.

What is the 'criminal law'?

21. Criminal law extends to laws that make certain conduct an offence punishable by fine or imprisonment such that criminal proceedings (i.e. proceedings prosecuted by Crown prosecutors and heard in criminal courts) can be taken. Criminal law can be State, Territory or Commonwealth-based.

What is meant by a 'pecuniary penalty'?

22. A 'pecuniary penalty' simply means a monetary or financial penalty designed to deter a person and others or an entity from breaching the law. For example:

    (a) the penalty payable in respect of an infringement notice or

    (b) the penalty payable in respect of civil contraventions of relevant provisions.

23. Pecuniary penalties generally include penalties for breaches of Commonwealth or State/Territory laws that are not criminal or that impose a penalty which is an administrative alternative to prosecution (they are often referred to as civil or administrative penalty provisions and are usually accompanied by a penalty unit payable).

24. Pecuniary penalties are generally paid to a Commonwealth, State/Territory body instrumentality (rather than the victim/affected party) and are imposed by civil (non-criminal) courts following a civil trial. They are designed to punish and deter unlawful behaviour, rather than compensate those directly affected by that behaviour.

25. Notably, the Explanatory Memorandum to the Data Retention Act provides that pecuniary penalties for the purposes of the statutory test in s 176A are not intended to encompass small-scale administrative fines, like minor library late-return fines.

What is meant by 'protection of the public revenue'?

26. The concept of 'public revenue' includes State and Territory revenue in addition to Commonwealth revenue. Lawful obligations charged on a regular basis such as taxes, levies, rates and royalties involve the protection of the public revenue. Occasional charges, such as fines, do not.

27. Protecting the public revenue would also include the activities of agencies and bodies undertaken to ensure that those lawful obligations are met; for example routine collection, audits, investigatory and debt recovery actions.

28. Protecting the public revenue would not include activities aimed at identifying and eliminating inefficient but lawful spending of public monies.

29. The term 'revenue' is not intended to be limited to incoming monies from taxation but could also extend to monies to which a Commonwealth, State or Territory government instrumentality has a right, or monies which are due to it.

Privacy

30. An enforcement agency must either comply with the Australian Privacy Principles, comply with a comparable framework or agree in writing to be bound to such a scheme.

Does your organisation comply with the Australian Privacy Principles?

31. The Australian Privacy Principles in the *Privacy Act 1988* include obligations relating to the:

(a) management of personal information (APP 1 and APP 2)

(b) collection of personal information (APP 3 – APP 5)

(c) use or disclosure of personal information (APP 6)

(d) security standards for retained information (APP 11)

(e) access to personal information (APP 12)

32. Guidelines and fact sheets are available via the Office of the Australian Information Commissioner. See:

(a) http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles

(b) http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP-guidelines-combined-set-v1.pdf

33. For organisations bound the *Privacy Act 1988*, your response should indicate how its processes and procedures are compliant with those principles.

Does your organisation comply with a privacy framework comparable to the APPs?

34. Your response should outline:

(a) how the binding scheme (for example, the State or Territory equivalent privacy legislation) under which your organisation operates provides protections commensurate with those which apply under the Australian Privacy Principles,

(b) identify the mechanism(s) that scheme provides to monitor privacy protections; and

(c) the provisions under which individuals can seek recourse for any alleged misuse of their personal information.

Does your organisation propose to agree in writing to comply with a privacy scheme?

35. If your organisation proposes to undertake to comply with other arrangements to provide similar or equivalent levels of privacy protection, then:

(a) the CEO or a senior officer within your organisation should provide a written undertaking affirming your organisation's compliance with a privacy protection scheme, and

(b) the undertaking should specify the scheme of arrangement to which the undertaking relates and its key privacy protection features, specifically the protection it confers in relation to personal information disclosed to carriers and how this is consistent with the Australian Privacy Principles or State/Territory equivalent privacy principles.

Public interest

36. Your response should identify the public interest considerations which weigh in favour of your organisation being given access to telecommunications data. Rather, the meaning of 'public interest' derives its content from the subject matter and the overarching context.

37. Some matters which may engage public interest considerations include, but are not limited to:

(a) public health and safety;

(b) national security;

(c) the prevention and detection of crime and fraud; and

(d) the economic wellbeing of the country.

Further information

39. The full text of the Data Retention Act is at: http://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r5375_third-reps/toc_pdf/14242b01.pdf;fileType=application%2Fpdf

40. The Explanatory Memorandum to the Data Retention Act is available at http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5375_ems_e6cf11b4-5a4e-41bc-ae27-031e2b90e001/upload_pdf/14242b01EM.pdf;fileType=application%2Fpdf