

Rec'd 230/3/2016



Australian Government
Attorney-General's Department

15/5524

16 March 2016

AF=>

Pls advise.

Mr Ahmed Fahour
Managing Director and Group CEO
Australia Post
GPO Box 1777
Melbourne Vic 3001

Dear Mr Fahour

Enforcement agency access to telecommunications data

In May 2015, I wrote to you in relation to the changes to the definition 'enforcement agency' made by the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*, and its effect on your agency's access to historical telecommunications data.

In your response, you indicated that Australian Postal Corporation continues to have an interest in obtaining direct access to metadata under the *Telecommunications (Interception and Access) Act 1979*. Thank you for the detailed information provided to the Department to support that position.

The Attorney-General acknowledges agency concerns generally and will continue to consider applications to be included in the Act as an enforcement agency on a case by case basis. However, it is unlikely that any agencies will be added to the legislated list of specified enforcement agencies in the immediate term.

You may wish to consider how Australian Postal Corporation might otherwise obtain the information it needs to undertake its functions. You could consider joint investigation arrangements with a criminal law-enforcement agency. Alternatively, I am advised that by virtue of the *Telecommunications Act 1997*, some agencies may be able to obtain information where they have separate notice to produce powers.

If you require further assistance or would like to discuss this matter in more detail, please contact [redacted] Director of the Electronic Surveillance Policy Section on [redacted] or email [redacted]

Thank you again for writing in relation to this matter.

Yours sincerely

[redacted]
Acting Secretary



06 July 2015

[REDACTED]
Deputy Secretary
National Security and Criminal Justice Group
Attorney General's Department
Robert Garran Offices, Barton ACT

Dear [REDACTED]

Enforcement Agency access to telecommunications data

I am writing in response to your letter of May 22nd 2015, addressed to the Australian Postal Corporation's ("Australia Post") Managing Director and Chief Executive Officer, and dealing with enforcement agency access to historical telecommunications data under the *Telecommunications (Interception and Access) Act*, as amended by the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*, (collectively "the Act").

Australia Post formally and respectfully requests that consideration be given to having the Minister declare Australia Post to be an 'enforcement agency' under the Act.

The reasons for and in support of the request, and detail of Australia Post's submission concerning the Corporations ability to fully and completely meet and satisfy all of the matters referred to in section 176A of the Act, appear in the attachment.

On behalf of the Managing Director and Chief Executive Officer I thank you in anticipation of consideration of the Corporations submission, and confirm that I am available to meet in person to discuss the substance of the Corporations submission at any time.

Yours sincerely,

(s 47F)

(s 22)

General Manager, Group Security

Direct telephone: (s 22)

Direct fax: [REDACTED]

Email: (s 22)

Group Security
Level 11, 111 Bourke Street Melbourne VIC 3000
GPO Box 1777 Melbourne VIC 3000

T: [REDACTED]
F: [REDACTED]
W: auspost.com.au



In the matter of the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 ("The Act")

and

In the matter of a request by the Australian Postal Corporation ("Australia Post") for a declaration that Australia Post be regarded as enforcement agency under the Act; and that persons specified, or of a kind specified, in the declaration to be officers of the enforcement agency for the purposes of the Act.

Australia Post Submission

About Australia Post

Australia Post is a Commonwealth Government Business Enterprise, constituted as a body corporate by the *Postal Services Amendment Act (1988)*, and continued in existence by the *Australian Postal Corporation Act (1989)*.

By law, Australia Post's principal function is to supply postal services within Australia, and between Australia and places outside Australia.

A subsidiary function of Australia Post is to carry on, outside Australia, any business or activity relating to postal services.

Australia Post's specific postal and postal-related powers, and its general and other powers, are set out in sections 17, 18 and 19 of the *Australian Postal Corporation Act (1989)*.

In order to fulfil its legislated functions, and in exercise of its powers, Australia Post

- o Directly employs approximately 37,000 people,
- o Engages approximately 12,000 additional service providers as contractors and licensees,
- o Operates (directly or through the licensed post office network) 4,417 postal retail outlets across Australia,
- o Operates a mails and parcels network of approximately 600 processing, sorting and delivery facilities,
- o Operates one of Australia's largest delivery vehicle fleets,
- o Receives, processes and delivers in excess of 4.5 billion domestically lodged, and approximately 200 million inbound international, postal articles per annum, and
- o Physically services approximately 11.5 million delivery points across Australia (98.8% at a five day per week frequency)

Additionally, Australia Post provides – both through physical and online channels – numerous and diverse trusted financial, identity and payment services, both as a direct provider, and, more frequently, as agent for more than 750 businesses and government entities, including over 70 financial institutions.

Relevantly for this submission, Australia Post is both a major retailer, and the largest single Australian carrier and delivery agent, of articles containing mobile telephones, and related accessories.

(s 47C), (s 47E)



Australia Post's Internal Security and Investigation Functions

For approximately 100 years, employees of Australia's national postal body (originally the Postmasters General Department, then the Australian Postal Commission, and now the Australian Postal Corporation) have acted as specialist security and investigation officers, tasked with the responsibility to

■ [REDACTED]

[REDACTED]

[REDACTED]

Australia Post is currently recognized as a "partner Commonwealth investigative agency" of the CDPP. The CDPP publicly states that

"...the CDPP has no investigative function and we can only prosecute where there has been an investigation by another agency. We rely upon Commonwealth investigative agencies to provide briefs of evidence and we work closely together to prepare and present cases in court..."

(s 47E)

[REDACTED]

The Current Security Group

(s 47E)

[REDACTED]

[REDACTED]

Use of telecommunications data

In connection with the functions of the corporations Security Group as a criminal intelligence and investigative unit, Australia Post has had historic access to telecommunications data for specific investigative purposes.

(s 47E)



Privacy and Confidentiality

For many decades, Australia Post has operated under a strict legislative regime which mandates the secrecy, privacy and confidentiality of all information held by Australia Post as a result of its operations, and which prescribes penalties, including possible imprisonment, if secrecy provisions are breached by current or former employees.

The provisions in question are set out in Part 7B of the *Australian Postal Corporation Act* (1989). All Australia Post staff and service providers are required to undertake regular 'core learning' training on privacy of personal information which includes reinforcement of the obligations imposed upon serving and former corporation personnel to maintain secrecy of business information at all times.

To support compliance with Part 7B, and to meet requirements under Commonwealth Privacy law, Australia Post has operational processes and procedures in place to fully comply with the:

- o Australian Privacy Principles (APPs) contained in the *Privacy Act 1988*.
- o Australian Direct Marketing Association (ADMA) Code of Practice in relation to how the corporation markets to our customers.
- o Spam Act 2003 in relation to electronic marketing.
- o Do Not Call Register Act 2006 where the corporation engages in telemarketing.
- o Telecommunications Industry Standard 2007 where we engage in telemarketing.
- o Payment Card Industry Data Security Standard for handling of payment card data.

[REDACTED]

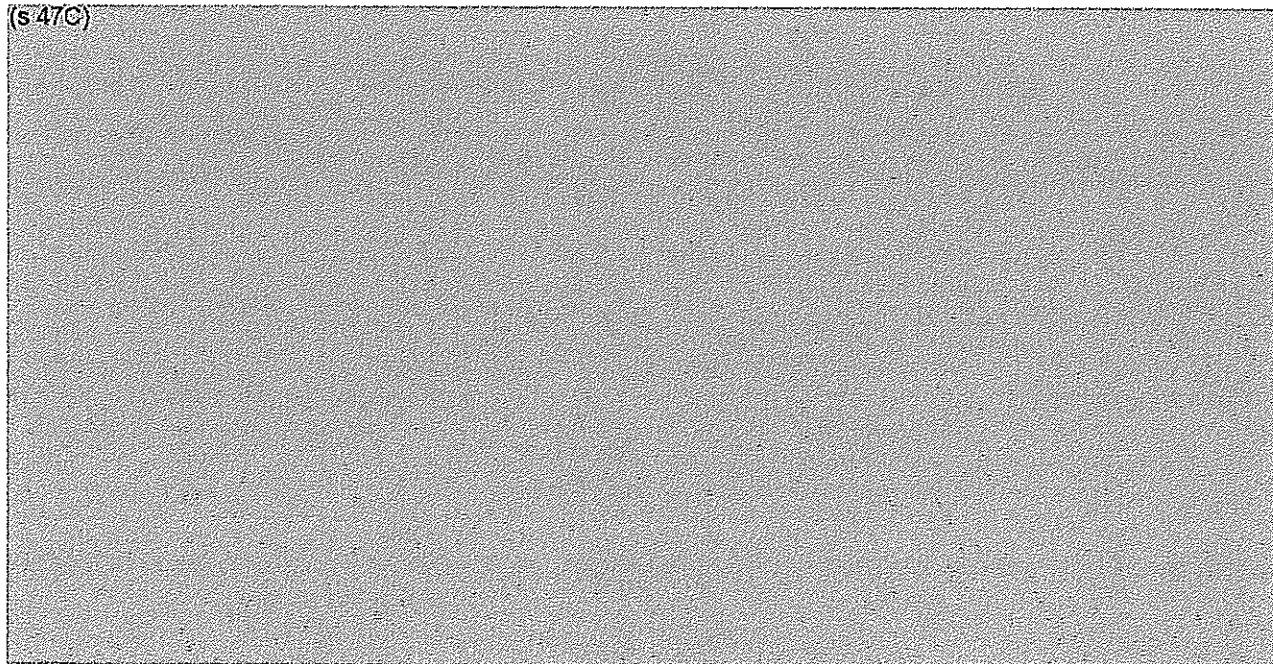
[REDACTED]

[REDACTED]

Chapter 4 of the Act

Australia Post has always fully met and complied with the obligations imposed upon enforcement agencies under Chapter 4 of the Act, and undertakes that it will continue to do so in the event that a declaration as sought by this submission is made.

(s47C)



(s 47C)



Designated Officers

In the event that, following this submission, a declaration is made that Australia Post may be declared to be an enforcement agency under the Act, Australia Post would propose that the occupants of four designated roles within the Australia Post Security function should be identified as officers of the enforcement agency for the purposes of the Act. The roles, and current incumbents are,

(s 22)



Submission dated the 6th day of July 2015

(s 47F)



For and on behalf of the Australian Postal Corporation

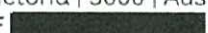
(s 22)



General Manager, Group Security
Level 11, 111 Bourke Street | Melbourne | Victoria | 3000 | Australia

(s 22)

(s 22)

| F 
| auspost.com.au



09 July 2015

[REDACTED]
Deputy Secretary
National Security and Criminal Justice Group
Attorney General's Department
Robert Garran Offices, Barton ACT

Dear [REDACTED]

Supplementary Information – Re Enforcement Agency access to telecommunications data

Further to my letter of July 6th, I have attached Australia Post's responses to the queries and requests for supplementary information posed in yesterday's message from the ESPB.

I trust that the additional comments are of assistance.

I also confirm the following matters:

1. I am authorised by Australia Post to make the statements below.
2. Australia Post is aware of the requirements under the amended legislation concerning new classes of records and documents which will be required to be created and retained by an enforcement agency, additional annual reporting requirements, the future statutory review, and new powers granted to the Commonwealth Ombudsman to monitor an enforcement agency's compliance with the Act, and
3. Australia Post undertakes that in the event of the making of a declaration affecting Australia Post under section 176A (3), Australia Post will fully and completely comply with the requirements of the Act.

Yours sincerely,

[REDACTED]
General Manager, Group Security

Direct telephone: [REDACTED]
Direct fax: [REDACTED]
Email: [REDACTED]@auspost.com.au

Group Security
Level 11, 111 Bourke Street, Melbourne VIC 3000
GPO Box 1777 Melbourne VIC 3000

T: [REDACTED]
F: [REDACTED]
W: auspost.com.au



In the matter of the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 ("The Act")

Australia Post Supplementary Submission

In response to the questions arising from the primary Australia Post submission, and posed on July 8th 2015, Australia Post provides further information in support of its submission as follows:

1. What are the specific penalties imposed by the legislation administered by Australia Post that enforces a criminal law, imposes a pecuniary penalty or protest public revenue.

Australia Post is the principal agency responsible for

- a. monitoring and ensuring compliance with, and for
- b. first line investigation of offences against,

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Commonwealth Criminal Code Act 1995	Maximum Penalty
471.1 Theft of mail-receptacles, articles or postal messages	Imprisonment 10 years

471.2 Receiving stolen mail-receptacles, articles or postal messages	Imprisonment 10 years
471.3 Taking or concealing of mail-receptacles, articles or postal messages	Imprisonment 5 years
471.4 Dishonest removal of postage stamps or postmarks	Imprisonment 1 year
471.5 Dishonest use of previously used, defaced or obliterated stamps	Imprisonment 1 year
471.6 Damaging or destroying mail-receptacles, articles or postal messages	Imprisonment 10 years
471.7 Dishonestly tampering with mail-receptacles	Imprisonment 5 years
471.7 Tampering with mail-receptacles without authority	Imprisonment 2 years
471.8 Dishonestly obtaining delivery of articles	Imprisonment 5 years
471.10 Hoaxes--explosives and dangerous substances	Imprisonment 10 years
471.11 Using a postal or similar service to make a threat to kill	Imprisonment 10 years
471.11 Using a postal or similar service to make a threat to cause serious harm	Imprisonment 7 years
471.12 Using a postal or similar service to menace, harass or cause offence	Imprisonment 2 years
471.13 Causing a dangerous article to be carried by a postal or similar service	Imprisonment 10 years
471.15 Causing an explosive, or a dangerous or harmful substance, to be carried by post	Imprisonment 10 years
471.16 Using a postal or similar service for child pornography material	Imprisonment 15 years
471.17 Possessing, controlling, producing, supplying or obtaining child pornography material for use through a postal or similar service	Imprisonment 15 years
471.19 Using a postal or similar service for child abuse material	Imprisonment 15 years
471.20 Possessing, controlling, producing, supplying or obtaining child abuse material for use through a postal or similar service	Imprisonment 15 years
Crimes Act 1914	
Section 85N Wrongful delivery of postal articles	Imprisonment 1 year
Section 85V Interference with property of Australia Post	Imprisonment 1 year
Section 85 W Causing controlled drugs or controlled plants to be carried by post	Imprisonment 2 years

(s47E)



(s 47E)



(s47E)



(s47C)



(s 47C), (s 47E)



Supplementary submission dated the 9th day of July 2015



For and on behalf of the Australian Postal Corporation

General Manager, Group Security
Level 11, 111 Bourke Street | Melbourne | Victoria | 3000 | Australia
T [REDACTED] | M [REDACTED] | F [REDACTED]
[REDACTED]@auspost.com.au | [auspost.com.au](mailto:[REDACTED]@auspost.com.au)

TO: IPND-enquiry

IPND-enquiry facsimile:

IPND-enquiry telephone:



SECURITY & INVESTIGATION
GPO BOX 1777
MELBOURNE VIC 3001
auspost.com.au

Case Investigator	ENTER S&I OFFICER's NAME
Contact No.	ENTER S&I OFFICER's CONTACT PHONE

--

NOTE: DO NOT USE FOR IMEI CHECKS Use this form when carrier is unknown, the search will cover all carriers.

Request for IPND - Enquiry

**Enforcement agency – Authorisation and notification
for access to existing information or documents**
Telecommunications (Interception and Access) Act 1979 (Cth)

1 Authorised officer

- (1) The Australian Postal Corporation is an enforcement agency within the definition of 'enforcement agency' in subsection 5(1) of the *Telecommunications (Interception and Access) Act 1979* (the Act).
- (2) I, **Enter name**, am an authorised officer of the Australia Post Security & Investigation, within the definition of 'authorised officer' in subsection 5(1) of the Act, as I am covered by an authorisation of the head of the Australian Postal Corporation under subsection 5AB(1) of the Act.

2 Authorisation

- (1) Acting under subsection 179(2) of the Act, I authorise the disclosure of the following specified information or documents, being information or documents that came into existence before the time the person from whom the disclosure is sought, **being Telstra in its capacity as manager of the IPND-enquiry facility**, received notification of the authorisation:

Service Number	Customer Name	Customer Address

- (2) I am satisfied that the authorised disclosure is reasonably necessary for the enforcement of the criminal law and/or enforcement of a law imposing a pecuniary penalty, AND in making the authorisation I declare that, **In accordance with section 180F of the Act**, I have had regard to whether any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable, having regard to:
 - (a) the likely relevance and usefulness of the information or documents; and
 - (b) the reason why the disclosure or use concerned was to be authorised.

3 Notification and disclosure

Acting under subsection 184(3) of the Act, I notify the person listed above of this authorisation.

The information or documents authorised to be disclosed by this authorisation should be delivered to the Australian Postal Corporation by the following means:

Return to Fax: **Enter Security & Investigation Fax Number for return of information**

Dated: **Enter Date**

Signature of authorised officer:.....

TIA Act 1979 Annual Report
Telecommunications Data Questionnaire YE 30 June 2015



Under section 186 of the *Telecommunications (Interception and Access) Act 1979*, the head of an enforcement agency must provide the Attorney-General after each 30 June a report that outlines the use of accessed telecommunications data.

Note: Grey field sum is an automatically generated figure.

Agency Name:

1 Access to Historical Telecommunications Data - s186(1)(a), s186(1)(b)

- | | | |
|------------|--|-----|
| 1.1 | Authorisations for historical data - s178 | |
| 1.1.1 | Total number of authorisations made for access to existing information or documents in enforcement of the criminal law | |
| 1.2 | Authorisations to locate missing persons - s178A | |
| 1.2.1 | The number of authorisations made for access to existing information or documents for the location of missing persons | |
| 1.3 | Authorisations for historical data - s179 | |
| 1.3.1 | Total number of authorisations made for access to existing information or documents in enforcement of a law imposing a pecuniary penalty or protection of the public revenue | 625 |

2 Access to Prospective Telecommunications Data - s186(1)(c)

- | | | |
|------------|--|---------|
| 2.3 | Specified duration of prospective authorisations - s180 | |
| 2.3.1 | Total number of authorisations made | |
| 2.3.2 | Total number of days authorisations specified in force | |
| 2.3.3 | Average specified duration | #DIV/0! |
| 2.4 | Actual duration of prospective authorisations - s180 | |
| 2.4.1 | Total number of days original authorisations actually in force | |
| 2.4.2 | Original authorisations discounted | |
| 2.4.3 | Average period in force | #DIV/0! |

3 Foreign law enforcement - s 186(ca), 186(cb) - AFP only

- | | | |
|------------|--|--|
| 3.1 | Foreign law enforcement - ss180A, 180B, 180C, 180D | |
| 3.1.1 | Number of authorisations made under ss180A, 180B, 180C and 180D | |
| 3.1.2 | Number of disclosures made pursuant to ss180A, 180B, 180C and 180D | |
| 3.1.3 | Names of foreign countries pursuant to s186(1)(cb)(i) TIA Act | |

**TIA Act 1979 Annual Report
Telecommunications Data Questionnaire**



Australian Government
Attorney-General's Department

Under section 186 of the *Telecommunications (Interception and Access) Act 1979*, the head of an enforcement agency must provide the Attorney-General after each 30 June a report that outlines the use of accessed telecommunications data.

Note: Grey field sum is an automatically generated figure.

Agency Name:

Australia Post YE 30 June 2016

1 Access to Historical Telecommunications Data - s186(1)(a), s186(1)(b)

1.1 Authorisations for historical data - s178

Total number of authorisations made for access to existing information or documents in enforcement of the criminal law

64

1.2 Authorisations for historical data - s179

Total number of authorisations made for access to existing information or documents in enforcement of a law imposing a pecuniary penalty or protection of the public revenue

0

[REDACTED]

From: ESPB <ESPB@ag.gov.au>
Sent: Wednesday, 27 May 2015 11:05 AM
Cc: [REDACTED]
Subject: Enforcement agency access to telecommunications data [SEC=UNCLASSIFIED]
Attachments: Guidance Note - explanation of Enforcement Agency induction process.pdf

UNCLASSIFIED

Dear Colleagues,

I am writing to advise you about changes to the Telecommunications (Interception and Access) Act 1979 that will affect your agency's ability to access historical telecommunications data. A letter in similar terms to this email (from Katherine Jones, the Deputy Secretary of the National Security and Criminal Justice Group of the Attorney-General's Department) to the chief executive of your organisation is in the post.

Background

The Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 will come into effect on 13 October 2015. The data retention legislation will ensure that law enforcement and national security agencies will continue to have the information they need to keep the community safe. To better protect individual privacy, Parliament reduced the number of agencies that may access telecommunications data from around eighty to twenty-one.

Our records indicate that your agency has accessed telecommunications data under the Telecommunications (Interception and Access) Act 1979 in the past. However, your agency is not included within the more limited access scheme commencing in October this year.

Next Steps

The legislative scheme reflects Parliament's intent that access to telecommunications data be limited to a small number of core agencies.

However, in the event you consider that your agency requires ongoing direct access to telecommunications data, please write to the Attorney-General's Department via ESPB@ag.gov.au by 12 June 2015. Your letter will need to make a compelling case for access and clearly demonstrate an ability to uphold the privacy safeguards embedded in the data retention scheme. In particular, section 176A of the Data Retention Act outlines a range of matters relevant to the possible inclusion of additional agencies on a temporary basis which should be addressed. I enclose a guidance document that may assist in considering whether your agency may be suitable for inclusion within the scheme in future. Your advice on these matters will assist the Department to advise the Attorney-General on appropriate access arrangements.

For further assistance please contact [REDACTED] Assistant Secretary of the Electronic Surveillance Policy Branch on [REDACTED] or [REDACTED] Director of the Electronic Surveillance Policy and Advice Section on [REDACTED]

Kind regards

[REDACTED] Legal Officer

Electronic Surveillance Policy and Advice

Attorney-General's Department | 3-5 National Circuit | Barton ACT 2600

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 an 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_ac4732e1-5116-4d8f-8de5-0ead3828012c/upload_pdf/501754%20Revised%20EM.pdf;fileType=application%2Fpdf