

Matter:		Date: 29.06.09	
Industry Consultation on a Mandatory Data Retention Regime		Line area: NSLDP	
Timing:	URGENT <input checked="" type="checkbox"/>	Routine <input type="checkbox"/>	Due by: ASAP URGENT
Adviser's Recommendation:	Approve <input type="checkbox"/>	Consider and/or Discuss <input checked="" type="checkbox"/>	Information Only <input type="checkbox"/>
Adviser's comment:	Requested by RW <input type="checkbox"/>	New matter <input type="checkbox"/>	Ongoing matter <input checked="" type="checkbox"/>
<p>Sub to Attorney seeks approval to consult with industry on a mandatory data retention proposal.</p> <p>Consultation paper for release - Att A</p> <p>Letter to PM seeking approval for consultation - Att B</p>			
Documents:	Minute <input checked="" type="checkbox"/>	Briefing/note <input type="checkbox"/>	Submission to Attorney <input checked="" type="checkbox"/>
			Letter to sign <input type="checkbox"/>
			Corro for RW <input type="checkbox"/>
Secretary's comment:	Discuss with Adviser <input type="checkbox"/>	Discuss with Line Area <input type="checkbox"/>	
OK to go up.		<div style="background-color: black; width: 100px; height: 50px; margin: 10px auto;"></div> <div style="text-align: center;">S47C(1)</div> <div style="text-align: right;">(7)</div>	



Australian Government
Attorney-General's Department

Sub No.
File No: 08/1219

ATTORNEY-GENERAL

Industry Consultation on a Mandatory Data Retention Regime

Deadline: As soon as possible to allow public consultation on a mandatory data retention proposal

Key Issues: You previously agreed (submission 1112 of 2008 refers) to the Department developing a proposal for a mandatory data retention regime, including the establishment of an Interagency Working Group (IWG) to advance work on specific details of the proposal. S37(2)(b), S47C(1)

The Department has finalised a draft document outlining the type of telecommunications data which would be retained under the regime (the 'data set'), options for storing that data and the scope of the proposal. The Department proposes to now consult with industry on these proposals.

AGD Analysis: Data retention in other international jurisdictions has been used as an effective tool to combat serious and organised crime. Mandatory data retention has been highlighted in S47C(1) of interception legislation as a potential mechanism to combat serious and organised crime in a global telecommunications environment.

Consultation with industry is essential for further consideration of the two year model for data retention. Consultation will include consideration of the draft data set to be retained, possible storage models and the associated cost and scope of the proposal. Industry will have strong views on all of these issues.

Financial Implications: Consultation with industry will have no financial implications, though the data retention proposal has cost implications for industry.

Recommendation: I recommend that you:

- (i) Agree to consultation with industry groups on the proposed data retention regime, including the release of the consultation paper at **Attachment A** and sign the letter at **Attachment B** seeking the Prime Minister's approval for consultation, and at **Attachment C** informing the Minister for Communications of recent developments.

Signed / Not Signed / Discuss

For Catherine Smith
Assistant Secretary
Telecommunications and Surveillance Law Branch
S47F(1)

29/06/2009

Attorney-General

/ / 2009

Cleared by:

Geoff McDonald

29/6/2009

Roger Wilkins AO
/ / 2009

Action Officer: Lionel Markey (02) 6141 3017

Background

1. You previously agreed (Submission 1112 of 25 March 2008 refers, see Attachment D) to the Department developing a proposal for a mandatory data retention scheme, consultation with government agencies and the setting up of a Commonwealth Inter-Agency Working Group (IWG) for the detailed development of data sets to be retained, the retention period and storage models, comprising The Department of the Prime Minister and Cabinet (Privacy and FOI Policy Branch), The Australian Federal Police, The Department of Broadband, Communications and the Digital Economy, The Australian Competition and Consumer Commission, The Australian Crime Commission, The Australian Securities and Investment Commission, The Australian Security Intelligence Organisation, South Australian Police and The Australian Customs and Border Protection Service.

2. [REDACTED] S37(2)(b), S47C(1)

[REDACTED]

[REDACTED]

[REDACTED]

3. As part of the agreed consultation process to progress mandatory data retention policy development, I now seek your approval to consult with the telecommunications industry on the proposal, [REDACTED]

[REDACTED] S47C(1)

The Data Retention Proposal

The proposal's role in the Organised Crime Strategic Framework

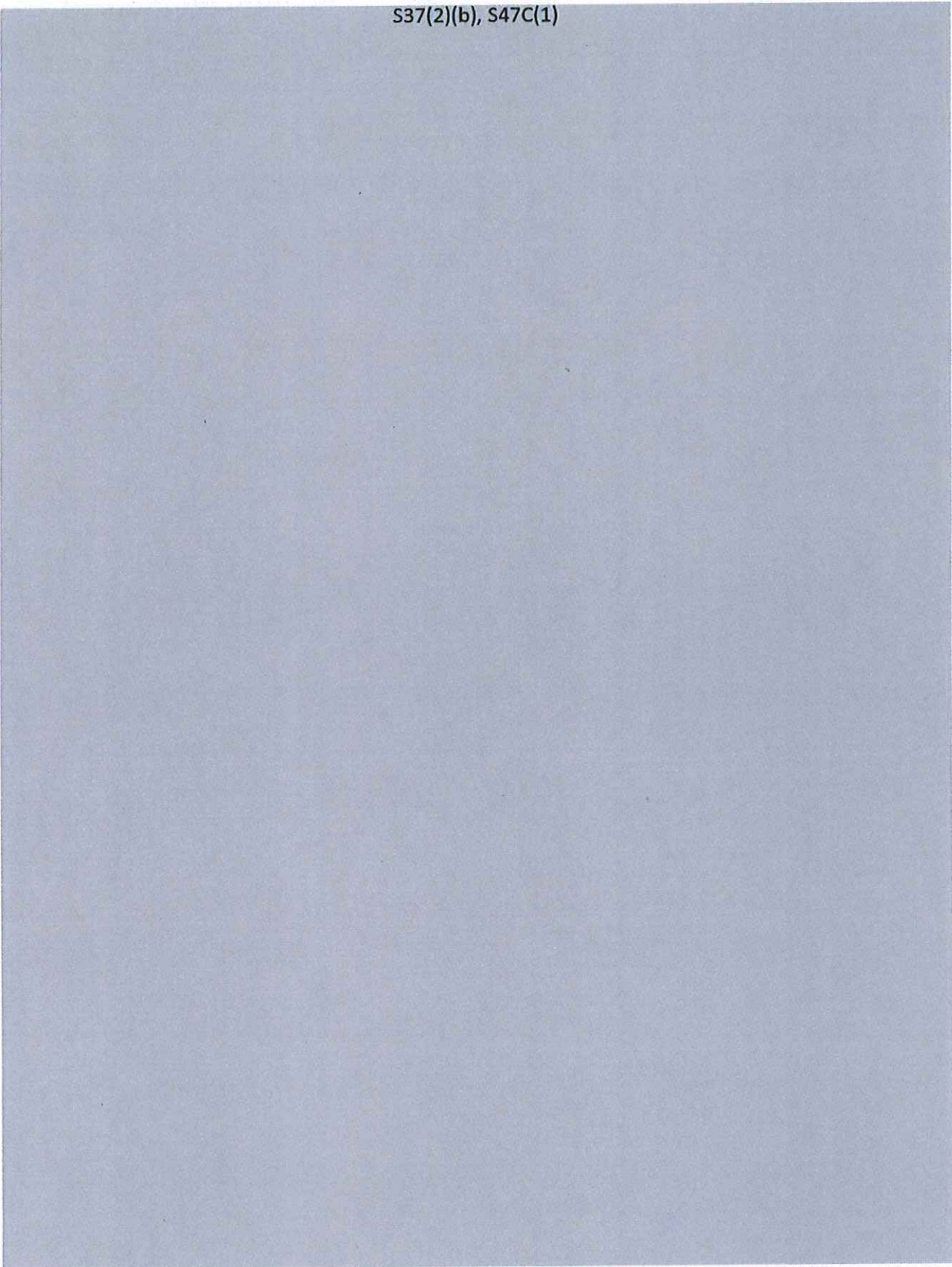
4. The Commonwealth has made an undertaking to ensure that the Commonwealth's legislative framework is responsive to the changes in the context of serious and organised crime. The *Organised Crime Strategic Framework* notes:

The Government continues to monitor the effectiveness of its legislative and operational response to organised crime to ensure it remains effective to respond to changes in society, technological advances and the criminal environment.

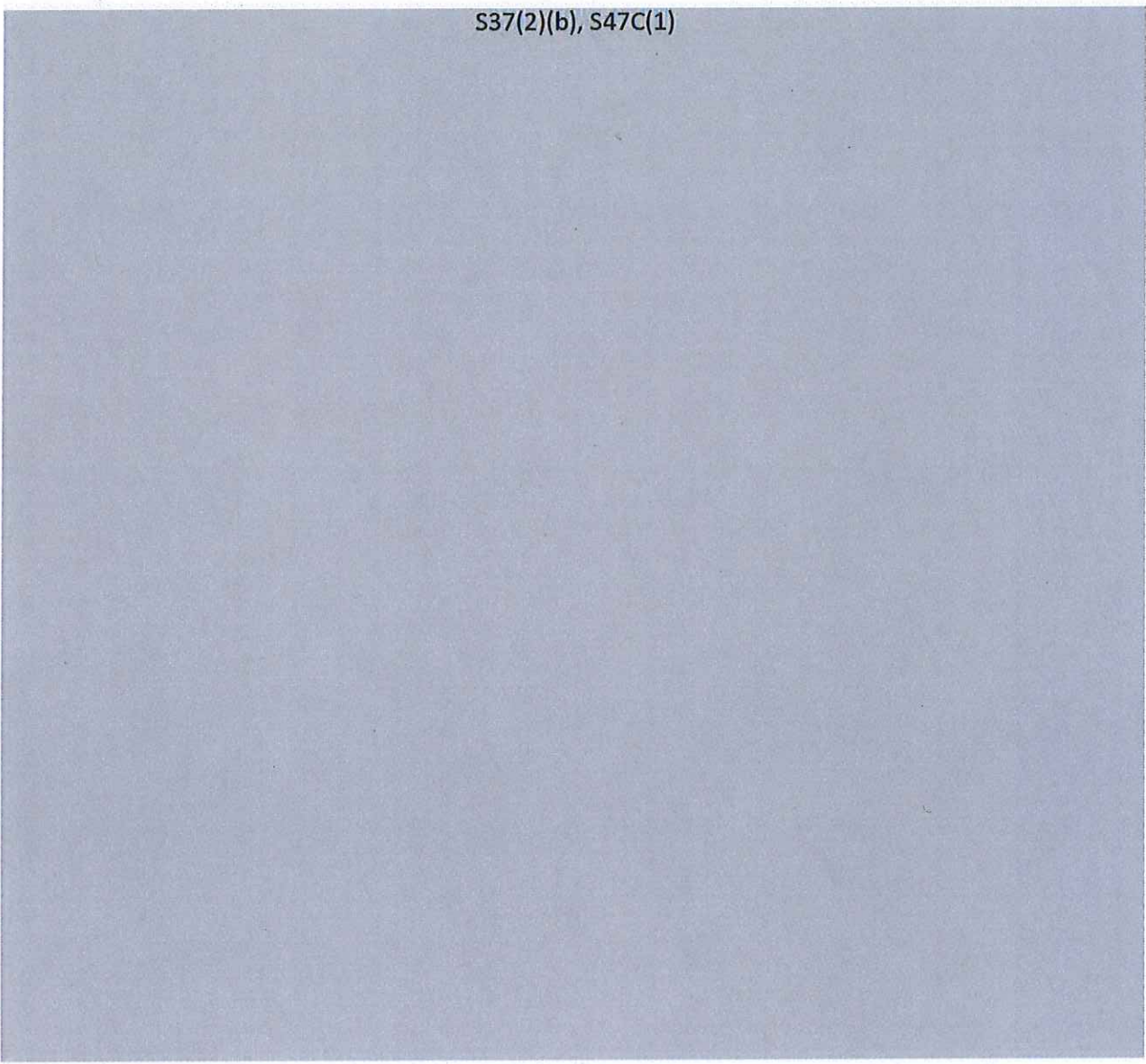
5. A mandatory data retention regime reflects the Commonwealth's commitment to respond to rapid technological and economic change in the telecommunications sector.

6. Telecommunications data has the potential to address the full spectrum of organised crime activities. When looking at classes of activity put forward in the framework, telecommunications data can be effective in the following ways:

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



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



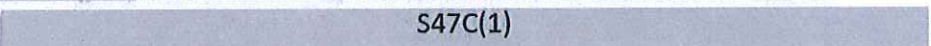
S47C(1)



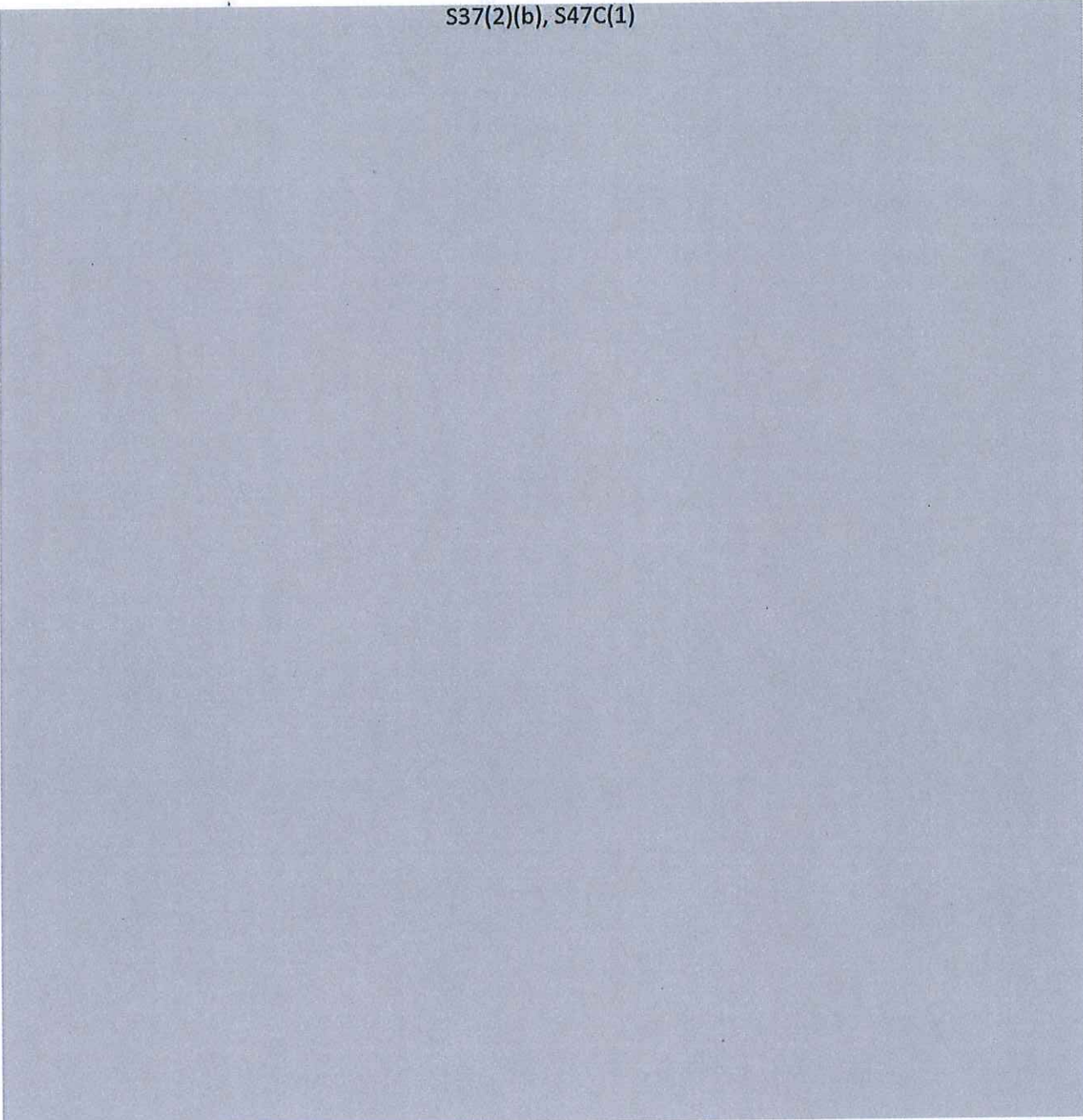
S4
7C



S47C(1)



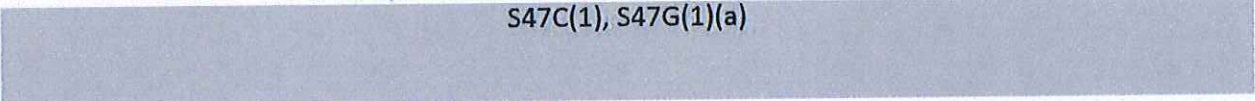
S37(2)(b), S47C(1)



Industry Consultation

20. The main telecommunications providers and industry bodies that the Department will consult with on the mandatory data retention proposal will be (but not limited to) mobile and fixed line carriers including

S47C(1), S47G(1)(a)



Consultation**Internal**

S47C(1)

External

22. As outlined, work on this proposal has been aided by an Interagency Working Group.
23. Commonwealth enforcement agencies, such as ASIO, AFP, Customs, ACCC and ASIC are strongly supportive of a mandatory data retention regime. State and territory agencies are equally supportive of the proposal.
24. PM&C Border Security and Law Enforcement Branch have been consulted S47C(1)
- S47C(1)

Sensitivities and Media Implications

25. Once public comment is made on a proposal for a mandatory data retention regime it is likely to attract considerable interest from the media and from privacy advocates. The Department will prepare relevant Question Time Briefs (QTB) and Minister's Office Briefs (MOB) prior to industry consultation.

~~IN-CONFIDENCE~~

*Carrier-Carriage Service Provider Data Retention Regime
Consultation Paper*

Version: 1.2

~~IN-CONFIDENCE~~

Page 1 of 15

~~IN CONFIDENCE~~

Table of Contents

Executive Summary.....	3
A. Data Set.....	5
1. Data necessary to identify supplementary information regarding a registered user of a service	5
2. Data necessary to trace and identify the source of a communication S37(2)(b), S37(2)(c)	5
3. Data necessary to identify the destination of a communication S37(2)(b), S37(2)(c)	6
4. Data necessary to identify the date, time and duration of a communication	6
5. Data necessary to identify the type of communication	7
6. Data necessary to identify users' communication equipment or what purports to be their equipment.....	7
7. Data necessary to identify the location of communication equipment.....	7
B. Data Set Explanatory Statements	8
1. Intent of Data Set Requirements	8
2. Definitions.....	12
3. Illustrative Data	14

~~IN CONFIDENCE~~

~~IN CONFIDENCE~~

Executive Summary

What is telecommunications data?

Telecommunications data 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).

Access to telecommunications data for law enforcement purposes is regulated by Chapter 4 of the *Telecommunications (Interception and Access) Act 1979*, which 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 also contains separate provisions enabling access for national security purposes.

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.

How important is telecommunications data?

The data provides agencies with an irrefutable method of tracing all communications from end-to-end, and in retrospect. It can be used to reveal associations between members of criminal organisations, as well as provide expansive intelligence on the social networks of criminal and terrorist organisations.

This data is also extremely useful in relation to counter-terrorism, given the requirement for sophisticated planning in relation to terrorist activity. Data interrogation can reveal the daily habits of targets to enable targeted surveillance. Another benefit of telecommunications data is that it can be analysed after the fact to enable the development of detailed intelligence briefs.

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.

In some situations, telecommunications type of data can be of equal or even greater benefit than the content of communications. Whereas people can communicate in different languages, or using code or other pre-approved systems which cannot be understood by agencies, traffic data is system-generated and cannot be altered by the communicator.

The existence of this information becomes even more vital as the use of new technologies, such as Voice over Internet Protocol (VoIP) and encryption, increases among agency targets. While these new technologies provide significant technical challenges to the interception regime, it is vital that even if agencies are unable to obtain the content of the communications, they are still able to determine how and with whom a person has been communicating.

~~IN CONFIDENCE~~

~~IN CONFIDENCE~~**Why is a mandatory data retention scheme necessary?**

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.

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.

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.

~~IN CONFIDENCE~~

~~IN-CONFIDENCE~~**A. Data Set****1. Data necessary to identify supplementary information regarding a registered user of a service****1.1. All service types:**

- a. current & historical name and address together with any associated account identifier (for example, the unique identifier used by the C/CSP to describe the customer);
- b. any service current or historical registered to the subscribers account
S37(2)(b), S37(2)(c)
- c. current & historical supplementary identification/contact information
S37(2)(b), S37(2)(c)
- d. current & historical service status
S37(2)(b), S37(2)(c)

2. Data necessary to trace and identify the source of a communication S37(2)(b), S37(2)(c)**2.1. Fixed network and mobile network telephony:**

- a. service identifier (for example, the calling telephone number, E.164, IMEI);
- b. full name of subscriber or registered user (contact name, billing name if different);
- c. address of subscriber or registered user (service and / or billing addresses at the time of service activation and any amendments since);

2.2. Internet access / Internet email / Internet telephony:

- a. customer identifier(s) allocated at the time of the communication (for example dynamic or static IP address or email address and assignment period information, username-realm identifier);
- b. customer identifier(s) and telephone number allocated to any communication entering the public telephone network (for example, Session Initiation Protocol address or screen name);
- c. full name of the subscriber or registered user to whom the customer identifier was allocated to at the time of the communication (contact name, billing name if different);
- d. address of the subscriber or registered user to whom the customer identifier was allocated to at the time of the communication (service and / or billing addresses at the time of service activation and any amendments since).

~~IN-CONFIDENCE~~

~~IN-CONFIDENCE~~

3. Data necessary to identify the destination of a communication S37(2)(b), S37(2)(c)

3.1. Fixed network and mobile network telephony:

- a. network or service numbers dialed (the telephone number(s) called);
- b. S37(2)(b), S37(2)(c)
- c. full name of subscriber or registered user (contact name, billing name if different);
- d. address of subscriber or registered user (service and / or billing addresses S37(2)(b), S37(2)(c))

3.2. Internet access / internet email / internet telephony:

- a. service identifier of the intended recipients of an Internet telephony call (for example user ID or telephone number);
- b. network identifier of the communication (for example IP address or email address, username-realm identifier);
- c. full name of subscriber or registered user (contact name, billing name if different);
- d. address of subscriber or registered user (service and / or billing addresses S37(2)(b), S37(2)(c))

4. Data necessary to identify the date, time and duration of a communication

4.1. Fixed network telephony and mobile network telephony:

- a. date and time of the start and end of the communication S37(2)(b), S37(2)(c)

4.2. Internet access / internet email / internet telephony:

- a. date and time of the log-in and log-off of the Internet access service, Internet email or internet telephony service S37(2)(b), S37(2)(c)

~~IN-CONFIDENCE~~

~~IN-CONFERENCE~~**5. Data necessary to identify the type of communication****5.1. Fixed network and mobile network telephony:**

S37(2)(b), S37(2)(c)

5.2. Internet access / Internet email / Internet telephony:

- a. Internet service used (for example ADSL, WI-FI, Dial-up, fixed, wireless or mobile);

6. Data necessary to identify users' communication equipment or what purports to be their equipment**6.1. Fixed network telephony:**

- a. calling and called telephone numbers;

6.2. Mobile network telephony:

- a. calling and called telephone numbers;
- b. IMSI of calling party;
- c. IMEI of calling party;
- d. IMSI of called party (if available);
- e. IMEI of the called party (if available);
- f. for pre-paid services — date and time of initial activation and cell ID from which the service was activated;

6.3. Internet access / Internet email / Internet telephony:

- a. calling telephone number for dial-up access;
- b. the Digital Subscriber Line (DSL) or other end point identifier of the originator of the communication S37(2)(b), S37(2)(c)
- c. in the case of cellular provided access, S37(2)(b), S37(2)(c)
- d. in the case of cellular provided access, S37(2)(b), S37(2)(c)
- e. for pre-paid services — date and time of initial activation and cell ID from which the service was activated.

7. Data necessary to identify the location of communication equipment**7.1. Mobile services (including wireless Internet services):**

- a. the location label (cell ID) at start and end of the communication S37(2)(b), S37(2)(c)

~~IN-CONFERENCE~~

~~IN CONFIDENCE~~

B. Data Set Explanatory Statements

1. Intent of Data Set Requirements

This section of the document outlines the purpose & intent of each specific retention requirement from the Data Set forming part of the *Carrier-Carriage Service Provider Data Retention Regime*. This section should be considered in conjunction with the Data Set to provide further explanation to the given Data Set requirement.

Note: Any examples given throughout this document are illustrative only. An example, or lack of, does not indicate only data pertaining to the specific exemplified scenario should be retained.

Table 1.

Requirement	Intent
1	Section one describes retention requirements for customer administration information held by the carrier or carriage service provider.
1.1.a	This requirement intends to capture both present and past subscriber name and addresses information as is known, or was ever known, to the service provider.
1.1.b	This requirement intends to capture any service, additional account or additional feature information which may be, or has been, linked to the subscriber's primary account. S37(2)(b), S37(2)(c), S47C(1)
1.1.c	S37(2)(b), S37(2)(c), S47C(1)
1.1.d	S37(2)(b), S37(2)(c), S47C(1)
2	Section two describes retention requirements relating to the origin of communications.
2.1.a	This requirement intends to capture any identifier which uniquely describes the service at the time of the successful S37(2)(b), S37(2)(c), S47C(1)
2.1.b	This requirement intends to capture the name (and subsequent related entities such as the billing name) of the subscriber in the successful S37(2)(b), S37(2)(c) In the case where the initiating party and terminating party name details are known to the provider it is intended both party's details are retained. An example of this information is the subscriber's full name and or business name.
2.1.c	This requirement intends to capture the address (and subsequent related entities such as the billing address) of the subscriber in the successful S37(2)(b), S37(2)(c) and the history of changes to this information should a change be made. In the case where the initiating party and terminating party address details are known to the provider it is intended both party's details are retained. An example of this information is the subscriber's full address and or business address.
2.2.a	This requirement intends to capture any identifier allocated which uniquely describes the service at the time of the successful communication. S37(2)(b), S37(2)(c), S47C(1)

~~IN CONFIDENCE~~

~~IN-CONFIDENCE~~

Requirement	Intent
2.2.b	This requirement intends to capture any identifiers allocated to a subscriber's communication when entering the public network. S37(2)(b), S37(2)(c), S47C(1)
2.2.c	This requirement intends to capture the name (and subsequent related entities such as the billing name) allocated at the time of the communication. In the case whereby the initiating party and terminating party name details are known to the provider it is intended both party's details are retained. This requirement is the corresponding data requirement of that outlined in 2.1.b. An example of this information is the subscriber's full name and or business name.
2.2.d	This requirement intends to capture the address (and subsequent related entities such as the billing address) allocated at the time of the communication S37(2)(b), S37(2)(c), S47C(1) In the case whereby the initiating party and terminating party address details are known to the provider it is intended both party's details are retained. This requirement is the corresponding data requirement of that outlined in 2.1.c. An example of this information is the subscriber's full address and or business address.
3	Section three describes retention requirements relating to the destination of communication.
3.1.a	This requirement intends to capture any numbers transmitted to the network to cause a communication to take place. S37(2)(b), S37(2)(c) An example of this is a telephone number or other numbers as dialled by the subscriber.
3.1.b	This requirement intends to capture the scenario in which a communication is routed to a subsequent number to that retained in 3.1.a. Examples of this is the number to which a call was forwarded, a voicemail short-dial to full number translation or a 13, 1300, 1800 prefixed number to other termination number translation.
3.1.c	S37(2)(b), S37(2)(c), S47C(1)
3.1.d	This requirement intends to capture the address (and subsequent related entities such as the billing address) allocated at the time of the communication and the history of changes should a change be made. In the case whereby the initiating party and terminating party address details are known to the provider it is intended both party's details are retained. An example of this information is the subscriber's full address and or business address.
3.2.a	This requirement intends to capture the service number, or other service identifier representative of a service number, for the intended recipient of an Internet telephony call. An example of a service identifier representative of a number is a SIP URI.
3.2.b	This requirement intends to capture the identifier allocated to the subscriber by the network for communication. An example of a network identifier is a username or IP address.
3.2.c	This requirement intends to capture the name (and subsequent related entities such as the billing name) for the party to whom the service or network identifier is allocated at the time of the communication. This requirement is the corresponding data requirement of that outlined in 3.1.c. An example of this information is The subscriber's full name and or business name.

~~IN-CONFIDENCE~~

~~IN CONFIDENCE~~

Requirement	Intent
3.2.d	This requirement intends to capture the address (and subsequent related entities such as the billing address) for party to whom the service or network identifier is allocated at the time of the communication. This requirement is the corresponding data requirement of that outlined in 3.1.d. An example of this information is the subscriber's full address and or business address.
4	Section four describes retention requirements relating to when communications occurred.
4.1.a	This requirement intends to capture the link between a communication and the time at which it occurred. S37(2)(b), S37(2)(c), S47C(1)
4.2.a	This requirement intends to capture the link between a communication and the time at which it occurred. S37(2)(b), S37(2)(c), S47C(1)
5	Section five describes retention requirements for the type of communication
5.1.a	S37(2)(b), S37(2)(c), S47C(1)
5.1.b	This requirement intends to capture the service type used in the communication. Examples of a service type are SMS, telephony, video telephony.
5.1.c	This requirement intends to capture the way in which the network is setup to facilitate the service generally, or specifically an individual communication. An example of this is line conditioning for DSL or facsimile transmission over cellular networks.
5.2.a	This requirement intends to capture the type of access service used. An example of an access service type is ADSL.
6	Section six describes retention requirements relating to the equipment used in communications
6.1.a	This requirement intends to capture both the number originating the communication and the recipient number for the communication, that is, the number of both parties in the communication. An example of this is the telephone number of the A & B party in telephone call.
6.2.a	This requirement intends to capture both the number originating the communication and the recipient number for the communication, that is, the number of both parties in the communication. An example of this is the telephone number of the A & B party in telephone call. This requirement is the corresponding mobile telephony requirement of that outlined in 6.1.a.
6.2.b	This requirement intends to capture the unique international subscriber identity of the party originating the communication.
6.2.c	This requirement intends to capture the unique hardware identifier of the device used to originate the communication.
6.2.d	This requirement intends to capture the unique international subscriber identity of the party receiving the communication. This requirement is dependant on this information being provided to the service provider of the communications originator.
6.2.e	This requirement intends to capture the unique hardware identifier of the device used by the party receiving the communication. This requirement is dependant on this information being provided to the service provider of the communications originator.
6.2.f	This requirement intends to capture the date & time referenced to a time zone of the subscriber's service activation together with a geographic indicator. S37(2)(b), S37(2)(c), S47C(1)

~~IN CONFIDENCE~~

Requirement	
6.3.a	This rec connec connec
6.3.b	This rec point o
6.3.c	
6.3.d	
6.3.e	This rec subscri
7	Section equipm
7.1.a	This rec possibl

~~IN-CONFIDENCE~~

2. Definitions

This section of the document provides definitions for the purpose of this data set of any key or ambiguous terms used.

Table 2.

Term	Definition
ADSL	Asynchronous Digital Subscriber Line.
BRAS	Broadband Remote Access Server. The BRAS terminates sessions from an access network aggregating them into a core network and can provide unique identifiers such as IP address to subscribers.
C/CSP	Carrier / Carriage Service Provider. The definition of C/CSP used in this document is the definition in the <i>Telecommunications Act</i> .
	S37(2)(b), S37(2)(c), S47C(1)
	S37(2)(b), S37(2)(c), S47C(1)
Dial-Up	This term is taken to mean a connection to a network made using a modem via the PSTN.
DSL	Digital Subscriber Line.
E.164	E.164 is the ITU recommendation entitled <i>the International Public Telecommunication Numbering Plan</i> . This recommendation is taken to be the international standard for telephone numbering.
Fixed Telephony	This term is taken to mean telephony using devices physically connected to a network.
FNN	Full National Number.
HSPA	High Speed Packet Access. This is a mobile network data communications technology.
IMEI	International Mobile Equipment Identity. An IMEI is a unique 15 or 17 digit code used to identify the hardware accessing a mobile network.
IMSI	International Mobile Subscriber Identity. An IMSI is a unique 15 digit number stored on the SIM card made up of the Mobile Country Code, the Mobile Network Code and the Mobile Subscriber Identity Number.
Internet Access	This term is taken to mean access (or a connection) to a publicly accessible network.
Internet Email	This term is taken to mean email sent or received via a publicly accessible network.
Internet Telephony	This term is taken to mean phone calls placed utilising data communications technology.
IP	Internet Protocol.
MAC	Media Access Control.
PSTN	Public Switched Telephone Network.
Short-Dial	This term is taken to mean the process whereby a pre-allocated number is translated by the network into a full E.164 compliant number.
SIP-URI	Session Initiation Protocol Uniform Resource Identifier. The SIP is specified by RFC 3261.
SMS	Short Message Service.
	S37(2)(b), S37(2)(c), S47C(1)
	S37(2)(b), S37(2)(c), S47C(1)

~~IN-CONFIDENCE~~

~~IN CONFIDENCE~~

Term	Definition
UTC	Universal Time, Coordinated.
Video Telephony	This term is taken to mean telephony utilizing images accompanying audible communications.
VoIP	Voice over Internet Protocol.
VPN	Virtual Private Network.
Wi-Fi	This term is taken to generically mean Wireless LANs (WLAN).

DRAFT

~~IN CONFIDENCE~~

~~IN CONFIDENCE~~


3. Illustrative Data

This section provides sample data to further illustrate the expected type of data to be retained for each specific retention requirement from the Data Set. This illustrative data should be considered in conjunction with the Data Set and Intent statements to provide further explanation to the given Data Set requirement.

Note: Illustrative data given throughout this document does not indicate the expected data format rather only provides an indication as to the type of data the requirement is intending to capture. Illustrative data, or lack of, does not indicate only data similar that provided must be retained.

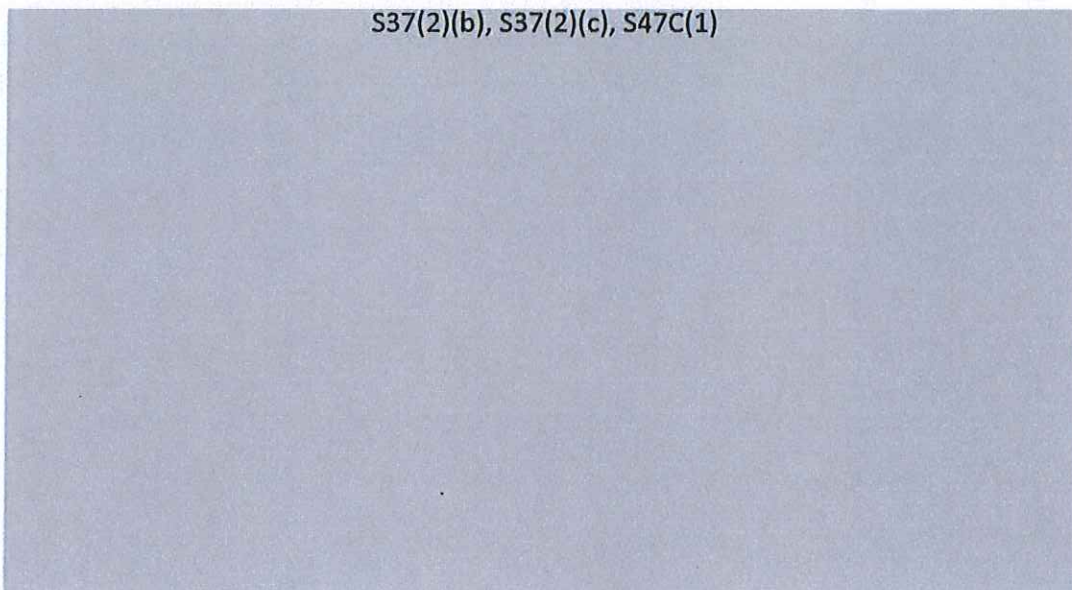
Table 3.

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

~~IN CONFIDENCE~~

~~IN-CONFIDENCE~~

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

~~IN-CONFIDENCE~~

Page 15 of 15



ATTORNEY-GENERAL
THE HON ROBERT McCLELLAND MP

08/1219

The Hon Kevin Rudd MP
Prime Minister
Parliament House
CANBERRA ACT 2600

Dear Prime Minister

I am writing to seek your approval to consult with the telecommunications industry on a proposal that my Department is working on to create a mandatory data retention regime, under the *Telecommunications (Interception and Access) Act 1979* (the TIA Act).

The possible regulatory impact on industry means that their support will be critical for its success. My Department is now in a position where it can consult with industry participants on a draft regulatory model.

Mandatory data retention has been highlighted in the S47C(1) as a potential mechanism to combat serious and organised crime in a global telecommunications environment.

A consultation paper which will be distributed to industry partners is at **Attachment A**.

The action officer for this matter in my Department is S47F(1) who can be contacted on S47F(1)

Yours sincerely

A handwritten signature in blue ink, appearing to read 'Robert McClelland', written over a light blue horizontal line.

Robert McClelland



ATTORNEY-GENERAL
THE HON ROBERT McCLELLAND MP

08/12/19

Senator the Hon Stephen Conroy
Minister for Broadband, Communications and the Digital Economy
Parliament House
CANBERRA ACT 2600

Dear Minister

I am writing to update you on developments in relation to the proposed mandatory data retention regime in Australia.

As chair of the Interagency Working Group on data retention, with assistance from members including representatives of your Department, my Department has completed work on a draft data set, options for storage models and a proposed period of retention of two years.

I have written to the Prime Minister (copy attached), asking for his approval to begin consultation on the draft proposals with telecommunications industry participants. I will keep you informed as to the progress and outcomes of these consultations.

I would like to thank Officers from your Department for their assistance in this project.

The action officer for this matter in my Department is S47F(1), who can be contacted on S47F(1).

Yours sincerely

A handwritten signature in blue ink, appearing to read 'Robert McClelland'.

Robert McClelland



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.

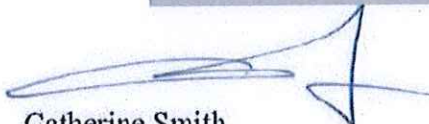
Recommendation

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)

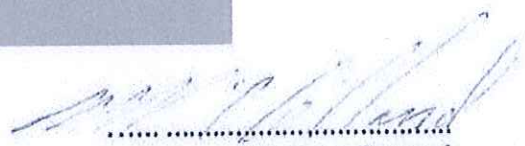
25 March 2008

Action officer:

S47F(1)

Principal Legal Officer

Telephone: S47F(1)


 Attorney-General

19/4/2008

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.

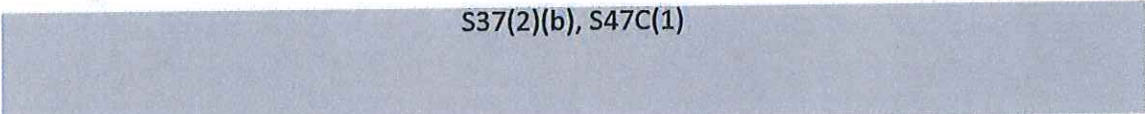
What are the likely costs?

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

Collection

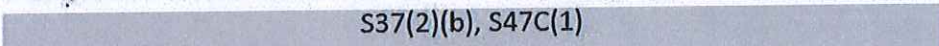
S37(2)(b), S47C(1)

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

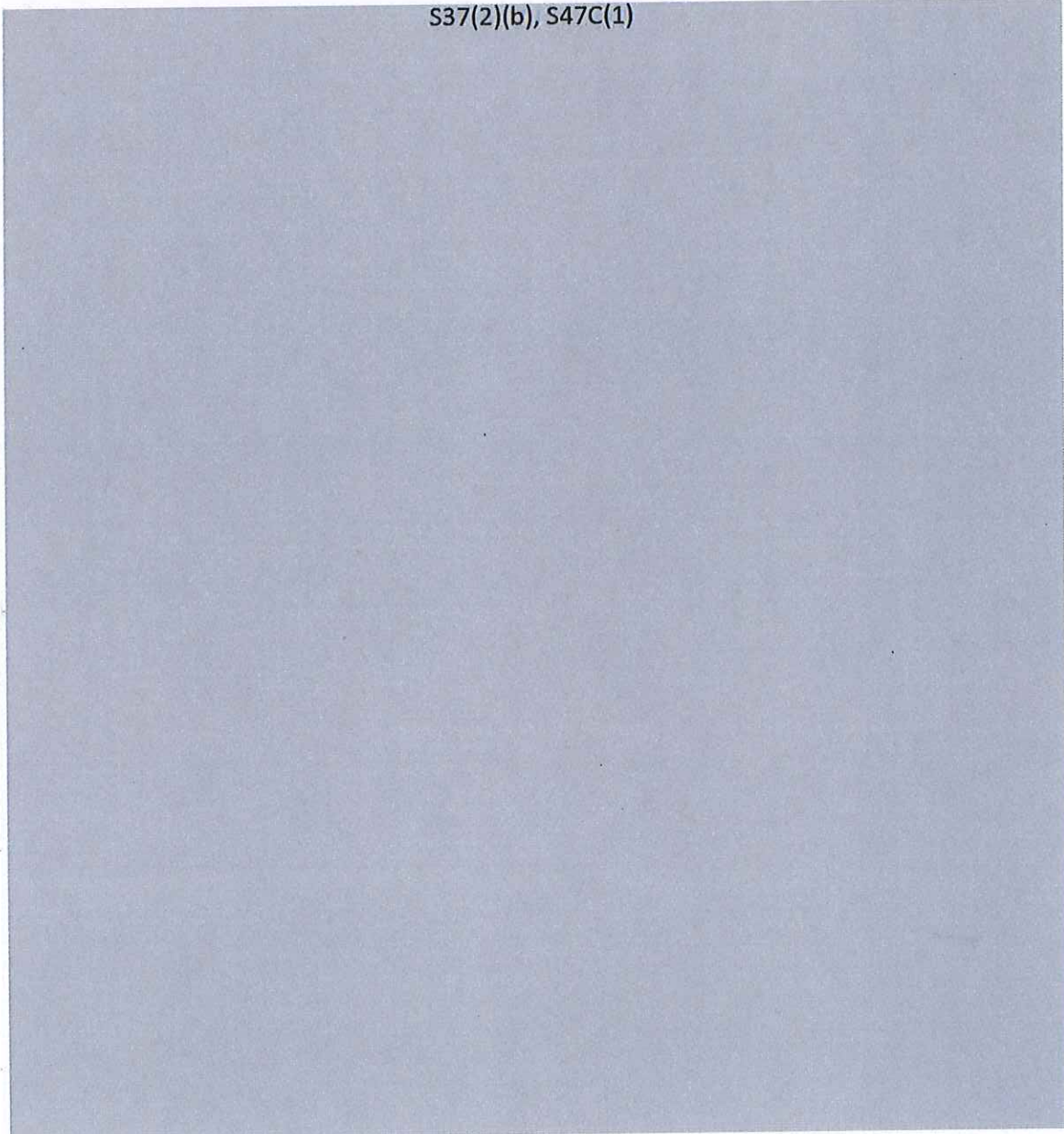
A rectangular grey box redacting a line of text.

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)

A rectangular grey box redacting a line of text.

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

A large rectangular grey box redacting the majority of the page content.

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.

Sub No:
File No: 09/19662

ATTORNEY-GENERAL

The mandatory retention of telecommunications data by carriers and carriage service providers

Deadline: None

Key Issues: You have previously approved consultation with industry on a proposed mandatory data retention regime (SB09/1922 refers) [redacted] S34(3), S47C(1)

[redacted] Industry has been consulted on a model agreed to by an Interagency Working Group (IWG). [redacted] S34(3), S47C(1)

AGD Analysis: [redacted] S47C(1)

Financial Implications: [redacted] S47C(1)

Recommendation: I recommend that you:

- (i) agree to [redacted] S34(3), S47C(1)

Agreed / Not Agreed / Discuss

- (ii) agree to further consultation with Commonwealth and State agencies, Office of the Privacy Commissioner and targeted representatives of the Telecommunications Industry.

Agreed / Not Agreed / Discuss

Catherine Smith
Assistant Secretary, Telecommunications and
Surveillance Law Branch

S47F(1)

17 / 12 / 2009

.....
Attorney-General

/ / 2009

Cleared by:

Geoff McDonald

17 / 12 / 2009

Miles Jordana

18 / 12 / 2009

Roger Wilkins AO

/ 2009

Action Officer:

S47F(1)

Background

2. [REDACTED] S37(2)(b), S47C(1)

3. You have previously approved the development of a draft mandatory data retention proposal (SB08/1112 refers), consultation with government agencies on the draft proposal (SB08/2504 refers) and subsequent consultation with industry and the Office of the Privacy Commissioner. [REDACTED] S47C(1)

[REDACTED] (SB09/1922 refers).

[REDACTED] S47C(1), S47G(1)(a)

[REDACTED] S47C(1)

S47C(1)

