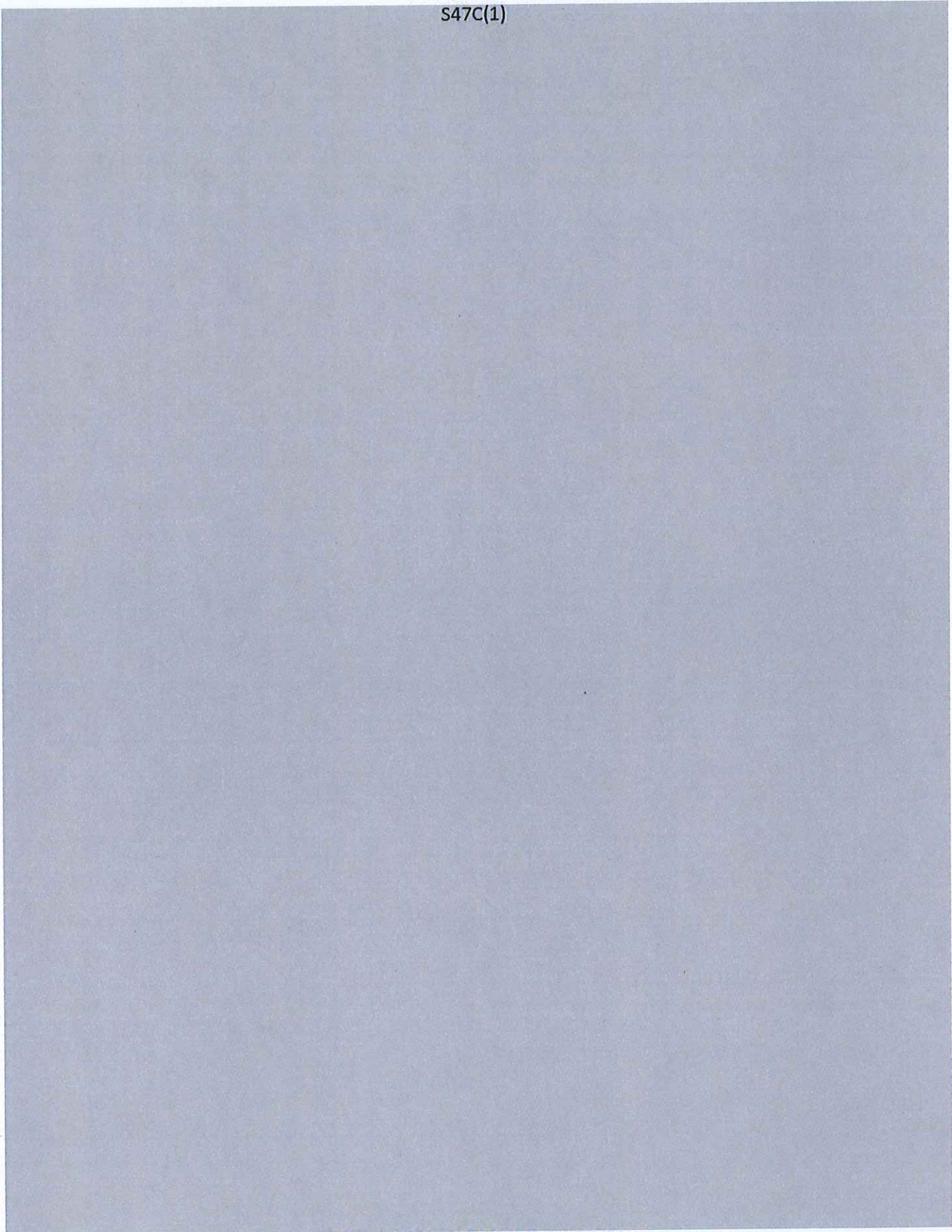


S47C(1)



S47C(1)

Consultation

Internal

21. S47C(1)

External

22. As outlined, work on this proposal has been aided by an Interagency Working Group. 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. PM&C Border Security and Law Enforcement Branch have been consulted S47C(1)

23. The Department of Broadband, Communications and the Digital Economy have been heavily consulted and involved in the development of this proposal. You have previously written to the Minister for Broadband, Communications and the Digital Economy about this proposal and he gave broad principled support to the proposal.

24. S47C(1)

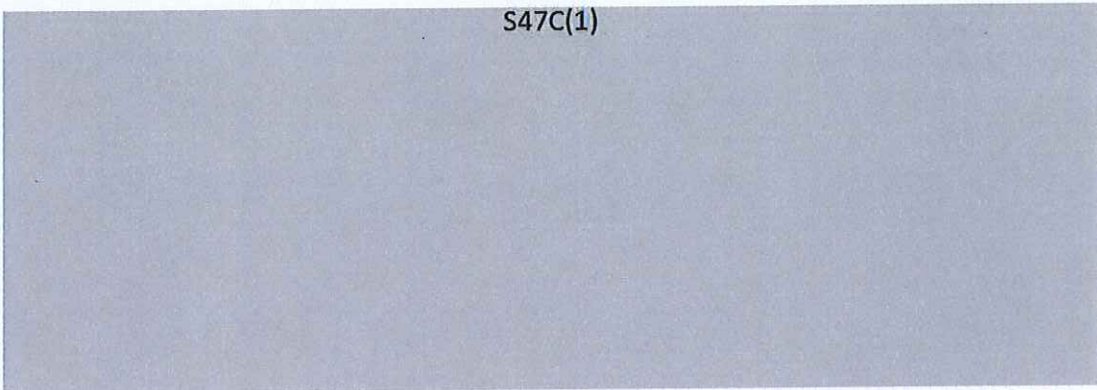
25. S47C(1)

Sensitivities and Media Implications

26. S47C(1)

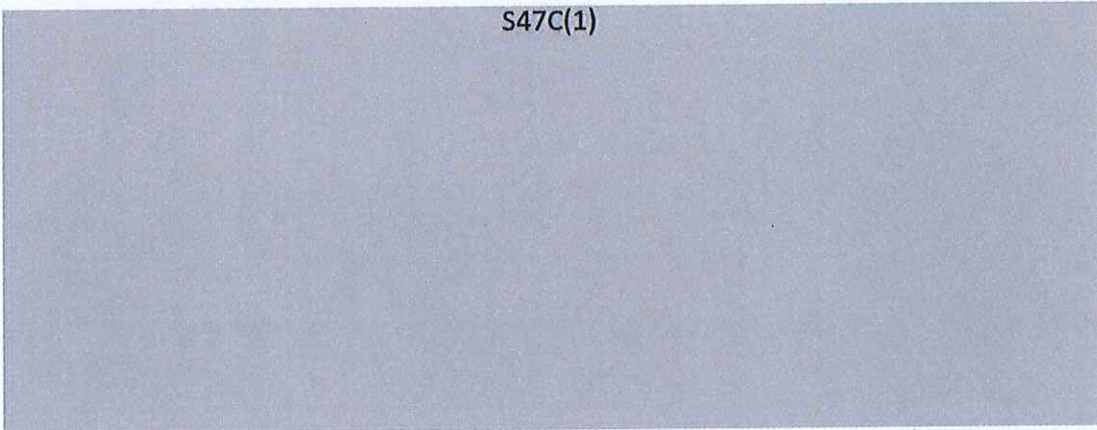
ATTACHMENT A

S47C(1)

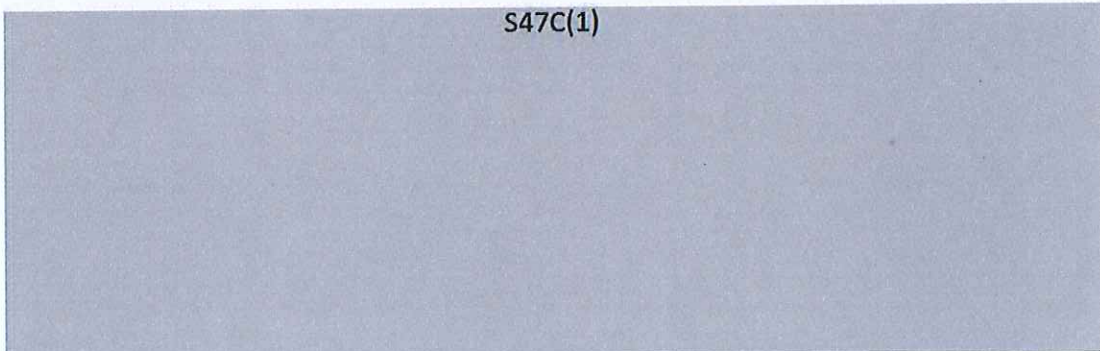


Article 6 of the EU Data Retention Directive requires EU Member States to retain categories of data specified in Article 5 for periods of not less than six months and not more than two years from the date of the communication.

S47C(1)






S47C(1)



Article 4 of the EU Data Directive requires Member States to adopt measures to ensure that stored data is provided only to the competent national authorities in specific cases and in accordance with national law.

S47C(1)

S47C(1)



Article 13.2 states that any access that is not permitted under national law is to be subject to penalties.

Chapter 4 of the TIA Act outlines the position for access to telecommunications data in Australia.

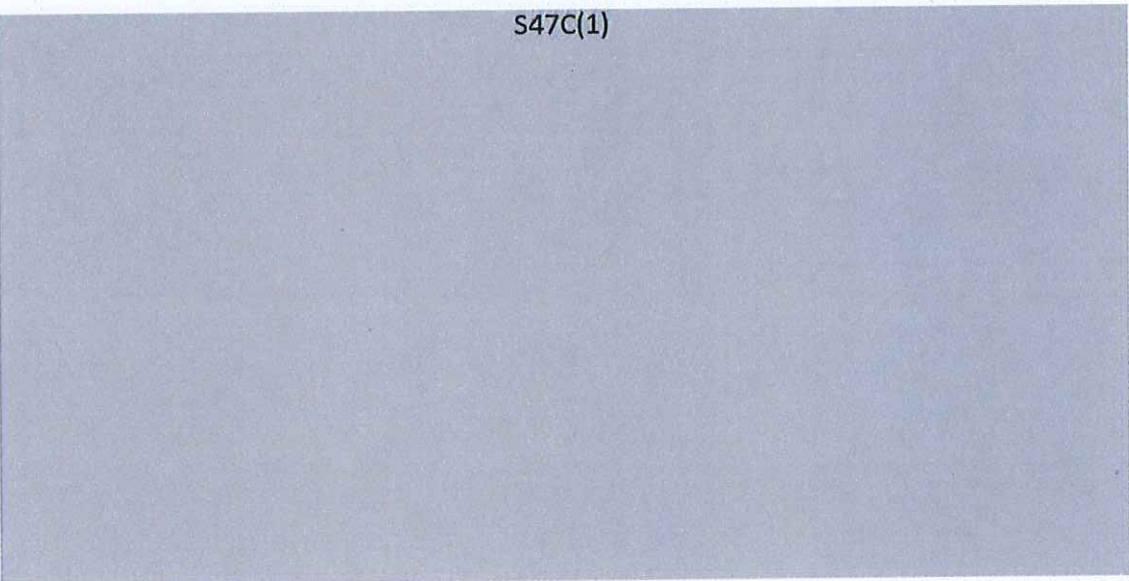
S47C(1)



Section 174 allows for the voluntary disclosure of telecommunications data to ASIO if the disclosure is in connection with the performance by the Organisation of its functions, and section 175-176 enables disclosure to ASIO subject to an authorisation. An authorisation to provide information to ASIO can only be provided if the disclosure would be in connection with the performance by ASIO of one of its functions. Authorisations are made by either the Director-General of Security, Deputy Director-General of Security or an officer or employee of the Organisation covered by an approval in force under section 175(4).

Section 177 enables disclosure of telecommunications data to enforcement agencies if the disclosure is reasonably necessary for the enforcement of criminal law or of a law imposing a pecuniary penalty or for the protection of the public revenue. Section 178-180 enables disclosure to enforcement agencies subject to an authorisation. Authorisations to enable enforcement agencies access to existing information or documents can only be provided if the disclosure is reasonably necessary for the enforcement of criminal law or of a law imposing a pecuniary penalty or for the protection of the public revenue (sections 178-179). Authorisations are made by an authorised officer of an enforcement agency.

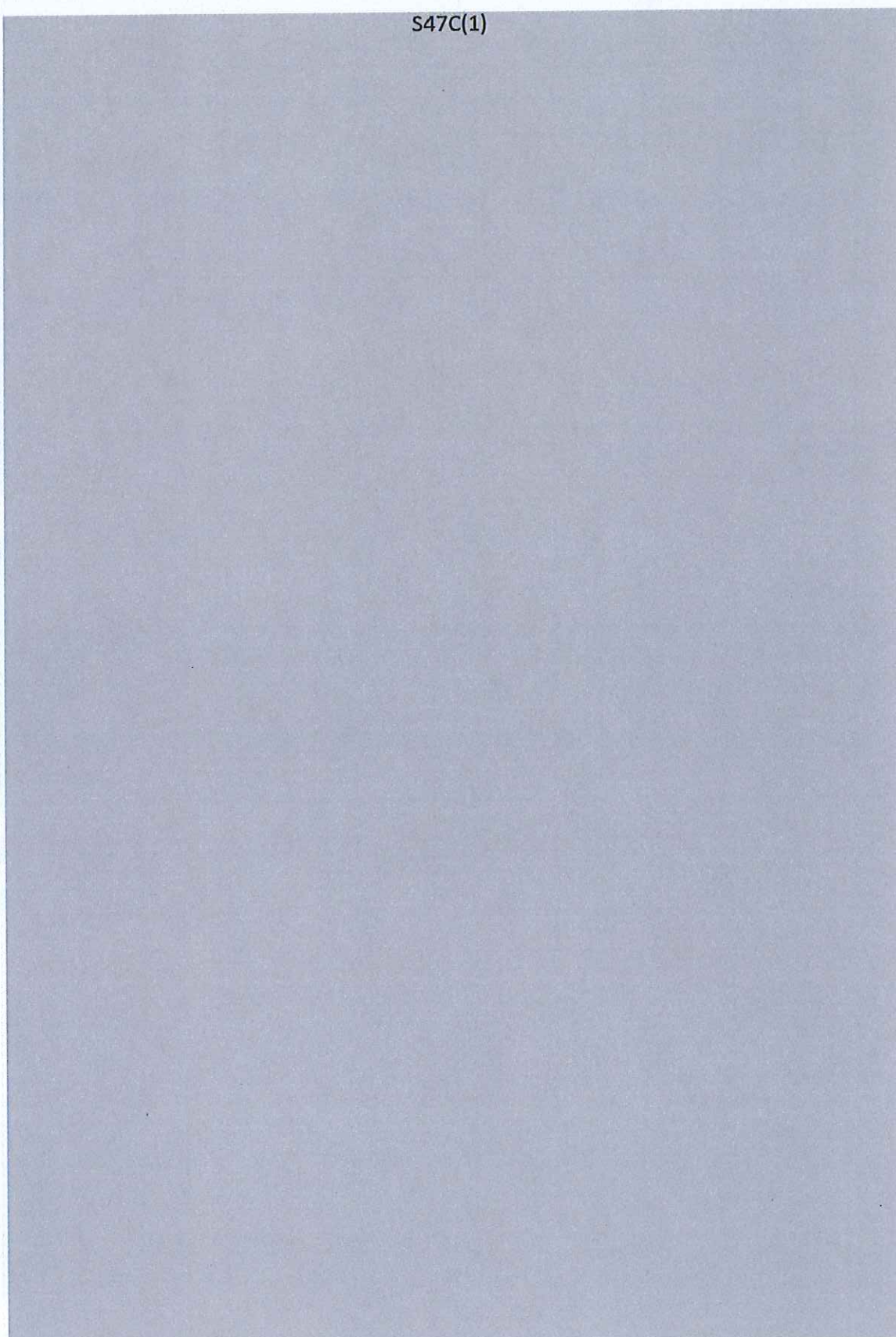
S47C(1)



S47C(1)



S47C(1)



S47C(1)

The use and disclosure principle

National Privacy Principle 2 prevents the use and disclosure of personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection (with some exceptions).

S47C(1)

The data security principle

S47C(1)

National Privacy Principle 4.1 and 4.2. Those principles state:

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.

S47C(1)

S47C(1)

EU Data Retention Regime

S47C(1)

This language comes from Article 15(1) of the EU Privacy Directive in Electronic Communications (2002/58/EC) which allowed Member States to adopt legislative measures to restrict the scope of the rights and obligations provided for in that Directive when such restriction constituted “a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system”.

S47C(1)

Article 15(1) of the Privacy Directive, and accordingly the discretion for Member States to establish their own data retention regimes, was repealed by Article 11 of the EU Data Directive (2006/24/EC).

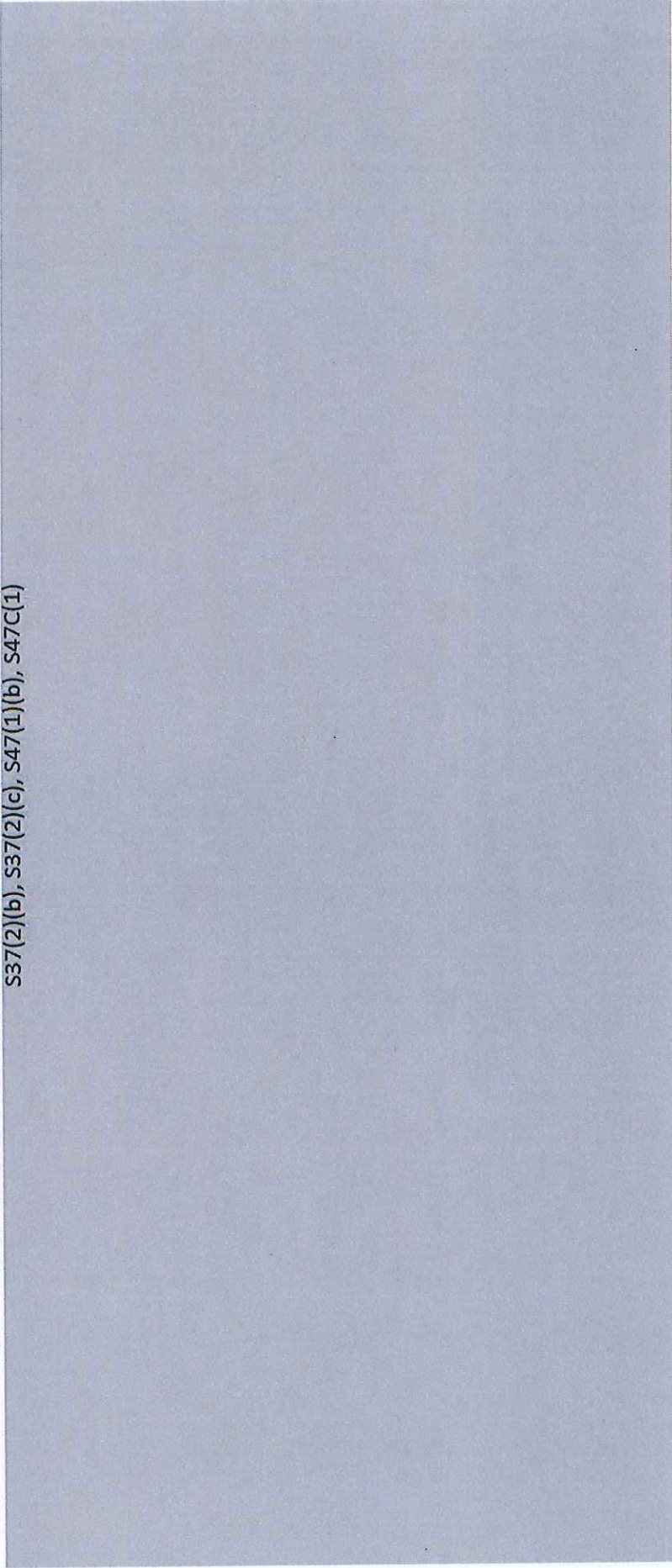
S47C(1)

~~COMMERCIAL - IN - CONFIDENCE~~

ATTACHMENT A

AGD Preliminary Analysis of Industry Response to "Data Retention Consultation Paper"

S37(2)(b), S37(2)(c), S47(1)(b), S47C(1)



~~COMMERCIAL IN CONFIDENCE~~

ATTACHMENT A

S37(2)(b), S37(2)(c), S47(1)(b), S47C(1)



~~COMMERCIAL IN CONFIDENCE~~
RELEASED UNDER THE FOIA ACT 1982 BY THE ATTORNEY-GENERAL'S DEPARTMENT

~~COMMERCIAL IN CONFIDENCE~~

ATTACHMENT A

S47(1)(b), S47C(1)



~~COMMERCIAL IN CONFIDENCE~~

ATTACHMENT A

S47(1)(b), S47C(1)



~~COMMERCIAL - IN - CONFIDENCE~~

ATTACHMENT A

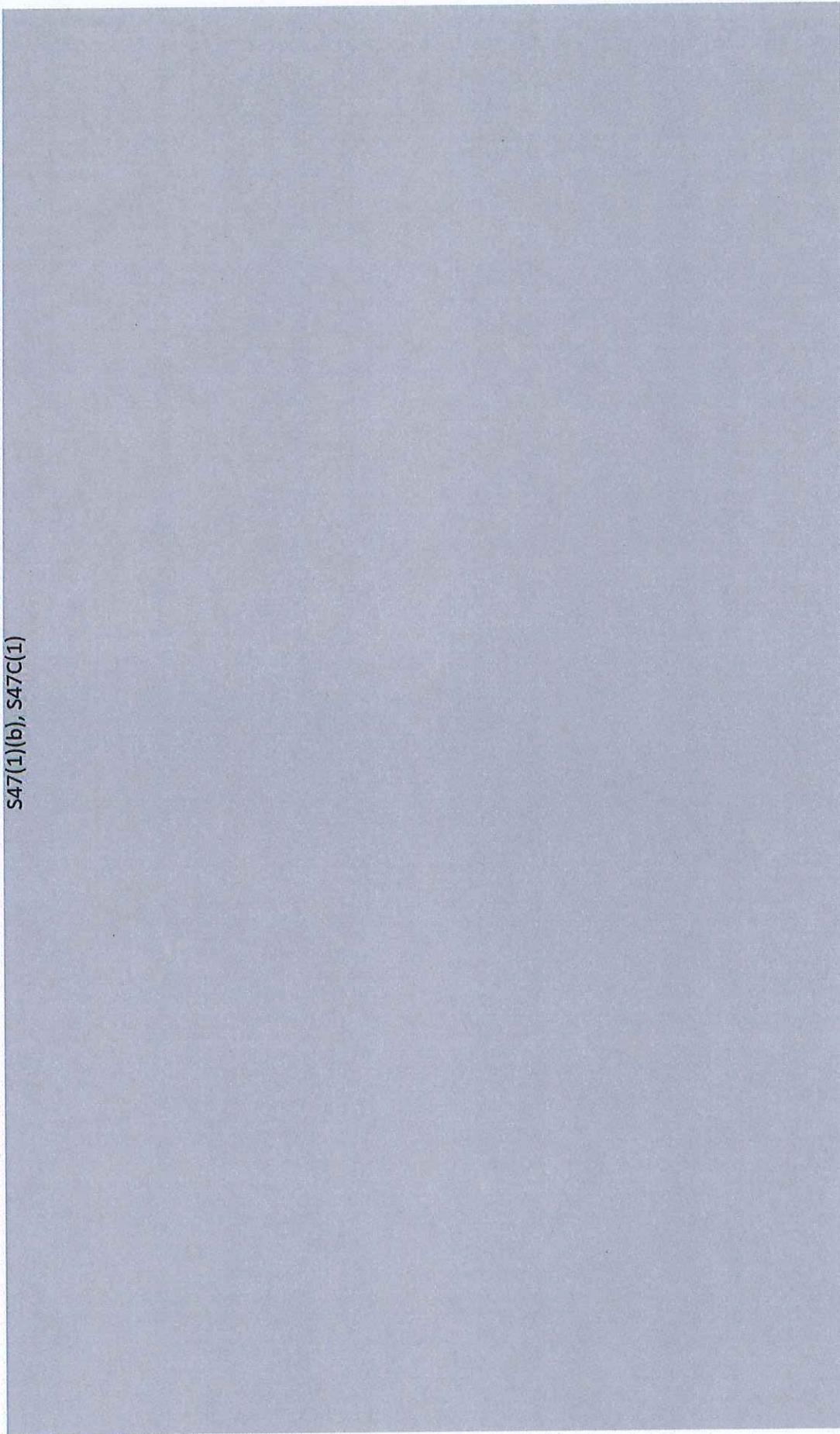
S47(1)(b), S47C(1)



~~COMMERCIAL - IN - CONFIDENCE~~

ATTACHMENT A

S47(1)(b), S47C(1)



~~COMMERCIAL - IN - CONFIDENCE~~
RELEASED UNDER THE FOIA ACT 1982 BY THE ATTORNEY-GENERAL'S DEPARTMENT

Sub No:
File No: 10/1516-04

ATTORNEY-GENERAL

Proposal for a mandatory data retention regime in Australia

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

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

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

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

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

Approved / Not Approved / Discuss

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

.....
Attorney-General

Ret 5 / 2010

/ / 2010

Cleared by:

.....
Geoff McDonald
28 / 5 / 2010

.....
Roger Wilkins AO
/ / 2010

Background

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

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

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

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

[Redacted]

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

7. S34(3), S47C(1)
[Redacted]

8. S34(3), S47C(1)
[Redacted]

9. S34(3), S47C(1)
[Redacted]

10. S34(3), S47C(1)
[Redacted]

S34(3), S47C(1)

11. S34(3), S47C(1)

12. S34(3), S47C(1)

Consultation

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

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

15. S34(3), S47C(1)

Sensitivities and Media Implications

16. S47C(1)

17.

S47C(1)

[REDACTED]

[REDACTED]

[REDACTED]



Sub No:
File No: 10/1516

COPY

ATTORNEY-GENERAL

Data Retention Proposal

Deadline: 27 October 2010 to ensure a decision regarding the development of a mandatory data retention regime is made prior to the hearing of the Senate Inquiry into the adequacy of protections for the privacy of Australian's online scheduled to be held on 29 October 2010.

Key Issues: Mandatory data retention in Australia is a contentious proposal. This has been demonstrated by public responses to the recent media interest and the submissions addressing data retention as part of the Senate Inquiry into the adequacy of protections for the privacy of Australian's online. However, the development of a data retention proposal remains crucial to ensure that public expectations about the capacity of security and law enforcement agencies to solve crime and to protect national security continue to be met.

AGD Analysis: Mandatory retention of telecommunications data is necessary to ensure that data which is of significant assistance in intelligence operations and law enforcement investigations continues to be available in nationally consistent and systematic way. Your approval is sought to continue developing this proposal and continue targeted consultations with industry and privacy organisations to inform the development of a discussion paper for public consultation. Adopting an open and transparent consultative approach will assist in ensuring that any public discussion around data retention is properly informed. Prior to the release of the discussion paper the Department will develop a media strategy to support the public consultations.

Financial Implications: It is expected that there will be financial implications for telecommunications industry participants and to a lesser extent government agencies which will be canvassed in the discussion paper.

Recommendation: I recommend that you:

- (i) Agree to the Department continuing to develop the mandatory data retention regime proposal,

Approved / Not Approved / Discuss

- (ii) Approve targeted consultation with industry and privacy organisations to inform the development of the discussion paper, and

Approved / Not Approved / Discuss

- (iii) Agree to the development of a data retention discussion paper in consultation with the Minister for Broadband, Communications and the Digital Economy and the Prime Minister for public consultation.

Approved / Not Approved / Discuss

Catherine Smith
Assistant Secretary, Telecommunications and
Surveillance Law Branch

.....
Attorney-General

S47F(1)
13/ 10/ 2010

/ / 2010

Cleared by:

Geoff McDonald
13 / 10 / 2010

Action Officer: S47F(1)

~~CABINET IN CONFIDENCE~~**Background**

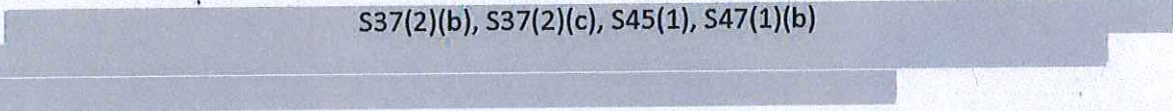
1. Telecommunications data is information about the process of a communication, as distinct from its content. It includes information about the identity of the sending and receiving parties and related subscriber details, account identifying information collected by the carrier/carriage service providers (C/CSPs) to establish the account, and information such as the time and date of the communication, its duration, location and type of communication.
2. Restrictions around access and the use of data reflect the *Telecommunications (Interception and Access) Act 1979* (the Act) focus on protecting the freedom to communicate and the privacy of parties communicating while allowing regulated access for security and law enforcement agencies where appropriate. Balancing these competing needs is a key role for Government as public concern about the use of telecommunications data crystallises around privacy issues.
3. The ability to lawfully access telecommunications data held by C/CSPs is a vital tool for agencies to investigate and solve crime and to protect national security. Access to telecommunications data incurs minimal costs, there are no operational risks and it raises fewer privacy concerns than other covert investigative methods. Additionally, telecommunications data is accessed by a range of investigative agencies (such as the Australian Securities and Investments Commission, Australian Customs and Border Protection Service, Australian Taxation Office, Australian Competition and Consumer Commission and Centrelink) that do not have access to interception powers. Telecommunications data assists these agencies to ensure the integrity of financial markets, Australia's borders, and the protection of the public revenue. Telecommunications data can provide:
 - evidence of connections and relationships within larger associations over time,
 - evidence of a targets movements and habits without the need for physical surveillance,
 - a snap-shot of events immediately preceding a crime,
 - evidence needed to obtain warrants for the use of more intrusive investigative techniques, including telecommunications interception or surveillance devices, and
 - evidence to provide alibis.
4. Crime continues to occur and targets of interest, now more than ever, are utilising the wide range of telecommunications services available to them to communicate, coordinate, manage and commit serious crimes. S37(2)(b), S37(2)(c)
[REDACTED]

Indeed Industry have acknowledged that the value of telecommunications data, depending on the circumstances, can be as important, or more important, than the content.
5. However, despite the increasing reliance on telecommunications data, industry have confirmed that there will be changes (reductions) in the type of data that is created and retained into the future and indicate that this is a natural evolution as a result of advances in technology and business models. Currently, upon receipt of a valid authorisation for access to telecommunications data the C/CSP will provide what they retain, this varies depending upon the C/CSP. While C/CSPs keep relevant data for business purposes such as taxation and billing (for up to seven years) there is no uniformity about what data is kept and the length of time the data it retained. Industry associations have confirmed that differing competitive needs produce differing retention requirements.

~~CABINET IN CONFIDENCE~~

~~CABINET-IN-CONFIDENCE~~

6. Anecdotal reporting from agencies is that increasingly requests for data are not being met as carriers do not retain the particular data requested. Unfulfilled requests waste agency resources, inhibit the making of requests, and can lead to investigations being stalled or abandoned with crimes going unsolved. Commonwealth intervention is required to ensure a national and systematic approach is taken for data retention for law enforcement and national security purposes.

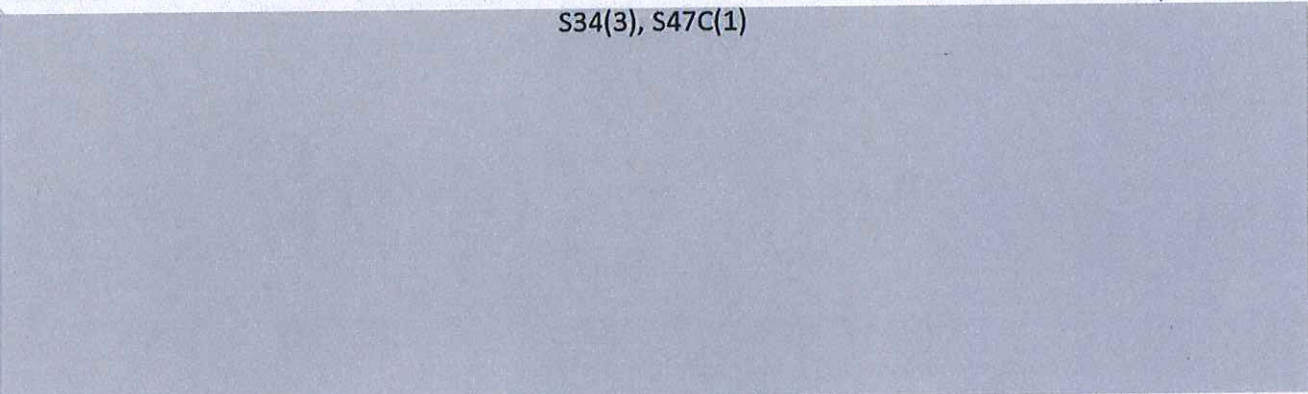
7.  S37(2)(b), S37(2)(c), S45(1), S47(1)(b)

8. The case studies at **Attachment A** are a sample of specific instances which demonstrate the usefulness of telecommunications data.

9. The advantage of mandating data retention is that it will retain current industry practices into the future while minimising costs. That is, introducing comprehensive data retention in the future when significant elements of the data set are no longer collected would be prohibitively expensive as it would necessitate the redesigning of infrastructure.

Status of the development of a mandatory data retention proposal

S34(3), S47C(1)



FOI and Media Attention

12. The Department has been consulting with Industry and the Office of the Privacy Commissioner on the proposed elements of a mandatory data retention regime since August 2009. At which time advice was requested on the proposal and the expected financial impact. Further meetings were held in March 2010 with a wider industry audience to inform the development of the proposal.

13. In June 2010, consultation documentation which was provided in these meetings was leaked to the media and reported in articles in the Sydney Morning Herald on 12 June 2010 and 17 June 2010. On 15 June 2010 a Freedom of Information (FOI) request was made for documents handed to the telecommunications industry at a briefing in March 2010.

14. The majority of information requested under the FOI requests was not released as it was created for the purposes of the deliberative processes of the Department and the Government. As the matters were not settled, the release of the information may have caused unnecessary concern and disclosure of the methods and procedures used by law enforcement agencies for investigating breaches of the law. A follow-up article regarding the outcomes of the FOI request was published on 23 July 2010.

~~CABINET-IN-CONFIDENCE~~

~~CABINET-IN-CONFIDENCE~~*Senate Inquiry*

15. On 24 June 2010 the Senate referred the issue of the adequacy of protections for the privacy of Australians online to the Senate Standing Committee on Environment, Communications and the Arts for inquiry. Senator Ludlam said 'the inquiry should also look at possible government plans to introduce European style laws compelling ISPs to keep records of the websites visited by their customers for the benefit of law enforcement agencies'. Media articles have indicated that Senator Ludlam will be seeking the censored documents, and all related documentation to be released publicly in an uncensored form as part of the Senate Inquiry.

16. Data retention is not specifically mentioned in the Inquiry Terms of Reference and whilst the majority of the submissions have not focused on data retention (it has been mentioned in nine of the 18 submissions received to date), the joint submission from the Australian Mobile Telecommunications Association, Communications Alliance and the Internet Industry Association focuses exclusively on data retention and is not supportive of the proposal providing an alternative option of 'data preservation'. Data preservation is where carriers and carriage service providers preserve existing records in its possession pending the issue of an authorisation or warrant for access to the data. It is intended to prevent data from being deleted after it has been identified as required but before the legal instrument for access is prepared. Whilst this option has some merit it would not address all of the issues identified as the data may have been deleted before it has been identified as being of relevance.

17. Submissions closed on 30 September and the Inquiry has a reporting date of 17 November 2010. Advice from the Committee Secretariat is that a hearing will be held on 29 October 2010 in Canberra. The Department will attend the hearing and provide evidence.

18. This issue has attracted considerable online media interest and is likely to gain further attention as a result of the Senate Inquiry.

Proposed Strategy

19. If you agree to the continued development of the data retention regime proposal, the Department recommends a more open, transparent and consultative approach to be undertaken to acknowledge the public interest in the proposal. The concept of a data retention regime has already been made public via the media and this approach will ensure that any public discussion is properly informed.

20. To support this process the Department recommends the development of a public discussion paper which would include options for retention of telecommunications data based on a consideration of proportionality. The discussion paper would clearly explain:

- the context within which the requirement for data retention arises
- the privacy implications
- the financial implications
- the draft data sets, and
- the benefits to the safety and security of Australians.

21. It is the Departments intention that the draft data sets be included in the discussion paper in such a way as to not disclose investigative methodologies. The draft data sets will clearly reaffirm that the data retention proposal would not require internet service providers to retain the contents of internet sessions or destination Internet Protocol addresses.

~~CABINET-IN-CONFIDENCE~~

CABINET-IN-CONFIDENCE

22. The Department recommends that the discussion paper be released for public consultation in consultation with the Minister for Broadband, Communications and the Digital Economy and the Prime Minister. S47C(1)

23. In parallel, and to inform the development of the discussion paper, the Department seeks your agreement to undertake targeted consultation with targeted industry and privacy organisations. Given the previous media interest in a data retention regime proposal, and in undertaking this consultation, the Department aims to engage with these organisations acknowledging that privacy and telecommunications issues are widely discussed publicly.

Sensitivities and Media Implications

24. The concept of a data retention regime attracted significant media interest when it became publicly known in June 2010. Combined with the upcoming Senate Inquiry hearing and report it is likely that the data retention proposal will continue to attract media interest.

25. Additionally, a report evaluating the application of the European Union Data Retention Directive and its impact is due for release late 2010. This report will inform the review of the Directive that the EU Commission has announced for the fourth quarter of 2011. If the report is critical of the impact of the Directive it will likely impact on the development of a data retention proposal in Australia.

26. There is the possibility that any consultation documentation may become public and it is crucial that the consultations and consultation documentation is clear and unambiguous – particularly the draft data sets.

27. Targeted media engagement is not recommended at this stage however the Department will develop a media strategy to support the release of the discussion paper.

~~CABINET-IN-CONFIDENCE~~

~~CABINET IN CONFIDENCE~~

ATTACHMENT A

Case Study 1 – Stroke Force Picadilly II

In the course of an investigation by New South Wales Police into attacks on automatic teller machines an authorisation [REDACTED] S37(2)(b) [REDACTED]

It took approximately three months for the data to be received.

[REDACTED] S37(2)(b) [REDACTED]

Further analysis identified the user of one of the mobile phone numbers. Whilst intelligence indicated that the group changed mobile phone numbers frequently the investigations progressed and enabled identification of other offenders. This identification through the telecommunications data formed the basis of the warrant application for interception which was granted.

Further in the investigation it was decided to ask for [REDACTED] S37(2)(b) [REDACTED] for one of the other attacks (Ruse ATM) to provide further evidence of the suspects involvement in the offence. Due to the period of time which had elapsed (approximately seven months) it was not possible to obtain the data required to complete the analysis. All opportunities to build further evidence on this group for the Ruse ATM Gas Attack were lost although two men were arrested and charged with the other attacks.

Case Study 2 – Purana Taskforce

In the above example, the period from the offences and the arrest was nine months. However, often a significant time period has elapsed between the offence and the investigation. The Purana Taskforce in Victoria was tasked to investigate a number of unsolved homicides dating back to 1998, and pro-actively target the criminal activities of persons involved in the upper echelon of established criminal networks in Victoria. Each of the unsolved homicides was investigated in light of information now known to investigators, telecommunications data (call charge records) were requested in an attempt to identify contact between persons who had become persons of interest (but were not known to police at the time of the offences), or to corroborate various investigative theories and occasionally to provide exculpatory evidence or eliminate suspects from an inquiry.

During an unsolved investigation into murder committed in 2002, call charge records collected in 2007 and 2008 were important in supporting the prosecution's circumstantial case. This material enabled investigators to allege approximate locations of persons central to the investigation at the time the murder was committed, and to make crucial inferences where contact between two 'covert' phones used by the suspects occurred (a 'covert' phone is one which has not obvious relationships to the suspect, such as a pre-paid service with insufficient identification requirements). Many phone numbers used by the suspects were only identified many years after their use. Some of the data requested was no longer available which left the prosecution case open to claims which could neither be provide or disproved.

~~CABINET IN CONFIDENCE~~

Sub No:
File No: 10/27823

COPY

ATTORNEY-GENERAL

Evidence in-camera to Senate Inquiry into the adequacy of protections for the privacy of Australians online

Deadline: None

Key Issues: Mandatory data retention in Australia is a contentious proposal which has attracted media interest and was addressed by nine of the 18 public submissions to the Senate Inquiry into the adequacy of protections for the privacy of Australians online. During the hearing, held on 29 October 2010, the Department committed to giving evidence in-camera regarding confidential aspects of the access to data regime under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and details of what was consulted on in the proposal for data retention, if the Committee wanted further details. The Committee has scheduled a further hearing date on 1 December 2010 and requested the Department provide in-camera evidence. Representatives from the Department and the AFP will appear – ASIO has been invited but is yet to respond to the request.

AGD Analysis: The Department intends to give evidence to the committee to explain the operation of the current data access regime in the TIA Act and outline the challenges facing the regime. Currently, telecommunications data is available to law enforcement and national security agencies for specific purposes, including enforcing the criminal law. Agencies are increasingly reporting that data requests are not being fulfilled because there is no consistency in the retention of information or carriers no longer retain the requested data due to changes to business practices or technologies. Unfulfilled requests can lead to investigations being abandoned and crimes going unsolved.

The Department also intends to advise the committee about the importance of the availability of telecommunications data going forward given the rapidly changing communications environment and the advanced techniques used by sophisticated criminals. A data retention proposal would aim to retain current industry practices into the future while minimising costs. That is, pursuing data retention in the future when elements of the data set are no longer collected would be prohibitively expensive as it would necessitate the redesigning of infrastructure.

The Department will not discuss any policy for going forward with a proposal nor speculate on what data would be required to be retained.

Financial Implications: None

Recommendation: I recommend that you note that the Department intends to give evidence in-camera to the Senate Inquiry regarding the operation of the current data access regime and the importance of mandatory data retention in light of changes in the telecommunications industry.

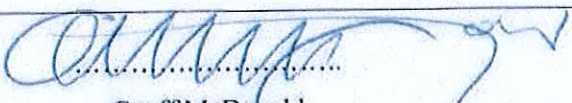
Note / Discuss

Catherine Smith
Assistant Secretary, Telecommunications and
Surveillance Law Branch

.....
Attorney-General

/ / 2010

S47F(1)
19 / 11 / 2010

Cleared by:  
Kelly Williams
19 / 11 / 2010
Geoff McDonald
19 / 11 / 2010

Action Officer: S47F(1)

Background

1. On 24 June 2010 the Senate referred the issue of the adequacy of protections for the privacy of Australians online to the Senate Standing Committee on Environment, Communications and the Arts for inquiry. During the 29 October 2010 hearing, the Electronic Frontiers Australia gave evidence that they considered data retention to be one of the biggest threats to privacy on the horizon and that they had yet to hear a good case as to why the scheme was necessary. They acknowledged that they can understand why law enforcement wants such a scheme and they thought the current regime for access to data was working well - however generally their evidence indicated that they had limited understanding of data retention.
2. The Department's opening statement gave unclassified background information about what telecommunications data is, the importance of telecommunications data and the rationale for the development of a data retention regime proposal in Australia. The Department and the AFP stated that there needs to be a balance between the concerns of privacy and the genuine needs of law enforcement and that this balance will ultimately be determined by the parliament.
3. The Department gave evidence that the consultation with industry was for the purposes of developing a model rather than consulting on a specific proposal. The Department provided the Senate Inquiry with a list of the industry organisations which were consulted in March 2010. However, the Department stressed to the Inquiry that the Department was still considering the merits of comparative data retention proposals and decisions concerning moving forward are a matter for government.
4. The Department provided the Committee with an In-Confidence version of the data sets and undertook to provide the Committee with a private briefing on data retention if required. The Inquiry is due to report on the second sitting day of the second sitting week in March 2011.
5. The Department will provide in-camera evidence to the committee outlining how industry trends, such as multi-function devices [redacted] S37(2)(b), S37(2)(c) [redacted]. In some circumstance telecommunications data can be as important, or more important, to agencies than the content of communications themselves. S37(2)(b), S37(2)(c) [redacted]
6. The AFP will provide more detailed operational examples to highlight the importance of continuing access to this information to investigate offences.

Sensitivities and Media Implications

7. The concept of a data retention regime attracted significant media interest when it became publicly known in June 2010. There was also some media coverage after the Senate Inquiry hearing.

Sub No:
File No: 10/27823-01

COPY

ATTORNEY-GENERAL

Online Privacy Inquiry - Response Recommendation 9

Deadline: Required by 30 September 2011 to align with timeframe for whole of Government response to the Committee's Recommendations being coordinated by the Department of Prime Minister and Cabinet.

Key Issues: The Senate Standing Committee on Environment and Communications completed their inquiry into the adequacy of protections for the privacy of Australians online on 7 April 2011. The Committee made nine recommendations in total. Recommendation nine specifically relates to mandatory data retention. A response to Recommendation 9 is at **Attachment A**.

The Department of Prime Minister and Cabinet is coordinating the response to the report with additional input from the Department and the Department of Broadband, Communications and Digital Economy. Department of Prime Minister and Cabinet are expected to finalise the Government response early October 2011.

AGD Analysis: A mandatory data retention proposal regime continues to be of public interest. In response to a request under freedom of information the Department released documents relating to the development of a data retention proposal (including documents relating to the Inquiry) which were published by the Australian Newspaper in July 2011. The Committee's recommendations focused on further justifying why such a regime is necessary, quantifying costs and greater consultation. These recommendations are consistent with the Departments approach in further developing data retention proposal options as part of holistic reconsideration of the *Telecommunications (Interception and Access) Act 1979*.

Financial Implications: None.

Sensitivities and Communications Plan: No specific communications strategy is being developed in response to this Inquiry however the Department of Prime Minister and Cabinet is coordinating a communications strategy as part of the broader Government response on privacy issues generally.

Recommendation: I recommend that you:

- a) approve the proposed Government Response to Recommendation 9 of the Committee Report, and

Approved / Not Approved / Discuss

- b) sign the letter to the Minister for Privacy and Freedom of Information at **Attachment B**.

Signed / Not Signed

Catherine Smith
Assistant Secretary – Telecommunications and
Surveillance Law Branch

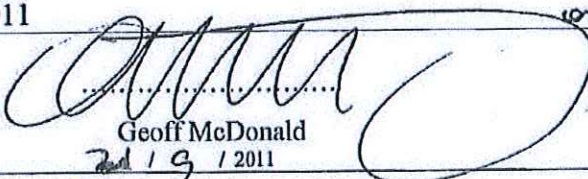
.....
Attorney-General

S47F(1)

/ / 2011

21 / 9 / 2011

Cleared by:


Geoff McDonald
21 / 9 / 2011

Action Officer: S47F(1), Date completed by AO 19/09./2011

Background

2. The Senate Environment and Communications References Committee tabled their report on "The adequacy of protections for the privacy of Australians online" on 7 April 2011. The Department of Prime Minister and Cabinet is coordinating the Government response to the Committee's report on behalf of the Minister of Privacy and Freedom of Information.
3. The Department appeared before the Committee and provided evidence about a possible data retention regime, part of this evidence was given in-camera. Recommendation nine of the Committee's report relates to data retention. Specifically, the Committee recommended that the Government must undertake an extensive analysis of the costs, benefits and risks of such a scheme, demonstrate the necessity of the data to law enforcement agencies to therefore justify the collection and retention of the data and the expense to Internet Service Providers, as well as assure the security of the information and consult with a range of stakeholders.
4. Consistent with previous public statements, the proposed response outlines the Government's commitment to an open, transparent and consultative approach. The concept of data retention is being progressed as part of holistic reconsideration of the *Telecommunications (Interception and Access) Act 1979* and it is intended that options for data retention regime will be put forward in the public discussion paper produced as part of the reform process.

Consultation

5. The Department of Prime Minister and Cabinet, Privacy and FOI Branch have been consulted in the development of this submission.

Sensitivities and Communication Plan

6. The concept of a data retention regime attracted significant media interest when it became publicly known in June 2010. There was some media coverage after the Senate Inquiry hearing and there have been a number of requests for release of documents under the *Freedom of Information Act 1982* since. The Department of Prime Minister and Cabinet have advised that they do not intend to engage in any media activity associated with the Government's response to the Committee's report. The Department of Prime Minister and Cabinet are developing a communications strategy as part of the broader work being undertaken with respect of privacy recommendations.



Australian Government
Attorney-General's Department

National Security
Law and Policy Division

10/27823-01

The Senate Environment and Communications References Committee conducted an inquiry into the adequacy of protection for the privacy of Australians online which was completed in April 2011. Recommendation 9 of the Committee's report:

The committee recommends that before pursuing any mandatory data retention proposal, the government must:

- *undertake an extensive analysis of the costs, benefits and risks of such a scheme;*
- *justify the collection and retention of personal data by demonstrating the necessity of that data to law enforcement activities;*
- *quantify and justify the expense to Internet Service Providers of data collection and storage by demonstrating the utility of the data retained to law enforcement;*
- *assure Australians that data retained under any such scheme will be subject to appropriate accountability and monitoring mechanisms, and will be stored securely; and*
- *consult with a range of stakeholders.*

Government Response

The Government agrees in principle with recommendation 9 of the Committee. The Government is committed to an open, transparent and consultative approach and acknowledges the public interest in these issues.

S47C(1)

Any proposal must strike the correct balance between community expectations regarding individual privacy, that unlawful behaviour is investigated and prosecuted, as well as the provision of competitive commercial telecommunications services.



ATTORNEY-GENERAL
THE HON ROBERT McCLELLAND MP

10/27823-01

The Hon Brendan O'Connor MP
Minister for Privacy and Freedom of Information
Parliament House
Canberra ACT 2600

Dear Minister:

I am writing to you in relation to the Senate Standing Committee on Environment and Communications report into the adequacy of protections for the privacy of Australians online which was completed on 7 April 2011.

One of the matters inquired into by the Committee was the concept of a mandatory data retention regime in Australia. The Attorney-General's Department, along with the Department of Prime Minister and Cabinet, the Department of Broadband, Communications and the Digital Economy, Australian Federal Police and the Australian Security Intelligence Organisation appeared before the Committee and gave evidence regarding the development of a mandatory data retention proposal.

Recommendation nine of the Committee's report specifically relates to data retention which falls within my portfolio responsibilities. Please find attached a response to Recommendation nine. I understand that the Department of Prime Minister and Cabinet is coordinating the Government response on your behalf.

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

Yours sincerely

Robert McClelland

Recommendation 9

The Senate Environment and Communications References Committee conducted an inquiry into the adequacy of protection for the privacy of Australians online which was completed in April 2011. Recommendation nine of the Committee's report:

The committee recommends that before pursuing any mandatory data retention proposal, the government must:

- *undertake an extensive analysis of the costs, benefits and risks of such a scheme;*
- *justify the collection and retention of personal data by demonstrating the necessity of that data to law enforcement activities;*
- *quantify and justify the expense to Internet Service Providers of data collection and storage by demonstrating the utility of the data retained to law enforcement;*
- *assure Australians that data retained under any such scheme will be subject to appropriate accountability and monitoring mechanisms, and will be stored securely; and*
- *consult with a range of stakeholders.*

Government Response

The Government agrees in principle with recommendation 9 of the Committee. The Government is committed to an open, transparent and consultative approach and acknowledges the public interest in these issues.

S47C(1)



Any proposal must strike the correct balance between community expectations regarding individual privacy, that unlawful behaviour is investigated and prosecuted, as well as the provision of competitive commercial telecommunications services.

Attorney-General's Department—National Security Law and Policy Division

08/1219

Secretary

Through Geoff McDonald – First Assistant Secretary

Industry Consultation on a Mandatory Data Retention Regime**Deadline:** None

Background: As well as the investigative benefit derived from analysing the content of targets' communications, law enforcement and security agencies can derive equally useful information from the data about those communications (data such as the parties making a communication, where and when that communication is made and the communication's duration).

Agencies have the legal authority to access this communications data, however due to technological advances and a demand for lower administrative costs, the telecommunications industry are no longer retaining the same amount of data, and retaining it for a shorter period of time.

In March 2008, in acknowledgment of this situation the Attorney-General gave approval for this Department to develop a proposal for a mandatory data retention regime. The Department formed and was chair of an Inter-Agency Working Group, comprising a number of Commonwealth and State law enforcement and regulatory agencies. The Department is working on the specific detail of the proposal and has recently settled on a draft standard for the type of telecommunications data to be retained. The Department is now in a position where it can consult with industry on this proposed data set and possible storage models.

Comment/Analysis: The benefit of a mandatory data retention regime [redacted] S47C(1) [redacted] as well as the recent review dealing with telecommunications interception. Retained [redacted] S37(2)(b) [redacted] to reveal the social networks of criminal organisations, locations of persons of interests [redacted] S37(2)(b) [redacted]. The development of a mandatory data retention regime is a key example of the Commonwealth's undertaking in the *Organised Crime Strategic Framework* to monitor the effectiveness of its legislative and operational response to organised crime.

Any data retention regime will have regulatory impacts. This can include costs relating to the storage and delivery of telecommunications data, [redacted] S37(2)(b) [redacted] as well as associated legal, administrative and staffing costs. However, these issues arose and have been addressed in the European Union where a mandatory data retention regime is in place. Therefore, consultation with industry is essential for the progression of this issue. In the attached submission, the Department asks the Attorney-General to approve consultation with industry to gauge regulatory impact and develop options to possibly offset this burden.

Recommendation

I recommend that you note this briefing and sign the attached ministerial submission

Signed / Not Signed / Discuss

Signed by:

For Catherine Smith
Assistant Secretary
Telecommunication and Surveillance Law Branch
Telephone: [redacted] S47F(1)

.....
Secretary

June 2009

/ / 2009

Action officer: [redacted] S47F(1), Director Telephone: [redacted] S47F(1)

29/7/10

Attorney-General's Department—National Security Law and Policy Division

10/13722

Secretary Through Geoff McDonald

Mandatory Data Retention Regime – Policy Proposal

Deadline: None

Background: The *Telecommunications (Interception and Access) Act 1979* (the TIA Act) currently allows a telecommunications provider to disclose telecommunications data if lawfully requested by an enforcement agency. The Attorney-General [REDACTED] S34(3), S47C(1)

[REDACTED] Earlier this year the Department consulted targeted industry participants on elements of a draft proposal. The existence of the draft proposal and consultation documentation has been leaked to the media resulting in FOI requests for this documentation.

Comment/Analysis: Access to telecommunications data is an extremely effective investigative tool for national security and law enforcement agencies to fight and solve crime and to protect national security by providing agencies with a method of tracing all communications from end-to-end, and in retrospect [REDACTED] S37(2)(b)

[REDACTED] It can also be used to reveal associations between members of criminal organisations, as well as provide [REDACTED] S37(2)(b) For example access to data enables agencies to:

- identify and build a picture of a suspect, provides vital clues to solve life threatening situations such as child abductions, and creates evidence for alibis and prosecutions
- counter terrorist threats, defeat cyber espionage and ensure border integrity and security, and
- investigate the ever increasing levels of technology enabled and cyber crimes such as child exploitation, online fraud, internet banking crimes and identity fraud

[REDACTED] S37(2)(b)

Industry has advised that they are moving towards business and billing models which will reduce the collection of telecommunications data. Accordingly destruction practices and developments in technology are resulting in telecommunications data not being available when disclosure is requested by agencies.

[REDACTED] S47C(1)

If no action is taken, vital information required to initiate investigations may not be available, investigations into serious crimes and terrorism may stall and the increasing number of cyber and online crimes will go unchallenged.

There is acknowledgement that developing technologies and the large uptake of online services as the preferred form of communication raises some privacy concerns. These concerns need to be balanced with commercial imperatives and community expectations that unlawful behaviour is investigated and prosecuted.

In response to similar challenges, on 15 March 2006 the European Union adopted Directive 2006/24/EC which requires Member States to ensure that communications providers retain certain data for up to 2 years. To date, 27 Member States have transposed the Directive with the exception of Ireland, Greece, Austria and Sweden. The implementation of the Directive has been subject to challenges in various States by privacy and consumer groups. In Germany, the Federal Constitutional Court declared the German data retention law void on the basis that the law went beyond the requirements of the Directive. The Court did not question the validity of the Directive.

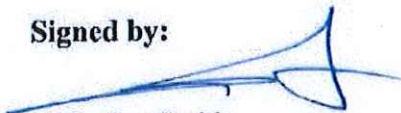
An Experts Group comprising representatives from law enforcement, the judiciary, privacy groups, industry and government was established by the European Council to develop guidelines for the implementation of the Directive and to undertake an assessment of its overall effectiveness. The Experts Group is expected to report to the European Council by 15 September 2010.

Last year, the United States of America introduced legislation requiring electronic communications providers to retain, for a period of at least 2 years, all records or other information relating to the identity of a user of a temporarily assigned network address and the services assigned to that use.

Recommendation

I recommend that you note the information provided.

Signed by:




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

29 July 2010

Action officer: S47F(1), Assistant Director, Telephone: S47F(1)

Noted / Discuss



.....
Secretary

29/ 7 / 2010