



ATTORNEY-GENERAL

CANBERRA

Senator the Hon Stephen Parry
President of the Senate
Parliament House
CANBERRA ACT 2600

3 SEP 2014

Dear Mr President

I refer to Senate Order No. 25 agreed by the Senate on 27 August 2014, requiring that I table a copy of the confidential industry consultation paper prepared by my Department, together with a definition of telecommunications data which will inform the Government's proposed data retention scheme.

The Order's terms are as follows:

(1) That the Senate notes:

- (a) the Government has not yet provided a definition of 'metadata' to be retained under the proposed mandatory data retention scheme, and*
- (b) media reports on 26 August 2014 suggested that the Attorney-General's Department has provided a definition in a document provided to the telecommunications industry; and*

(2) Orders that there be laid on the table, by the Attorney-General, no later than noon on Wednesday, 3 September 2014:

- (a) the definition of 'metadata' as defined by the Government's proposal on mandatory data retention, and*
- (b) a copy of the document distributed to the telecommunications industry within the past week which discusses this policy.*

The Government has publicly committed to consult with industry on a data retention model. Consistent with this commitment, my Department prepared an industry consultation paper to support further consideration of a data retention scheme by Government.

The paper was intended to facilitate and promote ongoing industry consultation. The paper promulgates a set of key indicia which could apply to a data set. The propositions put forward in the paper do not, however, and were not intended to, definitively represent the Government's position on the precise nature or scope of a data retention regime.

The items within the draft data set for discussion with industry have been included on the advice of agencies that those particular pieces of information are valuable and relevant for investigations. Ultimately, those items are valuable in protecting public safety. I expect the policy process to be informed by industry feedback. The consultation process does not presume a particular outcome and the scope of data retention is yet to be settled.

I am of the view that it is not in the public interest to provide a running commentary on consultations or the policy development process. The Government is seeking expert advice from across industry on carriers' current data retention practices in order to develop a robust and workable model. It is important to the integrity of this process that these consultations remain confidential.

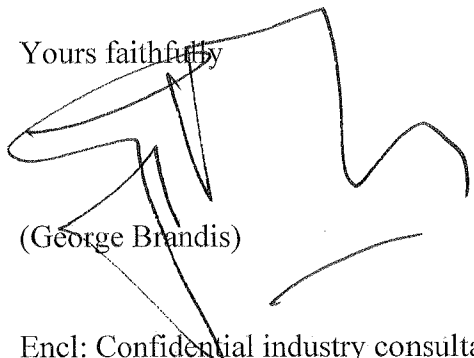
As consultations progress, the dataset and allied definitions to underpin it will evolve as part of a sensible, iterative process. It is not possible to proffer the definition anticipated in Order 2(a) before the dataset has been fully developed and subject to consultation with industry. The Government notes that the definition of telecommunications data which is informing present industry discussion is that contained in the *Telecommunications (Interception and Access) Act 1979* and canvassed on page 1 of the consultation paper. As indicated on page 2 of the paper, my Department has previously provided high level examples of what can be considered to be data, as opposed to content, to the Parliamentary Joint Committee on Intelligence and Security and the Senate Legal and Constitutional Affairs References Committee. The Government will make the final dataset available, together with any allied definitions, at the appropriate time.

In accordance with Senate Order 2(b), I provide the Senate with the attached confidential industry consultation paper – entitled *Telecommunications data retention – Statement of requirements*.

For completeness, I note that, contrary to claims by Senator Ludlam, this report was not 'leaked' by the Government to industry. Copies were provided to select industry representatives on a confidential basis to facilitate frank discussions as part of the policy development process. My office also provided a copy to Senator Ludlam, in his capacity as Chair of the Senate Legal and Constitutional References Committee Inquiry into comprehensive reform of the *Telecommunications (Interception) and Access Act 1979*, and the shadow Attorney-General, the Hon Mark Dreyfus MP, in light of their respective interest in the development of the policy.

I have copied this letter to the Leader of the Government in Senate, Senator the Hon Eric Abetz.

Yours faithfully



(George Brandis)

Encl: Confidential industry consultation paper – entitled *Telecommunications data retention – Statement of requirements*.



Australian Government
Attorney-General's Department

Version 1.0—August 2014

Confidential industry consultation paper

Telecommunications data retention—Statement of requirements

This document has been prepared for the purpose of preliminary consultation only. The outcomes of this consultation process will inform further policy development. This document does not represent approved policy of the Australian Government.

FOR CONSULTATION PURPOSES ONLY

This document has been disclosed to you in confidence for the purposes of consultation and may not be disclosed outside the members of your organisation involved in this consultation process without the approval of the Attorney-General's Department.

ACHIEVING A JUST AND SECURE SOCIETY | www.ag.gov.au

Executive Summary

The purpose of this paper is to provide the telecommunications industry with information to support further consideration of the development of a data retention scheme.

At this initial stage of consultation, Government is seeking information about the practicability of retaining a set of telecommunications data that meets the requirements outlined in this paper. The information provided by industry will assist Government to further develop policy on a range of issues, including future versions of the data set, retention periods for each element of the data set (to a maximum of 2 years), how to ensure requirements remain appropriate now and into the future, across different systems, services, networks and providers, exemption processes, information security arrangements, cost allocation, and implementation timelines and transitional arrangements.

Why is the Australian Government considering data retention?

Serious and organised criminals, and persons seeking to harm Australia's national security routinely exploit telecommunications services and applications to plan and carry out their activities. The records kept by providers about the services they provide are, therefore, vital to support law enforcement and security investigations. Data is an integral part of every national security investigation, and in virtually every serious and organised criminal investigation.

However, the telecommunications industry is competitive and technology driven. This has brought about a rapid increase of new services and the adoption of new business models that are eroding traditional business reasons for retaining telecommunications data. The declining availability of this information is degrading the ability of the Commonwealth, State and Territory Governments to combat serious crime and protect public safety.

It is timely to consider how the public interest in effective law enforcement and national security can be met without unduly impacting on the telecommunications industry. The requirements, outlined below, would ensure that a set of data continues to be available for law enforcement and national security purposes.

What is telecommunications data?

"Telecommunications data" is negatively defined in the *Telecommunications (Interception and Access) Act 1979*—it is information or documents about communications, but not the content or substance of those communications. The TIA Act does not positively define what is data; only what is not data.

The Department has previously provided high-level examples of what can be considered to be data, as opposed to content, to the Parliamentary Joint Committee on Intelligence and Security and the Senate Legal and Constitutional Affairs References Committee. Those submissions provided that data includes information about the parties to a communication (subscriber data) and information that allows a communication to occur (traffic data).

Examples of subscriber data include the name and postal and billing address of a customer as well as other contact details such as mobile numbers and email addresses. Examples of traffic data previously noted include internet identifiers, mobile numbers called or texted, the time, dates and durations of communications, and location information.

This document has been disclosed to you in confidence for the purposes of consultation and may not be disclosed outside the members of your organisation involved in this consultation process without the approval of the Attorney-General's Department.

A mandatory data retention scheme will apply to only a prescribed subset of “telecommunications data”.

This paper elaborates on earlier work to provide greater and more useful detail on an initial, proposed data set. The following dataset is based on the operational requirements of law enforcement and national security agencies. We anticipate that this data set may be further refined during this consultation process.

Who will data retention apply to?

The Australian Government’s current view, subject to consultation, is that data retention obligations should apply to all entities that provide communications services available in Australia. Providers should be subject to data retention obligations for all services they provide (including for roaming and international services), subject to appropriate exemptions for services that are of limited or no relevance to law enforcement or national security, potentially including IPTV services. Appropriate implementation and transitional arrangements should apply.

This document has been disclosed to you in confidence for the purposes of consultation and may not be disclosed outside the members of your organisation involved in this consultation process without the approval of the Attorney-General’s Department.

A. Requirements for data retention—Data set

The data set described in the following pages has been developed for consultation with the telecommunications industry. It reflects the requirements of security and law enforcement agencies, is designed to be technologically-neutral, and is broadly consistent with the categories of data set out in Article 5 of the former Directive 2006/24/EC; and ETSI Standards TS 102 656 (V1.2.1) *Retained Data: Requirements of Law Enforcement Agencies for handling Retained Data*, and TS 102 657 (V1.15.1) *Retained Data Handling: Handover interface for the request and delivery of retained data*.

The explanatory information in section B provides further information including examples of how we would expect these requirements to apply to particular technologies and services.

Nothing in this data set applies to or requires the retention of destination web address identifiers, such as destination IP addresses or URLs.

1. Information necessary to identify, and supplementary information regarding the subscriber or user of a service:

- (a) the current and historical name and address of the subscriber or user of the account, service and/or device
- (b) any current or historical account, service and/or device registered to the subscriber's or user's account
- (c) any current or historical permanent or transient identifier(s) allocated by the provider to an account, service and/or device
- (d) any current or historical supplementary identification, billing and payment, or contact information
- (e) current and historical account, service and/or device status
- (f) current and historical information about the usage of the account, service and/or device

2. Information necessary to trace and identify the source of a communication (including unsuccessful or untariffed communications):

- (a) the identifier(s) allocated to an account, service and/or device from which a communication is sent or attempted to be sent.

3. Information necessary to identify the destination of a communication (including unsuccessful or untariffed communications):

- (a) the identifier(s) allocated to an account, service and/or device to which a communication is sent or attempted to be sent
- (b) in cases where a communication is forwarded, routed, transferred or the like, the identifier(s) allocated to an account, service and/or device to which a communication is forwarded etc, or attempted to be forwarded etc.

This document has been disclosed to you in confidence for the purposes of consultation and may not be disclosed outside the members of your organisation involved in this consultation process without the approval of the Attorney-General's Department.

4. Information necessary to accurately identify the date, time of start and end or duration of a communication (including unsuccessful or untariffed communications)

- (a) the time and date of the start and end of the communication, or attempted communication
- (b) the time and date of the connection to and disconnection from the service

5. Information necessary to identify the type of communication:

- (a) the type of service used
- (b) service features used by or enabled for the communication

6. Information necessary to identify users' communication equipment or what purports to be their equipment:

- (a) the identifier(s) of the line, device and equipment connected to the service from which a communication is sent or attempted to be sent
- (b) the identifier(s) of the line, device and equipment connected to the service to which a communication is sent, including a device or equipment to which a communication is forwarded or transferred.

7. Information necessary to identify the location of communications equipment:

- (a) the location of the device or equipment used to send or receive a communication, based on the device's or equipment's connection to the service.

This document has been disclosed to you in confidence for the purposes of consultation and may not be disclosed outside the members of your organisation involved in this consultation process without the approval of the Attorney-General's Department.

B. Explanatory Statements

This section should be considered in conjunction with the requirements, and is intended to provide further explanation on each element.

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.

Requirement	Intent
1	Section one describes retention requirements for customer administration information held by the carrier or carriage service provider.
1(a)	This requirement intends to capture both present and past subscriber name and addresses information (including residence, business, post office, billing, payment or installation addresses) as are known, or were ever known, to the provider.
1(b)	This requirement intends to capture both present and past identifiers allocated to an account or service by the service provider (such as an IMSI, IP or email address, or other network identifier).
1(c)	This requirement intends to capture any present or past service, additional account or additional feature information linked to the subscriber's account(s), such as any bundled services or alternative email accounts the user may have.
1(d)	<p>This requirement intends to capture any additional information collected by the service provider as part of an enabling a service not explicitly outlined by a previous or subsequent specific requirement (such as identification information, date of birth, financial, billing and payment information, other transactional information, or contact information).</p> <p>In the case of mobile pre-paid services, this requirement intends to capture all identification and verification data obtained by a provider or its agent in accordance with the <i>ACMA Telecommunications (Service Provider - Identity Checks for Pre-paid Public Mobile Carriage Services) Determination 2013</i> (as amended), to the extent that they are not captured in the preceding items.</p>
1(e)	This requirement is to capture any change in the account state or billing type, such as information about an account being suspended due to a failure to pay, or about the pre-paid status of a service.
1(f)	This requirement is to capture any metrics that describe the use of the account, service or device, such as the available bandwidth, upload volumes and/or download volumes.
2	Section two describes retention requirements relating to the origin of communications.

This document has been disclosed to you in confidence for the purposes of consultation and may not be disclosed outside the members of your organisation involved in this consultation process without the approval of the Attorney-General's Department.

Requirement	Intent
2(a)	<p>This requirement intends to capture any identifier which uniquely describes the service at the time of the successful or attempted communication. An example of such an identifier is an ITU-T E.164 telephone number (FNN or international).</p> <p>For communications terminating on a provider's network or service, the source identifier should be retained even if the communication originated on another provider's network or service.</p> <p>Note: Category 2(a) does not apply to or require the retention of destination web address identifiers, such as destination IP addresses or URLs. This exception is intended to ensure that providers of retail and wholesale internet access services are not required to engage in session logging. However, operators of such services remain obliged to retain network address allocation records (including Network Address Translation records) under category 1(b).</p>
3	<p>Section three describes retention requirements relating to the destination of communications.</p>
3(a)	<p>This requirement intends to capture any identifier transmitted to the network to cause (or attempt to cause) a communication to take place. An example of such an identifier is an ITU-T E.164 telephone number (FNN or international). Related to this requirement is that of 3(b) which relates to the translation of identifier(s) obtained from 3(a) into subsequent identifier(s).</p> <p>For communications terminating on another provider's network or service, the destination identifier should be retained.</p> <p>Note: Category 3(a) does not apply to or require the retention of destination web address identifiers, such as destination IP addresses or URLs. This exception is intended to ensure that providers of retail and wholesale internet access services are not required to engage in session logging. However, operators of such services remain obliged to retain network address allocation records (including Network Address Translation records) under category 1(b).</p>
3(b)	<p>This requirement intends to capture the scenario in which a communication is routed to a subsequent identifier to that retained in 3(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.</p> <p>Note: Category 3(b) does not apply to or require the retention of destination web address identifiers, such as destination IP addresses or URLs. This exception is intended to ensure that providers of retail and wholesale internet access services are not required to engage in session logging. However, operators of such services remain obliged to retain network address allocation records (including Network Address Translation records) under category 1(b).</p>

This document has been disclosed to you in confidence for the purposes of consultation and may not be disclosed outside the members of your organisation involved in this consultation process without the approval of the Attorney-General's Department.

Requirement	Intent
4	Section four describes retention requirements relating to when communications occurred.
4(a) and (b)	These requirements intend to accurately capture the link between a communication or connection and the time at which it occurred. To achieve this, the provider must retain the service identifier with an accurate, unambiguous date & time marking; such a marking must include a method of indicating a time zone or reference to a global time. An example of this is a username with an accurate UTC & offset marking.
5	Section five describes retention requirements for the type of communication
5(a)	This requirement intends to capture the type of service used, including an access network or service (such as an ADSL or FD-LTE service) or an application service (such as VoIP, instant messaging or email).
5(b)	This requirement intends to capture any feature used by or enabled for the communication, such as call-waiting, bandwidth allocation, or upload and download allowances.
6	Section six describes retention requirements relating to the equipment used in communications.
6(a)	This requirement intends to capture the identifier(s) of the equipment from which a communication is sent or is attempted to be sent. Examples of such identifiers include the unique IMSI of the party originating the communication, the unique IMEI of the mobile device used to originate the communication, or the MAC address of the network interface used to originate the communication.
6(b)	<p>This requirement intends to capture the identifier(s) of the equipment used to receive a communication. Examples of such identifiers include the unique IMSI of the party receiving the communication, the unique IMEI of the mobile device used to receive the communication, or the MAC address of the network interface used to receive the communication.</p> <p>This requirement includes the scenario in which a communication is routed to a subsequent identifier to that retained in 3(a), such as the equipment to which a call was forwarded.</p> <p>Note: Category 6(b) does not apply to or require the retention of destination web address identifiers, such as destination IP addresses or URLs. This exception is intended to ensure that providers of retail and wholesale internet access services are not required to engage in session logging. However, operators of such services remain obliged to retain network address allocation records (including Network Address Translation records) under category 1(b).</p>

This document has been disclosed to you in confidence for the purposes of consultation and may not be disclosed outside the members of your organisation involved in this consultation process without the approval of the Attorney-General's Department.

Requirement	Intent
7	Section seven describes retention requirements relating to the location of the equipment used in communications.
7(a)	<p>This requirement intends to capture the physical and logical location of the device or equipment used to send or receive a communication.</p> <p>Note: Location information contained in the content of communications, such as assisted GPS information passing over a service or network, is not telecommunications data and is not included in this data set.</p>

This document has been disclosed to you in confidence for the purposes of consultation and may not be disclosed outside the members of your organisation involved in this consultation process without the approval of the Attorney-General's Department.