Australian Government
Attorney-General's Department

Version 1.1—September 2014

Industry consultation paper

Telecommunications data retention—Statement of requirements

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

Executive Summary

Government is seeking comments 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 finalise policy on a range of issues and finalise the draft data set. The purpose of this paper is to provide the telecommunications industry with clear and up-to-date information about the proposal to facilitate analysis and comment.

The information in this paper is provided for the purpose of consultation. The outcomes of this consultation process will inform further policy development.

What is data retention?

Mandatory data retention is the creation of a consistent minimum standard across industry for what data is collected and how long it is retained. The proposed minimum standard includes no data that is not currently collected by some industry participants. The policy recognises that providers may need to modify some systems to ensure they meet the minimum standard. Retention would be for two years.

The minimum standard, as outlined in this document, would be included in primary legislation to ensure the telecommunications industry has clarity and certainty about its obligations. Industry would be able to apply for exemptions in recognition of the fact that its services are varied and dynamic.

Why is the Australian Government considering data retention?

Serious and organised criminals, and persons seeking to harm Australia's national security, routinely use telecommunications services 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 national security investigations. Data is an integral part of every national security investigation and virtually every investigation of serious and organised crime.

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.

A. Additional Policy explanation

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 data is; only what data is not.

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.

A mandatory data retention scheme will apply to only a prescribed subset of telecommunications data. The data set is not an exhaustive list or a definition of telecommunications data. The data set is a narrow selection of telecommunications data of particular value to law enforcement and national security and appropriate for providers to retain for two years even if this exceeds business needs.

This paper elaborates on earlier work to provide greater detail on the proposed data set. Each item in the following data set is derived from the operational needs of law enforcement and national security agencies but it does not represent the totality of data. For example, destination IP addresses are telecommunications data, but are not included in the data set and therefore will not be subject to data retention obligations.

Who will data retention apply to?

Data retention obligations, consistent with existing legal and regulatory obligations, should be able to apply to all entities that provide communications services available to the public in Australia.

Therefore, data retention obligations should not be limited to licenced carriers but should also extend to any entity that provides communications services to the Australian public.

Limited to the services of each provider

Providers should be subject to data retention obligations for all services they provide to the public, whether directly or through contracts involving third parties. Providers should not be required to collect or retain data for services they do not offer. This limitation acknowledges that providers have various wholesale and retail relationships where different data is visible to different providers. Data retention obligations will avoid overlap by only applying to the provider that has direct access to the relevant data.

Exemptions and tailoring of data sets

Government is exploring the merits and scope of an exemption regime. Data retention obligations may include appropriate exemptions for services that are of limited or no relevance to law enforcement or national security, such as IPTV services. Exemptions will be available for entire services as well as particular elements of the data set for particular services or to reduce the retention period for large data sets. The exemption regime will be administered taking into account both the interests of law enforcement and national security agencies as well as the objects of the Telecommunications Act. To ensure targets are not attracted to exempted services and protect the commercial interests of providers, exemption applications will be confidential.

The Australian Government has considered releasing individual data sets for particular kinds of services, such as voice and IP. While this approach has merit and has been adopted internationally, Australia considers that it is not sufficiently technologically neutral and not suitable for inclusion in primary legislation. To address concerns about the application of the data set to new and emerging technologies, Government proposes to make available suitable guidance material over time. The scope of guidance will be limited by the primary legislation.

Commencement provisions

The Australian Government acknowledges that cost are minimised to the extent that system upgrades can be conducted in line with existing business cycles. Therefore, Government is exploring commencement provisions matched with the above exemptions regime designed to balance the pressing needs of national security and law enforcement agencies with appropriate transitional time frames for planning, building and testing systems.

Data formatting or request management

Data retention does not require the centralising of data to a single point on each provider's network, the formatting of data in accordance with any technical standard, or the development of request management systems to interface with agencies.

Security and data accuracy

Providers are already subject to a range of regulation and business incentives to appropriately secure data and ensure that it is sufficiently accurate. Providers have existing practices designed to address these imperatives, including the use of encryption in many circumstances. Data retention does not propose to mandate particular security standards.

B. Obligations 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 key 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 these requirements would 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 of a service:**
    (a) the current and historical name and address of the subscriber of the account, service and/or device
    (b) any current or historical account, service and/or device registered to the 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 or transferred, the identifier(s) allocated to an account, service and/or device to which a communication is forwarded etc, or attempted to be forwarded etc.
4. **Information necessary to accurately identify the date, time of start and end or duration of a communication (including unsuccessful or untarriffed 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 subscribers 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 at the start and end of a communication or session.

C. 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 subscriber administration information held by the provider. The word 'subscriber' intends to refer to the person who is the customer or account holder in relation to the service. This could include additional authorised or registered users, but acknowledges that providers can rarely confirm the particular person actually using a service.
1(a)	This requirement intends to capture both present and past subscriber name and address information (including residence, business, post office, billing, payment or installation addresses).
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 accounts the subscriber may have.
1(d)	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, charging, billing and payment information, other transactional information, or contact information). This requirement intends to capture identification and verification data recorded by a provider or its agent in accordance with rules, regulations or determinations, including the ACMA *Telecommunications (Service Provider - Identity Checks for Pre-paid Public Mobile Carriage Services) Determination 2013* (as amended), to the extent that they are not captured in the preceding items. This item does not capture documents or identifying numbers to the extent that recording those documents or numbers is otherwise prohibited by law.
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.

Requirement	Intent
2	Section two describes retention requirements relating to the origin of communications. For the purpose of unsuccessful or untarriffed communications, retention obligations accrue only for events where one service or device attempts to contact another service or device and a connection is established, regardless of whether the communication is completed, terminated or fails for another reason. This includes where a phone rings, but is not answered.
2(a)	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). 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. 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).
3	Section three describes retention requirements relating to the destination of communications For the purpose of unsuccessful or untarriffed communications, retention obligations accrue only for events where one service or device attempts to contact another service or device and a connection is established, regardless of whether the communication is completed, terminated or fails for another reason. This includes where a phone rings, but is not answered.
3(a)	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). For communications terminating on another provider's network or service, the destination identifier should be retained. 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).

Requirement	Intent
3(b)	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. 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).
4	Section four describes retention requirements relating to when communications occurred. For the purpose of unsuccessful or untarriffed communications, retention obligations accrue only for events where one service or device attempts to contact another service or device and a connection is established, regardless of whether the communication is completed, terminated or fails for another reason. This includes where a phone rings, but is not answered.
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 a sufficiently accurate 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. These obligations are limited to identifiers which are used by the service in question and are therefore available to the provider. For instance, the operator of a mobile network may not be able to identify a MAC address while the operator of a WiFi network may not be able to identify an IMEI.

Requirement	Intent
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 IMSI of the party originating the communication, the 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)	This requirement intends to capture the identifier(s) of the equipment used to receive a communication. Examples of such identifiers include the IMSI of the party receiving the communication, the IMEI of the mobile device used to receive the communication, or the MAC address of the network interface used to receive the communication. 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. 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).
7	Section seven describes retention requirements relating to the location of the device or equipment used in communications.
7(a)	This requirement intends to capture the physical and logical location of the device or equipment used to communicate. The requirement applies whether the subscriber is the sender or recipient of a communication. The requirement applies to the location when a communication or session starts and when a communication or session ends. The requirement does not extend to the location of a service or device during a communication or session. The obligations do not require retention of location of devices while they are not communicating. 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. Note: Category 7(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).