DATA RETENTION

Frequently Asked Questions for Industry

Issued by the Office of the
Communications Access Co-ordinator
Version 1.1 – July 2015

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Attorney-General's Department has prepared Version 1.1 of the guidance materials to further assist industry participants to understand the obligations arising from the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015. The latest iteration of the industry frequently asked questions (FAQs) provides further information about data retention obligations and is intended to be read together with the accompanying materials, including:

- a flow chart of the sequence for applying data retention provisions
- case studies (Annexure B), and
- a series of matrices (Annexure C) providing a guide to the kinds of information that should be typically kept for different service types.

The key topics that are addressed in Version 1.1 reflect the breadth of enquiries, such as compliance, exemptions, variations and implementation plans, which have been directed to the Communications Access Coordinator (CAC).

Version 1.1 of the guidance materials is not a substitute for professional or legal advice. It is intended to inform and explain the data retention obligations to industry.

This document is subject to periodic review to reflect continuing engagement with industry. To ensure that you have the latest version, please contact the Attorney-General's Department at cac@ag.gov.au or (02) 6141 2884.

FLOW CHART EXPLANATION

The following flow chart, developed to assist providers to understand their data retention obligations, represents the sequence for applying provisions and makes clear that certain provisions need to be applied to each relevant service independently.

The flow chart includes section references to the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*. While the flow chart includes most provisions relating to service providers' obligations, its purpose is to explain the sequencing of provisions and needs to be read in conjunction with other supporting material. Case studies at Annexure B are also provided to assist in using the flow chart.

Step 1 - Am I a carrier, carriage service provider or internet service provider?

Only carriers, carriage service provider and internet service providers (C/CSP/ISPs) have obligations under the data retention regime. Providers will typically be aware of their regulatory status through their compliance with other regulatory regimes. For example, CSPs that supply a standard telephone, public mobile or end-user internet access service are required to be members of the Telecommunications Industry Ombudsman. Similarly, carriers will hold a carrier licence. Note that under *Telecommunications Act 1997* section 87(5), a person who arranges the supply of a listed carriage service to a third person for reward is a CSP.

Step 2 - Do I operate a "relevant service"?

A relevant service is a service for carrying communications, or enabling communications to be carried, by means of guided or unguided electromagnetic energy or both. A "relevant service" is broader than a "carriage service" because it includes services that enable carriage. For example, a voicemail service or an authentication system enables communications to be carried.

Not all telecommunications services are relevant services. For example, a domain name system (DNS) service is not a relevant service. DNS is required for the operation but it does not enable them within the legislative scheme.

Step 3 - Pick one relevant service

Providers need to consider the application of obligations and exclusions for each relevant service individually.

The meaning of "service" is limited to the particular service element offered by a given provider, not the totality of a service provided to a customer by many providers. For example, a wholesale service provider's obligation is limited to its wholesale element and a retail service provider's obligation is limited to its retail element.

A useful way to think about the extent of a relevant service is to consider the data "visible" to each provider. For example, where a provider does not have "visibility" of a customer's IP address, it is likely that the IP address was assigned as part of a different relevant service. Similarly, if a provider does not have "visibility" of certain authentication information, it is likely that the authentication is an element of a different relevant service.

Providers do not need to consider the application of obligations to services provided only to a "same area" or an "immediate circle". Please refer to the frequently asked questions section for further information about "same area" and "immediate circle".

Step 3a - Apply "communications" or "sessions" to a relevant service

Data retention obligations do not apply to every packet. Transactional retention obligations are at the level of entire communications or sessions. Customer information in Item 1 of the data set needs to be retained regardless of communications or sessions.

The meaning of communication or session depends on each particular relevant service. For instance, for VoIP services, obligations are applied to each call scenario. For SMS, each SMS is a separate communication. For email, the session is the customer's log-in to the email service and the communications are each email. For internet access services, the session will typically be the period for which a private IP address is allocated.

Obligations do not extend to metadata that is not customer information and is not related to a particular communication or session. For example, a mobile network operator is not required to keep the location of a handset when the customer is not using the handset.

Step 3b - Apply the data set to those communications or sessions

The data set is applied to a relevant service only after the above considerations have been completed. A series of matrices at Annexure C have been prepared to help providers apply the data set to their relevant services.

The obligation to "create information" in section 187A(6) applies only to particular communications/sessions on a relevant service offered by a provider where that data is in the data set. The obligation to create does not extend to information that the provider is not required to retain. For instance, if a provider offers an "unlimited-calls" service and does not "create" information about the time at the beginning and end of a call, that provider would be required to create that information. The time at the beginning and end of a call is part of the data set and those calls are part of the service provided. However, the obligation to create information does not require one provider to obtain information from another provider about the other provider's service. This point is illustrated by the case studies at Annexure B.

Step 3c - Apply any relevant exclusions

After a provider has considered the application of the data set to communications or sessions on a particular relevant service, certain exclusions apply. Section 178A(4) excludes:

- the contents or substance of a communication
- if the relevant service in question is an internet access service, destinations on the internet
- data about other provider's over the top services
- information required not to be kept by of the *Telecommunications (Service Provider — Identity Checks for Prepaid Mobile Carriage Services) Determination 2013*, and
- information about the location of devices that is not used by the relevant service in question.

In most instances these exclusions operate for the avoidance of doubt. For instance, items in the data set do not in any event include content. Likewise, both over-the-top services and location data not used by a service are not data about communications or sessions of that relevant service.

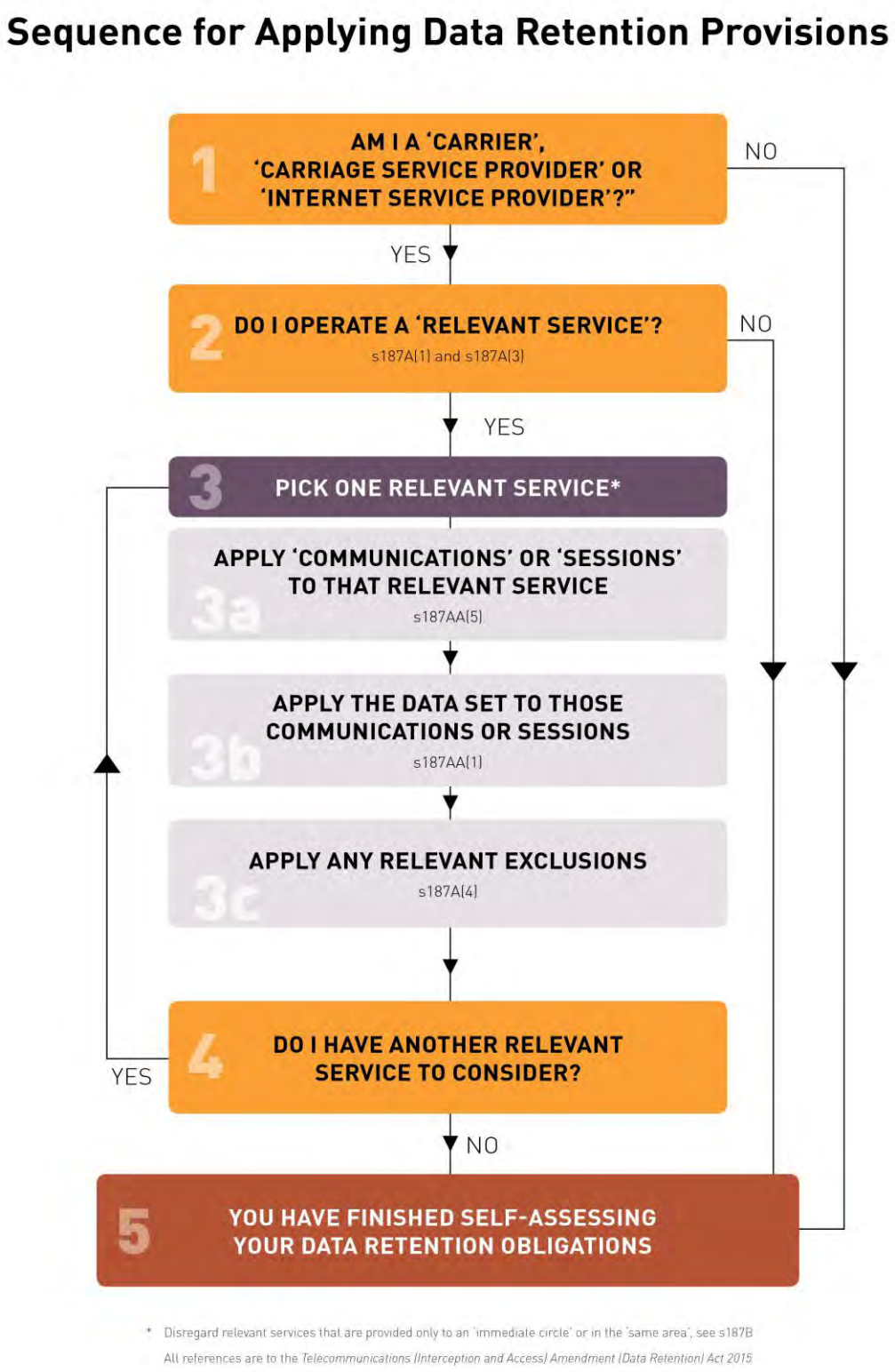
The exclusion of destinations on the internet only applies if the relevant service being analysed is an internet access service. If, for instance, the relevant service being analysed is a VoIP service, destinations on the internet are required to be obtained for that VoIP service. If a provider is operating both a VoIP service and an internet access service, consideration of these relevant services separately will ensure there is no confusion—destinations are excluded for the internet access service, but not for the VoIP service.

Step 4 - Do I have another relevant service to consider?

Many providers will offer more than one relevant service. Obligations need to be applied to each relevant service individually. The steps are repeated until data retention obligations have been considered for each relevant service unless it is provided only to an immediate circle or a same area.

Once a provider has considered its data retention obligations it is equipped to complete a data retention implementation plan and/or to consider seeking an exemption or variation.

FLOW CHART


Sequence for Applying Data Retention Provisions
1
AM I A 'CARRIER', 'CARRIAGE SERVICE PROVIDER' OR 'INTERNET SERVICE PROVIDER'?"
NO
YES
2
DO I OPERATE A 'RELEVANT SERVICE'?
s187A(1) and s187A(3)
NO
YES
3
PICK ONE RELEVANT SERVICE*
3a
APPLY 'COMMUNICATIONS' OR 'SESSIONS' TO THAT RELEVANT SERVICE
s187AA(5)
3b
APPLY THE DATA SET TO THOSE COMMUNICATIONS OR SESSIONS
s187AA(1)
3c
APPLY ANY RELEVANT EXCLUSIONS
s187A(4)
4
DO I HAVE ANOTHER RELEVANT SERVICE TO CONSIDER?
YES
NO
5
YOU HAVE FINISHED SELF-ASSESSING YOUR DATA RETENTION OBLIGATIONS
* Disregard relevant services that are provided only to an 'immediate circle' or in the 'same area', see s187B
All references are to the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015

FREQUENTLY ASKED QUESTIONS

1. DATA SET

1.1. What is telecommunications data?

- Telecommunications data is information or documents about communications, but not the content or substance of those communications.
- The data set specifies the categories of telecommunications data that must be retained for at least two years.

1.2. What is included in the data set?

- There are six categories of data that must be retained under the data retention obligations.
- Broadly, these six categories relate to:
    1. Subscriber and other relevant service-level account information
    2. The source of a communication
    3. The destination of a communication
    4. The date, time and duration of a communication
    5. The communication type
    6. The location of communication equipment
- A copy of the data set that explains its application in more detail and includes some practical examples can be found at Annexure A.

1.3. How long must service providers retain the data?

- Providers must retain the prescribed data for a minimum two year period from when it was generated.
- The data retention obligations do not stop a service provider from retaining items in the data set for longer than the required two year period for its own business purposes. If a provider retains data for longer than two years, authorised agencies can request access to that data.
- Specified subscriber data needs to be retained for two years after closure of an account. This allows the subscriber to be associated with a particular communication, and the service facilitating that communication, for the historical two year retention period.

1.4. What is a "service" for the purposes of data retention? (NEW)

- The Australian telecommunications industry uses the term "service" in a number of ways. Some industry participants use the term "service" to refer to a commercial product that can be sold to a customer, such as "a mobile phone service". The term is also used where many providers work together to deliver the final commercial product.
- In the context of data retention, a provider's "service" is the particular element of a commercial product that the provider operates.
- For example, a voicemail product offered to a customer may comprise a telephony service that connects users to the voicemail server. An SMS service would alert users to the existence of a

voicemail message on the server, and the voicemail server itself. These services could be operated by different providers or the same provider depending on business models.

- Providers need to take into account the commercial and technological context of a "service".
    - While a wholesaler, retailer and reseller may all provide an internet access service, each of the elements is a different "service" for the purpose of data retention.

- Understanding "service" in this way helps ensure that providers only need to keep data that relates to the service they provide (being data they have "visibility" of).

1.5. What data will service providers need to retain for their services?

- Service providers must retain each of the six categories of the data set for each of the services they offer, to the extent that the data set relates to each service.
- The data retained against each of the categories will differ depending on the type of service offered.
    - For example, the source of a communication (category 2) for a traditional voice call will be the originating phone number, whereas the source of an internet access service will be the IP address (and network address translation (NAT) information, if applicable) associated with a subscriber.

- Depending on the type of service offered, service providers may not be required to retain all of the six categories.
    - For example, internet access service providers are not required to retain category 3 data in relation to the provision of this particular service (relating to destination of a communication) as this would amount to a subscriber's web browsing history. Retention of this kind of information is explicitly excluded from the obligations under the legislation.
    - Service providers are not required to retain data about services offered by other service providers and do not need to retain data that is not relevant to the provision of their service.
    - For example, if a service provider offers a wholesale service only, it is only required to retain the categories of data in the data set that are relevant to the provision of that wholesale service.

- Service providers are required to retain data within the data set relating to unsuccessful or untariffed communications.
- If a service provider offers a free service (therefore generating no billing information) it is not required to retain billing information with respect to that service. However that provider will still need to retain subscriber and transactional data with respect to that service.

1.6. What constitutes a communication "session"?

- A series of communications, constituting a session, are to be taken as a single communication. This means that the data retention obligations do not require packet-level retention. A communication session is service-dependent and context-specific. A starting point for considering sessions is in terms of the service types below:
    1. **Access service** (lower level)—the communication session is bounded from authentication (i.e. log-on) to de-authentication (i.e. log-off).
    2. **Application service** (higher level)—the communication session is bounded from application-level session establishment messages to application-level session terminating signalling messages.

- The following examples may assist:
    - An **email communication session** is defined at the application service level as starting when a user connects to the mail server to check his or her email and finishing when that user disconnects from that mail server. However, **each email sent and received** during that session is an individual, discrete communication. Providers of email services will be required to keep relevant records about each email. This is different to the **access-level communication session**, defined as starting when a user logs onto his or her internet service via an access network, such as ADSL, and finishing when a user logs off from that network.
    - If carrier ABC provides an **access service**, then it retains communication session records appropriate to its level, such as the times a user logs on and off and its allocated network identifiers. If carrier ABC also provides an **application service**, then it retains communication session records appropriate to its level, such as the times a user connects and disconnects from the mail server and data relating to all email transactions that took place within that timeframe.
    - In a **mobile** environment, a mobile operator may provide both an access service and an application service. SMS works as an application service, where each SMS sent or received is a communication. The mobile service is the access service, where the handset is connected to the mobile network. Data relating to both services needs to be retained as per the data set.

1.7. There are a number of IP protocols used on the internet, such as SIP, FTP and IMAP, which are not specific to web-browsing use. Do providers need to retain IP destination addresses for these protocols?

- The data retention obligations do not require internet access service providers to keep data pertaining to the destination of a communication for internet access services.
- While the note under 187A(4) refers to "web browsing history", the subsection operates to exclude all addresses accessed via an internet access service. The operation of the exclusion extends to SIP, FTP and IMAP.
- As the data retention obligations apply to each relevant service that a provider operates, if an internet access service provider also operates an OTT service, such as VoIP, it must retain data pertaining to the destination of a communication for that service. For example, a provider will be required to retain SIP address information about a VoIP product even if the same provider offers an internet access service.

1.8. What NAT information are providers required to retain?

- The requirement to keep NAT records falls under obligations relating to an identifier allocated to an account or service.
- Where a carrier network uses multiple layers of NAT, records are required to be kept of each layer.
- For the avoidance of doubt, the requirement to keep NAT records will (at minimum) apply to the [Internal IP address; Internal Port; External IP address; External Port] elements of a NAT table. Whatever elements are kept as part of a provider's NAT records, it must be possible to uniquely identify and associate the Internal IP address/Internal Port to an External IP address/External Port and vice versa. If a carrier's NAT tables also include [Destination IP address; Destination Port] elements (for example, under a Symmetrical NAT model), data retention obligations will not apply to those elements. Whether a carrier wishes to retain those additional elements is a decision for the carrier.

1.9. What customer usage data is required?

- Data volume usage refers to the amount of information transmitted and received by the subscriber of a service. This information can be measured and retained per session, or in a way that aligns with the operation and billing of the service in question, such as per day or per month.
- The obligations do not require a provider to retain information relating to allowances that are rolled over from previous billing cycles. Item 5 of the data set captures data volume usage associated with communications or sessions.

1.10. What data relating to attempted and untariffed communications must be retained?

- The data retention obligations require a service provider to retain data relating to attempted and untariffed communications for services it provides. This does not include a provider retaining incoming connection attempts for accounts or destinations that do not exist. For example, scanning for active email accounts.
- Examples of attempted communications include where:
    - a phone number is dialled but the call is unanswered or rings out
    - an email or VoIP call is sent to a non-existent or incomplete address
    - an email server attempts to send a new email to an email client, but the client email server does not exist or is not working, and
    - a mobile phone number is dialled, but the destination mobile phone is switched off and the caller is informed that the phone is switched off or unavailable.
- Examples of untariffed communications include:
    - 1800 phone calls
    - communications sent using ‘unlimited’ phone or internet plans, and
    - free internet or application services.
- If a service provider does not currently retain required data relating to attempted or untariffed communications for a service that it provides, it must retain this data or seek approval for an exemption from this requirement from the Communications Access Co-ordinator (CAC).

1.11. What is meant by location of a device or equipment and what level of accuracy is required?

- Data retained will differ according to the service provided and the network’s configuration. As such, the requirement to keep information about the location of a telecommunications device is limited to circumstances where the information is used by the service provider in relation to that service.
- This means that the nature of the location records that service providers are required to keep will depend on how their network and service uses location information. For example:
    - In the case of a mobile network, a service provider is generally required to record the logical (cell ID) location(s) of the cell(s) to which a device was connected at the start and end of a call.
    - In the case of a Wi-Fi network, a service provider is generally required to record the logical and physical location of the access point to which a device was connected.

    - For a fixed-line service, including a wholesale service, this item of the data set can be complied with by providing the premises to which the service is provided, or the equivalent information.

- Where logical locations are retained, to ensure that the identifiers are meaningful, providers will need to ensure that the corresponding physical location of each logical location is available for the entire retention period.
- Providers will not be required to conduct additional processing or triangulation to more precisely determine a device's location, beyond what their network does for the purposes of providing the service.
- Importantly, location records are only required to be kept at the start and end of a communication, such as a phone call or SMS, not for each packet, poll or background update.

1.12. If a user moves off a provider's network, are service providers still required to retain location information relating to the end of that communication session?

- Yes. In this circumstance it is expected that the service provider would retain the last known location before the communication moved off that provider's network. Typically, this would constitute the point at which the communication involving that provider's network ended.
- The Department appreciates that there are circumstances in which devices will not properly detach from the network, such as where reception is suddenly lost, and that under these circumstances the retained data may be incomplete.

1.13. What resolution of time accuracy is required?

- Systems should be designed to allow sufficient accuracy to associate a subscriber or account with a particular communication.
    - For instance, a change of customer address may be kept to the nearest day, while NAT information for IP address may need to be accurate to a fraction of a second.
- Existing time stamps generated by service providers are to a granularity suited to particular business purposes and data retention does not modify existing practices.
- Service providers are best placed to know the granularity required to make a time stamp meaningful.

1.14. Is there a requirement to determine the customer equipment identifiers within customer home and business networks if these are not visible to a provider?

- No. Service providers are not required to retain equipment identifiers for customer premises equipment (CPE) that is not visible to the provider (i.e. the CPE is beyond the network termination point of a service provider).

1.15. Will service providers that do not currently create particular types of data for any business purpose be required to create that data solely to meet their data retention obligations?

- The data retention obligations have been drafted in a technologically-neutral manner and apply to types of information that are used in the provision of a service. Accordingly, we do not anticipate that service providers will be required to "create" data to meet their obligations.
    - For example, the data retention obligations do not require providers of free services that do not involve any form of billing or payment, to create or retain billing or payment data.

- The technologically-neutral approach to the data retention obligation means that many of the categories of data listed in the data set are limited to information used by the relevant service.
    - For example, Wi-Fi services generally use IP addresses, port numbers and Media Access Control (MAC) addresses to deliver communications to mobile devices, not IMEI or IMSI numbers. In that instance, IMEI and IMSI would not be relevant and therefore do not need to be retained, while IP addresses, port numbers and MAC address would.
    - Location information is expressly limited to location information used in relation to delivering the service; if the service does not use location information to operate, the service provider is not required to create and retain location information.
- In some instances, some types of information that are used in the provision of a service and that are covered by the data retention obligations may only be present transiently on the network or system. In these circumstances, service providers are required to keep this information.

2. OBLIGATIONS AND THE DATA RETENTION REGIME

2.1. Will there be a transitional period before the introduction of any obligations to provide time for planning, building a capability, testing?

- Service providers must comply with the data retention obligations by 13 October 2015.
- Service providers that cannot fully comply by 13 October 2015 must apply to the CAC for:
    - an extension of up to 18 months by lodging an implementation plan that details how they will achieve compliance by 13 April 2017, and/or
    - an exemption from and/or variation of their data retention obligations in relation to a service they provide.
- Implementation plans provide a mechanism to set out and seek approval for a pathway to compliance for each relevant service, including agreed milestones towards this goal.
- The CAC is able to grant exemptions from and variations to a service provider's data retention obligations.
- A template form, Data Retention Implementation Plan and/or Exemption and/or Variation Application, is available from the CAC.

2.2. What is the difference between interception capability and data retention?

- Telecommunications interception differs from data retention in that interception requires live interception of content passing over a network, whereas data retention requires the retention of a limited subset of telecommunications data, not content, for a minimum two year period.
- Under the interception regime set out in the TIA Act, Carriers/Carriage Service Providers (C/CSPs) are required to have interception capability for the services they offer.
- In addition to their interception obligations, C/CSPs will also be required to comply with their data retention obligations.

2.3. Can I use retained data for business purposes?

- Retained data remains the property of the service provider. As such, it can be used for lawful purposes, such as network trouble shooting.
- There are legislative restrictions on using certain types of information under the Privacy Act 1988 (Privacy Act) and the Telecommunications Act 1997 (Telecommunications Act).

- Service providers intending to use retained data for other business purposes are encouraged to seek advice.
- The Office of the Australian Information Commissioner (OAIC) may be able to assist in this matter. For more information please see The OAIC's Privacy fact sheet 17 and Australian Privacy Principle guidelines: Chapter 6 — Use or disclosure of personal information.

2.4. Does the data retention regime require duplication of the data set between wholesale service providers, retail service providers and/or resellers? (NEW)

- Section 187A(1) restricts a provider's data retention obligations to the relevant service/s it provides (see 1.4. What is a "service for the purposes of data retention"? for information on relevant services). This means that retailers/resellers and wholesalers do not need to share data with each other solely for the purpose of complying with their data retention obligations.
- Data that is shared between two service providers for the provision of a relevant service may be subject to data retention obligations. Given the layered nature of telecommunications services there will be some duplication of data across providers.
- Please refer to the case studies at Annexure B for an illustration of this point.

2.5. How does data retention differ between wholesale service providers, retail service providers and resellers? (NEW)

- A service provider is only obliged to retain data from the data set that it uses to provide its relevant service. The concept of having "visibility" can be useful in understanding what data a service provider must retain to meet its data retention obligations in relation to a particular relevant service.
- For example, data relating to an over the top email service is only retained by the relevant over-the-top provider.
- Contractual agreements can be used to define the boundaries between a wholesaler's and retailer/reseller's relevant services or for one provider to cause another provider to retain data on its behalf. The data retention obligations will remain with the provider who operates the relevant service.

2.6. What does own or operate infrastructure in Australia mean? (NEW)

- "Infrastructure" for the purpose of data retention refers to a broader range of infrastructure than traditional carriage infrastructure as referred to in the *Telecommunications Act 1997*.
- The Explanatory Memorandum specifically refers to servers used to operate an 'over the top' service such as VoIP, and consequently these would fall within the definition of infrastructure.
- Infrastructure includes traditional network infrastructure as well as servers located within Australia that are used to provide a relevant service.
- For example, billing systems and/or subscriber databases for an over-the-top service provider that are held on servers located within Australia are infrastructure.
- Operating infrastructure includes leasing or renting third party infrastructure to provide a relevant service.
- Operating infrastructure also includes situations where one piece of infrastructure, for example lit fibre, carries many distinct services.

2.7. Will off-shore over-the-top (OTT) providers that don't own or operate infrastructure in Australia be captured by the data retention obligations? (NEW)

- The data retention obligations only apply where the service meets all three of the following criteria:
    1. the service is for carrying or enabling communications to be carried by electromagnetic energy,
    2. the service is operated by a C/CSP or an Internet Service Provider (ISP), and
    3. the provider owns or operates infrastructure in Australia that enables provision of any relevant service.
- Criterion one captures a broad range of services including OTT services like VoIP and chat or other online/application messaging services.
- Criterion two acts as a limitation on the first criterion. That is, a person might host a website or an FTP server that facilitates communications via electromagnetic energy. But if that person does not have a carrier licence and does not meet the CSP or ISP definition, that person does not attract data retention obligations.
- Criterion three provides a further limitation by excluding providers that do not have any communications infrastructure in Australia. Infrastructure means any line or equipment used to facilitate communications across a telecommunications network. This includes servers that host websites or services furnished by OTT providers, as well as line links and network units.

2.8. In the event that a service provider provides a "low-level" communications service and does not have visibility of some elements of the prescribed data set, will it still be required to retain these?

- The obligation to retain data for a service only applies to the service provider that operates that service. Providers are not required to retain data that is not relevant to the provision of their services.
- For example, if a service provider offers a wholesale service only, that provider will only be required to retain the elements in the legislated data set that are relevant to the provision of that wholesale service.
- If a wholesale access service is on-sold by another provider to a retail customer, the wholesale provider is obliged to retain data in respect of its provision to the retail provider. The retail provider, rather than the wholesaler, is obliged to retain data in respect of the retail provider's own subscribers.
- Data relating to services provided on top of another service needs to be retained by the relevant OTT provider to the extent that provider is subject to the data retention regime.
- Put another way, the data retention obligations do not require a service provider to inspect another service provider's packets to determine what service may be running over the top.
- Given the layered nature of telecommunications services, it is expected that different items of the data set relating to a specific service will be retained across a number of service providers in many instances.

3. EXCLUSIONS

3.1. What services are excluded from the obligations?

- The legislative framework sets out that the prescribed data set does not need to be retained for some specified communications services. These include:
    - broadcast services (as defined by the *Broadcasting Services Act 1992*);
    - services supplied within an "immediate circle" (as defined by section 23 of the Telecommunications Act), and
    - services provided to places in the "same area" (as defined by section 36 of the Telecommunications Act).
- The purpose of these exclusions is to ensure that entities such as universities and corporations will not be required to retain telecommunications data in relation to their own internal networks (provided these services are not offered to the general public), and that providers of communications services in a single place, such as free Wi-Fi access in cafes and restaurants, are not required to retain telecommunications data in relation to those services.
- Although information about the use of such networks and services may be of value in relation to investigations, retention of that information is not mandated by the data retention obligations.
- The CAC may exempt a service provider from all or part of its data retention obligations in relation to a particular service. Given the considerable variation between networks and services, exemptions will generally be considered on a case-by-case basis. Exemptions made under this power will be made on the basis that they remain confidential; the disclosure of the existence of an exemption would create provider-of-choice concerns by disclosing an absence of capability. This would likely affect the law enforcement and national security interests that the CAC is required to take into account when granting or revoking an exemption.
- Exemptions may also reference a class of service providers, for example the CAC may specify that any service provider that provides an Internet Protocol television (IPTV) service is not required to retain any data in relation to that service. Similarly, an exemption or variation may be expressed to apply to a class of obligations.

3.2. What is considered a "same area" and how does a service provider know whether the exclusion will apply to a particular service? (NEW)

- The definition of "same area" for the purpose of the exclusion is contained within s36 of the *Telecommunications Act 1997*.
- The section provides that places are in the same area if they are the same property or form a combined area. This includes where the land is under a single title or contiguous properties have the same people as their principal users.
- Data retention obligations will not apply to a service provider in relation to a relevant service where that service is provided only to places that are all in the "same area".
- As a service provider, providers will need to consider who the receivers of a particular service are and then determine whether the receivers are within the "same area".
- Generally, a particular place will be considered a "same area" if it is contained within a single property. An area may be considered a "same area" where it is made up of adjoining properties, where the use of those properties is by a single user or group of users, and the purpose of their use is primarily the same.

3.3. What is an example of a "same area" comprised of more than one property? *(NEW)*

- Where a company has two adjacent office buildings it is likely the "same area" exclusion will apply to a relevant service that is provided only within that area. This is because the properties are contiguous and being used by a group of people for a common purpose.
- Companies should also consider the application of the immediate circle exclusion, see 3.5 for more information about immediate circles.

3.4. How does the same area exclusion apply where a lease is held over a part of a property that would otherwise be considered "same area"? *(NEW)*

- An example of this situation is a typical university campus. Usually, the single property will be comprised of a number of locations set aside for university groups. This may include a student union or a student publication, as well as a number of leased areas made up of commercial businesses, for instance, a bank or café. Assuming the entire university campus is a single title property, it would normally be considered a "same area". The fact that certain areas are set aside for particular university functions does not change the application of a "same area" test because it goes towards the same group of users working to achieve the same primary purpose. However, the commercial leases will not fall into the "same area" as they are not utilised by the same group of people in the interests of the same primary purpose.
- While the exclusion may still be applied to the university property, the areas taken up by commercial lease arrangements will not fall into the "same area". If a particular relevant service was provided to both the "same area" and the commercially leased area, that service would not be provided only to a "same area", meaning it would have data retention obligations.
- Providers may wish to consider applying for exemptions in certain circumstances, see 9.1. for further information about exemption applications.

3.5. What is classified as an "immediate circle" and how can I determine whether the exclusion applies to me? *(*NEW)

- The immediate circle exclusion applies to a relevant service that a provider supplies only to a person's immediate circle.
- A relevant service offered both to an immediate circle and to other unrelated people is not offered only to an immediate circle.
- Providers should consider the application of the immediate circle exclusion on a service-by-service basis. A provider may offer multiple services, some of which are provided only to an immediate circle and others which are available more broadly.
- The exclusion will apply where a particular relationship exists between the receivers of a relevant service. Section 23 of the Telecommunications Act 1997 sets out the particular relationships that fall within the scope of an immediate circle, for example:
    - where the person is a body corporate, a person's immediate circle consists of the body corporate itself, together with an officer of the body corporate and any other related body corporate.
    - where the person is an individual, a person's immediate circle consists of the individual, together with any employee of the individual.
- A relevant service provided only to an immediate circle, such as an internal corporate computer network or point-to-point links between a company's shop-fronts and its headquarters, has no data retention obligations.

3.6. Will government web sites that have a public access interface, e.g. Centrelink, be subject to the data retention obligations?

- No. These websites will generally not meet one or more of the test criteria for application of the data retention obligations, depending on how they operate and who operates them.
- Moreover, as web browsing history is excluded from the data retention obligations, there is also no obligation for information relating to who accesses this web portal to be retained.

3.7. Will entities providing services (e.g. free Wi-Fi) to their customers or members of the public be required to comply with data retention obligations?

- Entities that offer services in a "same area", such as free Wi-Fi access in cafés or restaurants, are not required to retain telecommunications data in relation to those services.
- The data retention obligations will, however, apply to the service provider supplying the service to that entity's venue. Simply put, a coffee shop offering free internet access to its customers will not have data retention obligations, but the café's ISP will.
- The CAC can provide guidance about whether a service falls into the "same area" category.

3.8. Will entities that provide communications to their staff (or students) be required to comply with data retention obligations?

- Entities that offer services only to a "same area" or only to an "immediate circle", such as free Wi-Fi access in cafés or restaurants, or internal corporate networks, are not required to retain telecommunications data in relation to those services.
- The data retention obligations will, however, apply to the service provider supplying the service to that entity's venue.
- The CAC can provide guidance about whether a service falls into the "same area" category.

4. INTERNET ACCESS SERVICE

4.1. What are the data retention obligations relating to a provider who only offers an internet access service (i.e. no additional OTT) services offered)?

- The data retention obligations for a service provider that only offers an internet access service involve retaining (for two years):
    - the time, date and location of a subscriber when the service was authenticated (logged-on) and the time, date and location of that subscriber for when the service was de-authenticated (logged-off), which represents a single communication session under section 187A(5).
    - all IP addresses and, where applicable, port numbers allocated to the subscriber during that session, including the associated dates and times.
    - Information relating to the subscriber and the service/s and device/s provided (as per category one of the data set). Certain types of subscriber information must be retained for the life of the account and for a further two years after the account is closed.
- Internet access service providers are not required to retain data pertaining to the destination of a communication for their internet access service, see sections 187A(4).

4.2. What are the data retention obligations relating to a provider who offers an internet access service and additional OTT services (e.g. email services and VoIP services)? (NEW)

- In applying the data retention obligations, each relevant service must be considered separately. Please refer to the flow chart as a useful guide to assessing the data retention obligations to each relevant service.
- For a service provider who offers an internet access service, the legislation excludes the retention of data pertaining to the destination of a communication in relation to their internet access service.
- The exclusion applies to information obtained 'only as a result of' providing an internet access service. This exclusion does not apply to additional OTT services (e.g. email services and VoIP services) as these are separate relevant services offered by the service provider and must be considered independently from the internet access service.
- In the VoIP context, destination information for VoIP calls must be retained by VoIP providers.

4.3. If provider offers an internet access service, is it required to retain IP addresses allocated by other providers?

- If the service in question only offers connection to the internet, a service provider will not be required to retain IP addresses allocated by other providers.
- However, if a provider offers an additional OTT service, such as VoIP, it will be required to retain the relevant destination communication information.
- For example, if a provider operates both an internet access service and an OTT service—it will be required to retain destination information only for the OTT service.
- Retained data for OTT services will be different to retained data for internet access services as they represent two different communications services. Some of the legislated categories of data will be relevant to one service type and not relevant to the other.
- In a wholesale/retail situation, if the retail provider allocates IP address/port number combinations, the retail provider will be required to retain that information, not the wholesaler—although the wholesaler could agree to provide data retention capability to the retailer for that requirement on a commercial basis.
- Wholesalers still attract data retention obligations, but the customers of that wholesale service will be retail providers or wholesale aggregators.

5. VOICEMAIL

5.1. What are the data retention obligations for service providers offering "voicemail" to their customers? (NEW)

- The process of determining whether data retention obligations apply needs to be completed for each relevant service with reference to the flow chart. For the purpose of data retention, a product like voicemail may be a conglomerate of relevant services. For example, a voicemail product offered to a customer may be made up of:
    - a phone service
    - an SMS service
    - an internet access service (for instance, an online portal for retrieval), and
    - the voicemail service itself.

5.2. What data is required to be retained in relation to "voicemail"? (NEW)

- A customer's voicemail communication session is bounded from authentication and de-authentication for the service. That is, when a customer logs in to their voicemail account and when that customer logs out of their account.
- Additionally, each voicemail message received is an individual communication. Providers of voicemail services will be required to keep records about each message.
- In applying the data set to a session, the types of information to be retained include:
    - subscriber information, such as the name, address and contact details of the customer
    - source of a communication, such as the phone number of the caller
    - destination of a communication, such as the phone number of the receiver
    - the date, time and duration of a communication. This category is also inclusive of a customer's connection to a relevant service, and
    - location of equipment or line used in connection with the communication, if known. The location records are limited to the location of a device at the start and end of a communication.
- Particular actions that occur inside a session, such as someone pressing a button to cause a message to be deleted or saved, would be the content of that communication and should not be retained for data retention purposes.

6. EMAIL

6.1. If a provider offers an email service, does the provider have data retention obligations for the email service? (NEW)

- If a provider supplies an email service, the provider of the service will have data retention obligations unless the email service is provided only provided to a person's "immediate circle".
- Data retention obligations will not apply for email services provided only to a person's "immediate circle", such as email services provided only to corporate or university networks (refer to 3.5. for more information on immediate circle).

6.2. If a provider offers an email service that has data retention obligations, what data does the provider need to retain? (NEW)

- Each authenticated connection to an email server (IMAP, POP, SMTP or web interface) is a communication session. Providers should retain information relating to this session, including:
    - identifiers of the subscriber connected to the server, for example, user name, IP address
    - the date and time when the session started
    - the date and time when the session ended
- Each email, either sent or received, is also a discrete communication. Information relating to each email sent or received should also be retained, including:
    - identifier for the sender and recipient of the e-mail who the email was sent to and received from
    - the date and time the email was sent/received
- The data retention obligations relate to information about a communication—not the content or substance of a communication (such as the subject or the body of an email).

- Providers are required to retain information about emails, including identifiers of all potential recipients of an email that a provider's subscriber has attempted to send or forward:
    - This includes destinations using the Carbon Copy (CC) and Blind Carbon Copy (BCC) functions, as well as emails that are unsuccessful.

6.3. Some fields in email headers may not be accurate e.g. the "from" field. Am I required to confirm the accuracy of this information? (NEW)

- Providers of email services are not required to ascertain the accuracy of the information in fields.

7. WI-FI

7.1. Where I offer a Wi-Fi service, do I have data retention obligations? (NEW)

- In many circumstances, a provider will offer an internet access service and a Wi-Fi service.
- Assuming that the provider is a C/CSP/ISP, a Wi-Fi service, is a relevant service, as it carries communications and enables the provision of the Wi-Fi service.
- Wi-Fi services have data retention obligations unless they are excluded under the "same area" or "immediate circle" exclusions – refer to 3.5.

7.2. If my Wi-Fi service has data retention obligations, what data do I have to retain for the Wi-Fi service? (NEW)

- A session for a Wi-Fi service begins when a device authenticates the Wi-Fi connection and ends when the device terminates or ends the connection.
- Typically, a Wi-Fi provider must retain information pertaining to this session including:
    - the time a device authenticates and terminates the session
    - the MAC address (or other identifier) of devices that connect to the Wi-Fi network, and
    - logical and physical location of the Wi-Fi access point to which the device was connected.
- A provider is not required to retain information about devices where there is no authenticated session. For example, if a person walks past a Wi-Fi hotspot without connecting, the Wi-Fi provider has no obligations with respect to that person.

8. DATA CENTRES AND MANAGED SERVICES

8.1. How does data retention apply to a "managed service"? *(NEW)*

- While a managed service may be a single product that a business offers, for the purposes of data retention, a managed service may be comprised of various 'relevant services', which the provider needs to consider individually.
    - For example, if a provider offers an internet access service and an email service as part of a single managed service product, the provider needs to consider these services separately for the purposes of data retention.
- Not all services that a provider offers, as part of a managed service solution, may be "relevant services" and subject to data retention obligations.
- Providers should also consider whether a managed service that it offers is to a person's immediate circle – refer to 3.5 for further information.

- If a provider offers a managed service, which is a relevant service, and is not captured by the "immediate circle" exclusion, then the provider should consider submitting an application for exemption for that particular service.

8.2. What are the obligations of data centres for the services they offer? (NEW)

- A typical data centre provides a variety of "relevant services". Data centre providers, and providers offering services from within the data centre, should consider the particular service they provide and apply data retention obligations only to that particular element.
- A provider that offers physical infrastructure inside a data centre does not have data retention obligations for this service. The reason for this depends on the particular service:
    - the provision of a business premise, air conditioning, electricity, server racks and hard disks are all excluded because these services do not carry communications or enable communications to be carried
    - cabling (including unlit and lit fibre) and switches inside the data centre are relevant services, as these services carry communications or enable communications to be carried. However, these services do not have data retention obligations, as the services are provided to places all in the same area
    - a provider that only offers the services mentioned above will therefore not have data retention obligations.
- Services that carry or enable communications to or from the data centre will have data retention obligations, unless otherwise excluded or exempted. Services with obligations may include:
    - physical infrastructure such as fibre cables connecting to the data centre (refer to), and
    - internet access services provided to the data centre.
- Any provider that hosts a server within a data centre may have data retention obligations relating to this particular service (refer to 1.4.).

8.3. Where I operate a Domain Name System (DNS) server, what data retention obligations do I have for this service? (NEW)

- The operation of the DNS is not a "relevant service", as it does not carry communications or enable communications to be carried. While a DNS server is convenient to the carriage of communications, it is not so central to the carriage of communications that it enables them.
- Therefore, the operation of a DNS server does not have data retention obligations.
- However, where the provider hosts the DNS server, it will have data retention obligations for the hosting of the server.

8.4. Where I offer an internet access service, do I have to retain DNS requests from my customers? (NEW)

- Where a provider offers an internet access service, the internet access service provider does not have to keep any DNS information.
- The DNS server is a "destination on the internet" and retaining that information would reveal browsing history.

8.5. Where I supply point to point services, do I have data retention obligations on these services?

- A provider that supplies point to point links (whether physical, wireless or logical) has data retention obligations as the link carries communications between various locations and is a relevant service. This is with the exception of specific exclusions, such as "immediate circle".
- A provider of such services should only consider the information that it has for the service it offers:
    - If the service provider only offers a point to point link the provider is only required to retain the elements of the data set that are relevant to that service.
    - If the provider only offers the physical infrastructure of the link without any "visibility" of traffic that passes over the infrastructure then typically the provider would retain:
        - The location of the physical infrastructure
        - The type of service it is, for example, fibre, wireless, and
        - The customer details for the physical infrastructure.
- Where some of a provider's point to point services are provided within an organisation, or to a single organisation, that provider should consider whether the service may be excluded from the data retention obligations under the "same area" or "immediate circle" exclusions (refer to 3.2.).

9. EXEMPTIONS

9.1. Under what circumstances would an application for an exemption from data retention be considered?

- As is currently the case for interception capability, exemptions will be considered on a case-by-case basis.
- In considering an exemption application, the CAC must take into account the interests of law enforcement and national security and the objects of the Telecommunications Act. The main (but not the only) objects of the Telecommunications Act are set out in subsection 3(1) and are to provide a regulatory framework that promotes:
    - the long-term interests of end-users of carriage services or of services provided by means of carriage services
    - the efficiency and international competitiveness of the Australian telecommunications industry, and
    - the availability of accessible and affordable carriage services that enhance the welfare of Australians.
- The CAC is also expressly required to consider:
    - the service provider's history of compliance with its data retention obligations
    - the service provider's costs, or anticipated costs, of complying, and
    - any alternative data retention arrangements that the service provider has identified (for example, if the service provider requests a variation of its obligations rather than a complete exemption).
- When considering the interests of law enforcement and national security, some of the factors that the CAC may consider are the number of subscribers, the risk profile of subscribers (including advice from agencies), the frequency with which authorised data requests have been or are likely to be made with respect to that system, and the adequacy of current arrangements or partial capability that can be implemented.

- Where granted, case-by-case exemptions could, for example, exempt providers from retaining some or all transactional data in categories 2-6 while still requiring the retention of subscriber and account data in category 1. This would reduce the burden on the service provider while still ensuring some more limited information remains available to agencies.
- Exemptions will be confidential.

9.2. Is the Government considering exemptions for services supplied to news sites and/or Government web sites?

- Browsing history is explicitly excluded from the data retention obligations, so retention of information about people visiting news or government web sites, including by companies providing services to those websites, is not required.

9.3. Is the Government considering exemptions for IPTV services?

- If a particular IPTV service falls exclusively within the meaning of broadcast services, it is excluded from the data retention obligations so there is no need for a specific exemption application to the CAC.
- The Explanatory Memorandum acknowledges that IPTV services may have limited or no relevance to law enforcement or national security.
- The Explanatory Memorandum also states that, under the exemption provision in the TIA Act, the CAC may make a determination specifying that any service provider that provides IPTV services is not required to retain any data in relation to its IPTV service.
- The Department cannot prejudge a decision by the CAC about whether an exemption will be granted.
- However, the Data Retention Implementation Working Group (IWG) has advised the Government that it considers that the following services represent possible candidates for full or partial exemptions from data retention obligations:
    - IPTV
    - On-demand video service
    - Internet Radio
    - Music Streaming
    - Telehealth services
    - Lifelogging services
- Providers can apply for exemptions they consider may be appropriate. All applications will be considered in accordance with the legislative requirements.

10. ENCRYPTION

10.1. Are service providers required to protect retained data? (NEW)

- Under the *Privacy Act 1988*, service providers are required to take steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

    o All service providers, including small business operators, are required to comply with the Privacy Act in relation to retained data.

- Service providers are also required to protect the confidentiality of retained data by encrypting it, and by protecting it from unauthorised interference or unauthorised access.

10.2. When must data be encrypted and protected pursuant to the Data Retention Act? (NEW)

- Data that a provider keeps to meet the data retention obligation needs to be encrypted.
- The Data Retention Act does not require providers to encrypt and protect other instances of the data that the provider is not keeping to meet its data retention obligations but to meet their business purposes, including where it meets the descriptions in the dataset that may be kept on various parts of their network or systems.
- This means that "one set" of data needs to be stored, encrypted and protected for a minimum of two years (or the life of the account plus two years, as applicable) and as long as the data is retained. If additional instances of the data exist for other purposes, they do not need to be encrypted.
- Providers can meet this obligation in two ways. Providers can create a stand-alone data store that is encrypted and protected and retains the necessary data whilst leaving operational systems unchanged. Alternatively, providers can expand operational systems to meet the required storage period and ensure the necessary data is encrypted and protected. Providers can also implement a combination of these two approaches.
- Back-ups that contain data being held to meet the obligation also need to be encrypted and secured.
- Providers may apply for partial or full exemptions from, or variations to this obligation. The Explanatory Memorandum to the Bill states that an example of a situation in which such an exemption or variation might be appropriate would be where the cost of encrypting a legacy system that was not designed to be encrypted would be unduly onerous and the provider has identified alternative measures that could be implemented. However, an exemption would not normally be appropriate where fulfilling the data protection obligations would be merely inconvenient.

10.3. Does the Act require data in transit (e.g. buffers) to be encrypted and protected, prior to it being retained? (NEW)

- No. Once data is being stored for data retention purposes, then the specific data retention requirement to encrypt and protect applies.

10.4. Does the Act require data on operational business systems need to be encrypted and protected? To what extent? (NEW)

- If the obligation to encrypt retained data is being met using a purpose built data retention system, data on operational business systems do not need to be encrypted.
- If a provider chooses to meet its obligation using existing systems, then the data retained for purposes of data retention will need to be encrypted.
- Back-ups that contain data being held to meet the obligation also need to be encrypted and secured.
- Providers may apply for an exemption from, or variation to those obligations. For example, if encrypting frequently accessed data would have a significant impact on a provider's business, the provider might wish to seek a variation to its obligations, substituting the encryption obligation for other, more practicable information security measures. Providers may also apply for a data retention implementation plan setting out a pathway to full compliance over a period of up to 18 months.

10.5. Are service providers required to comply with particular information security or encryption standards? (NEW)

- The legislative framework does not require service providers to comply with particular information security or encryption standards.
- The choice of the most appropriate information security and encryption measures will depend upon a range of factors, including the nature and configuration of a service provider's systems, and the volume and sensitivity of the data stored in each particular system.
- The Australian Government has published a range of guidance materials on information security and encryption, which may be of assistance:

  o Office of the Australian Information Commissioner Guide to securing personal information, which contains detailed information on how to protect personal information

  o Australian Signals Directorate Top 4 Mitigation Strategies and Strategies to Mitigate Targeted Cyber Intrusions, and

  o Australian Government Evaluated Products List, which includes detailed guidance on how to select, install and configure encryption products.

10.6. Can service providers obtain an exemption from the obligation to encrypt retained data? (NEW)

- Service providers may apply for an exemption from or variation to their information security obligations.
- In some cases, encrypting legacy systems may be unduly onerous, particularly where those systems were not originally designed to be encrypted. In such circumstances, alternative information security measures may be more appropriate.
- Service providers may also apply for approval of a Data Retention Implementation Plan that sets out the steps towards full compliance over a period of up to 18 months to facilitate progressive compliance.

10.7. Does the Act require data disclosure requests need to be encrypted and protected? (NEW)

- No. The encryption and security obligation under the Act applies to data being retained to meet the data retention obligation.
- Data disclosure is subject to separate statutory protections.

11. STORAGE AND SECURITY OF RETAINED DATA

11.1. Will data archived offsite (possibly taking days to access) be compliant under the data retention obligations?

- There is no required storage model or access timeframes for retained data.
- However, an excessive delay in accessing telecommunications data may breach a service provider's obligations under section 313 of the Telecommunications Act, namely to provide such help as is reasonably necessary in giving effect to a data authorisation. If retained data is archived, providers would need to have processes in place to access that information without undue delay. By way of example, if retrieving archived data involves sending a staff member offsite to retrieve it, it is expected that a provider would be able to send that person offsite promptly on receipt of an authorisation.

11.2. Are service providers required to centralise retained data?

- No, service providers are not required to centralise retained data.

11.3. Will service providers have to ensure high-reliability, duplicated data storage?

- Service reliability should mirror existing levels. That is, if billing type information is held for extended periods to a level sufficient to satisfy customers and applicable legal obligations, it is expected that information of this kind would continue to be held at that level.
- For other network information that is currently retained for business purposes, such as for network trouble shooting, that information may be kept to the standard appropriate to achieve that purpose.
- The CAC expects data retention systems to function correctly most of the time, but acknowledges occasional, minor disruptions as a result of unforeseen technical issues are a natural incident of the provision of the capability.

11.4. Are there requirements for the destruction of retained data?

- The data retention obligations do not require destruction of data, though other laws, such as the Privacy Act, may apply. See 12.7. for more detail.
- For more information on the Privacy Act please see the Office of the Australian Information Commissioner's Australian Privacy Principles guidelines: Chapter 11- Security of personal information.

11.5. Can data be optimised for storage or does it need to be retained in raw form to meet evidentiary requirements?

- Service providers are free to process information to minimise storage, provided they meet their data retention obligations.

11.6. What security standards are required for the retained data set?

- Service providers must protect retained data through encryption and prevent unauthorised access and interference.
- Guidance on the protection and encryption of retained data will be available from the CAC in due course.

11.7. What standards, if any, would service providers be asked to build to, e.g. international standards such as ETSI, or an agency standard?

- Service providers are not required to build data retention capability to a particular standard.
- The CAC is available to engage with service providers wishing to obtain guidance and advice on this issue.

11.8. What format is required for retained data? Will there be specific requirements around cataloguing, indexing and search criteria? Does the Government envisage the need for new technical standards to specify this?

- There are no particular formatting requirements or new Australian standards imposed on providers for retained data.
- The Department appreciates that usefully structured data can be of benefit to both industry and agencies.

11.9. Are vendors selling compliant systems now?

- The Department is aware of a number of vendors in the market that are selling systems designed to be compliant with the data retention regime.

- The Department is unable to recommend particular vendors.
- Industry representative bodies may be able to provide more information.

11.10. Will service providers be permitted to outsource their data retention obligations?

- Service providers may outsource some functions to meet the legislated requirement to keep data, to the extent consistent with laws on data handling (including protection of retained data) and disclosure.
- However, the data retention obligations remain with the service provider even if the provider outsources some technical capabilities. That is, the legislative obligation cannot be outsourced.
- Agencies' requests for retained data will continue to be made to the service provider directly.

12. REQUESTS AND ACCESS TO THE RETAINED DATA

12.1. Who can request access to data? (NEW)

- The Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Data Retention Act) limited data access to an approved list of agencies that have a clear operational or investigative need, as well as well-developed internal systems for protecting privacy. From 13 October 2015, the agencies authorised by law to request data from service providers are:
    - the Australian Security Intelligence Organisation
    - the Australian Federal Police
    - a Police Force of a State
    - the Australian Commission for Law Enforcement Integrity
    - the Australian Crime Commission
    - the Department of Immigration and Border Protection
    - the Australian Securities and Investments Commission
    - the Australian Competition and Consumer Commission
    - the New South Wales Crime Commission
    - the New South Wales Independent Commission Against Corruption
    - the New South Wales Police Integrity Commission
    - the Victorian Independent Broad-based Anti-corruption Commission
    - the Crime and Corruption Commission of Queensland
    - the Western Australian Corruption and Crime Commission, and
    - the South Australian Independent Commissioner Against Corruption.
- The Attorney-General may also declare that an agency has the authority to request access to telecommunications data through a legislative instrument, which will be publicly available. Service providers can contact the CAC if they have concerns about whether an agency is lawfully authorised to request data.

12.2. What will an agency's request for data look like? What do I need to do?

- Law enforcement and security agencies will continue to make requests for access to telecommunications data in the same way. Authorisations for access to telecommunications data under the TIA Act must be in writing (for example, via email).

- There are also strict oversight mechanisms around who can access data, including limitations on which agencies may make authorisations, and who within these agencies may make authorisations.
- A service provider should take steps to verify the authenticity of the request with the agency directly in the first instance, when they are in doubt of the authenticity of a request. Service providers that have residual concerns may request assistance from the CAC.
- The Telecommunications Act requires providers to record certain details of a request where an agency makes a request. These obligations include the need to record details such as a statement of the grounds for the disclosure.
- Service providers must give a written report annually to the Australian Communications and Media Authority (ACMA) relating to disclosures the provider made, as requested by agencies, within two months after the end of the financial year.

12.3. What will be the process by which agencies request access to, or be provided with, retained data? Is remote access to data envisaged? Will agencies query data directly?

- Law enforcement and security agencies will continue to make requests for access to telecommunications data as previously. Authorisations for access to telecommunications data under the TIA Act must be in writing (for example, via email).
- There are also strict oversight mechanisms around who can access data, including limitations on which agencies may make authorisations, and who within these agencies may make authorisations.
- A service provider should take steps to verify the authenticity of the request with the agency directly in the first instance, when they are in doubt of the authenticity of a request. Service providers that have residual concerns may request assistance from the CAC.
- The Telecommunications Act requires providers to record certain details of a request where an agency makes a request. These obligations include the need to record details such as a statement of the grounds for the disclosure.
- Service providers must give a written report annually to ACMA relating to disclosures the provider made, as requested by agencies, within two months after the end of the financial year.

12.4. What attributes will a lawful request ask a service provider to search for?

- Requests will continue to be made as they are now, on the basis of a request catalogue that is consistent with the types of information collected and retained by each service provider.
- The data retention obligations do not alter the data access authorisation arrangements. Service providers should expect that the kinds of requests they receive will change only to the extent that, once the data retention regime is fully implemented, requested data within the prescribed data set may be two or more years old.
- A request to a service provider for data for the purpose of identifying a journalist's source will have the same form as other data requests. Requesting agencies have additional requirements relating to these types of requests, including a requirement to obtain a journalist information warrant, before such a request can be made to a service provider.
- However, the existence of a journalist information warrant will not be disclosed to the service provider as part of an agency's data request. It is the responsibility of the requesting agency, not the service provider, to determine whether requested data falls under this category. Agencies' decisions in this respect will be subject to independent oversight by the Inspector-General of Intelligence and Security, in the case of ASIO, and the Commonwealth Ombudsman, in the case of enforcement agencies.

12.5. Do data requests negate the need for interception warrants?

- No. Agencies will continue to require a warrant to access the content of a communication.
- Communication content is separate to telecommunications data. Examples of communication content include any information that reveals the substance of a communication, such as the body and subject line of an email, private social media posts or what a subscriber searched for online.

12.6. Do data requests negate the need for data preservation notices?

- No. Data preservation notices relate to storage of communications content in the short term, while agencies obtain necessary warrants. Prescribed telecommunications data that is required to be retained under the data retention obligations refers to information or documents about communications, it does not include content.

13. OBLIGATIONS UNDER THE PRIVACY ACT 1988

13.1 Do all service providers (including small businesses) that have data retention obligations have obligations under the Privacy Act 1988? (NEW)

- Yes, all service providers must comply with the Privacy Act in relation to retained data. This includes data retained under an approved data retention implementation plan.
- This applies to all service providers with data retention obligations, including service providers who are otherwise small businesses for the purposes of the Privacy Act and, therefore, might otherwise have been exempt from the Privacy Act. Service providers that are already covered by the Privacy Act should ensure they continue complying with their obligations under the Act, both in relation to retained data and in relation to all other personal information they handle.

13.2 Does the Privacy Act apply to all retained data? (NEW)

- Yes, in the data retention legislation retained data is classified as personal information for the purposes of the Privacy Act and, therefore, must be handled in accordance with the Australian Privacy Principles.

13.3 Do all service providers need to have a privacy policy? (NEW)

- Yes, all service providers that are required to comply with the Privacy Act must have a clearly expressed and up to date policy about their management of personal information, including retained data.
- If the service provider is a small business within the meaning of the Privacy Act and would, therefore, otherwise be exempt from complying with the Australian Privacy Principles, the privacy policy only needs to address the provider's activities that relate to retained data.
- For more information about how to develop a privacy policy, see the Office of the Australian Information Commissioner's (OAIC) Guide to developing a privacy policy.

13.4 What do service providers need to notify their customers about? (NEW)

- Under Australian Privacy Principle 5 service providers that collect retained data about an individual must take reasonable steps to either to notify individuals of certain matters, or to ensure the individual is aware of those matters. These matters include:
    - the fact that the retained data is being collected and circumstances of that collection
    - that the collection is required by Part 5-1A of the Telecommunications (Interception and Access) Act 1979 (TIA Act)
    - the purposes of collection

- the consequences if personal information is not collected, including if the service provider would not be able to provide the relevant service
- the service provider's usual disclosures, including that the provider may disclose retained data to enforcement agencies
- information about the service providers privacy policy, including that it contains information about how the individual may complain about a breach of the Australian Privacy Principles by the provider
- whether the service provider is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located.

- What constitutes reasonable steps for a service provider will depend upon the circumstances and an individual may be notified or made aware of these matters through a variety of formats. For example, in some circumstances it may be appropriate for a brief privacy notice to be supplemented by longer notices or links to the provider's privacy policy. For more information please see the OAIC's Australian Privacy Principle guidelines: Chapter 5 — Notification of the collection of personal information.

13.5 What security obligations apply to service providers under the Privacy Act? (NEW)

- Under Australian Privacy Principle 11.1 in the Privacy Act service providers are required to take reasonable steps to protect retained data from misuse, interference and loss and from unauthorised access, modification or disclosure. These security obligations work together with providers' security obligations under the data retention legislation.
- For further information see the OAIC's Guide to securing personal information.

13.6 Do service providers have obligations to provide individuals with access to retained data held about them? (NEW)

- Yes, Australian Privacy Principle 12 in the Privacy Act requires service providers to give an individual access to retained data that the provider holds about them on request by the individual, subject to certain exceptions.
- The Privacy Act permits a service provider to charge the individual for access to retained data provided that the charge is not excessive and does not apply to the making of the access request.
- For further information see the OAIC's Australian Privacy Principle guidelines: Chapter 12 — Access to Personal Information.

13.7 Does the Privacy Act require service providers to destroy retained data after the end of the retention period? (NEW)

- Australian Privacy Principle 11.2 in the Privacy Act requires service providers to take reasonable steps to destroy or de-identify personal information where the provider no longer needs the information for a purpose for which it can be used or disclosed, unless an exception applies.
- One such exception includes where the service provider is required by law to retain the information, which would include service providers' data retention obligations. However, once the retention period for specific items of retained data ends, service providers should consider whether their obligation under Australian Privacy Principle 11.2 would require them to take reasonable steps to destroy or de-identify that data.
- For further information see the OAIC's Australian Privacy Principle guidelines: Chapter 11-Security of personal information.

14. OVERSIGHT AND COMPLIANCE

14.1. What compliance monitoring regime is envisaged and what are the implications of non-compliance?

- From a privacy perspective, the Information Commissioner will continue to have responsibility for monitoring industry's compliance under the Privacy Act and Part 13 of the Telecommunications Act. The Data Retention Act extends the Privacy Act to apply to small business operators in relation to retained data, ensuring that all service providers are subject to privacy obligations in relation to retained data.
- From a compliance perspective, the CAC will lead negotiations with industry on behalf of agencies. Serious or ongoing non-compliance may be referred to the ACMA for enforcement.
- Industry participants may face pecuniary penalties and infringement notices if they do not comply with their data retention obligations. Compliance with the obligations is also a condition of all carrier licences and part of the service provider rules.
- ACMA can issue infringement notices where a service provider contravenes the obligation to retain and secure the relevant data. Penalties under the infringement notice regime are currently set at $10,200 per contravention.
- Under the Telecommunications Act, if the Federal Court is satisfied that a person has contravened a condition of its carrier licence or the service provider rules, the Court may order the person to pay to the Commonwealth up to $10 million for each contravention.

14.2. What oversight and accountability mechanisms are in place?

- The Data Retention Act introduced new oversight and accountability mechanisms that apply to agencies. The Department does not expect that these mechanisms will materially impact industry.
- The Data Retention Act also limited the range of agencies permitted to access telecommunications data. "Criminal law-enforcement agencies" continue to be permitted to access this information. Other agencies can apply to the Attorney-General to be declared eligible to access telecommunications data, subject to strict criteria. Declarations may be subject to conditions, such as providing that a particular agency may only access specified subscriber records, or may only make data authorisations for the purpose of investigating specified offences. Either House of Parliament will be able to disallow a declaration.
- In addition, the Data Retention Act introduced independent, comprehensive oversight by the Commonwealth Ombudsman for all Commonwealth, state and territory enforcement agencies that access telecommunications data. The Ombudsman is required to inspect each agency to determine its compliance with the TIA Act, and the Attorney-General is required to table the Ombudsman's reports in Parliament.
- The Inspector-General of Intelligence and Security continues to have a role in ensuring that the Australian Security Intelligence Organisation (ASIO) acts legally and appropriately in accessing data under the legislation. The Office of the Inspector-General's findings, including any recommendations it may have issued, will continue to be included in its Annual Report.
- The Attorney-General is required to include information about the operation of the data retention regime in the Annual Report for the TIA Act. This information will be in addition to existing information that is published about agencies' requests for telecommunications data.
- In addition, the Parliamentary Joint Committee on Intelligence and Security is required to commence a review of the operation of the data retention scheme within two years after it is fully implemented, and to report within three years after it is fully implemented.

15. INFORMATION ON FUNDING

- The Attorney-General's Department engaged PricewaterhouseCoopers (PwC) to cost the implementation of the proposed data retention regime in consultation with industry. PwC estimated the upfront capital cost of the regime to all of business to be between $188.8 million and $319.1 million. This estimate has helped inform the Australian Government in delivering on its commitment to make a reasonable contribution to the upfront capital costs of data retention. The Budget includes funding of $128.4 million available to affected businesses over three years.

16. CONTACT

16.1. Who can I contact to find out more information?

- The Communications Access Coordinator (CAC) can be contacted at cac@ag.gov.au or by calling (02) 6141 2884.
- It is anticipated that some requests for information will be technical in nature, ranging across different areas of expertise. As such, it is preferred that requests are made via email. This allows the CAC to review the content and ensure that the person with the right technical expertise is assigned your query for response.

Annexure A – Kinds of information to be kept

Matters to which information must relate	Data set	Explanation and examples
1. The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service	The following: (a) any information that is one or both of the following: i) any name or address information; ii) any other information for identification purposes; relating to the relevant service, being information used by the service provider for the purposes of identifying the subscriber of the relevant service; (b) any information relating to any contract, agreement or arrangement relating to the relevant account, service or device; (c) any information that is one or both of the following: (i) billing or payment information; (ii) contact information; relating to the relevant service, being information used by the service provider in relation to the relevant service; (d) any identifiers relating to the relevant service or any related account, service or device, being information used by the service provider in relation to the relevant service or any related account, service or device; (e) the status of the relevant service or any related account, service or device	This category includes customer identifying details, such as name and address. It also includes contact details, such as phone number and email address. This information allows agencies to confirm a subscriber's identity or link a service or account to a subscriber. This category also includes details about services attached to account, such as the unique identifying number attached to a mobile phone, or the IP address (or addresses) allocated to an internet access account or service. This category further includes billing and payment information. Information about the status of a service can include when an account has been enabled or suspended, a relevant service has been enabled or suspended or is currently roaming, or a telecommunications device has been stolen. The phrases 'any information' and 'any identifiers' should be read to mean the information that the provider obtains or generates that meets the description which follows that phrase. If the provider has no information that meets the description, including because that kind of information does not pertain to the service in question, no information needs to be retained. For instance, if a provider offers a free service and therefore has no billing information, no billing information needs to be retained by that provider with respect to that service the provider will need to retain subscriber and transactional data with respect to that service, but no billing information needs to be retained. Service providers are not required to collect and retain passwords, PINs, secret questions or token codes, which are used for authentication purposes.
2. The source of a communication	Identifiers of a related account, service or device from which a communication has been sent or attempted to be sent by means of the relevant service.	Identifiers for the source of a communication may include, but are not limited to: the phone number, IMSI, IMEI from which a call or SMS was made

Matters to which information must relate	Data set	Explanation and examples
		identifying details (such as username, address, number) of the account, service or device from which a text, voice, or multi-media communication was made (examples include email, Voice over IP (VoIP), instant message or video communication) the IP address and port number allocated to the subscriber or device connected to the internet at the time of the communication, or any other service or device identifier known to the provider that uniquely identifies the source of the communication. In all instances, the identifiers retained to identify the source of the communication are the ones relevant to, or used in, the operation of the particular service in question.
3. The destination of a communication	Identifiers of the account, telecommunications device or relevant service to which the communication: a) has been sent; or b) has been forwarded, routed or transferred, or attempted to be forwarded, routed or transferred.	Paragraph 187A(4)(b) puts beyond doubt that service providers are not required to keep information about subscribers' web browsing history. The destination of a communication is the recipient. Identifiers for the destination of a communication may include, but are not limited to: • the phone number that received a call or SMS • identifying details (such as username, address or number) of the account, service or device which receives a text, voice or multi-media communication (examples include email, VoIP, instant message or video communication) • the IP address allocated to a subscriber or device connected to the internet at the time of receipt of the communication, or • any other service or device identifier known to the provider that uniquely identifies the destination of the communication. For internet access services, the Bill explicitly excludes anything that is web-browsing history or could amount to web-browsing history, such as a URL or IP address to which a subscriber has browsed. In all instances, the identifiers retained to identify the destination of the communications are the ones

Matters to which information must relate	Data set	Explanation and examples
		relevant to, or used in, the operation of the particular service in question. If the ultimate destination of a communication is not feasibly available to the provider of the service, the provider must retain only the last destination knowable to the provider.
4. The date, time and duration of a communication, or of its connection to a relevant service	The date and time (including the time zone) of the following relating to the communication (with sufficient accuracy to identify the communication): • the start of the communication • the end of the communication • the connection to the relevant service, and • the disconnection from the relevant service.	For phone calls this is simply the time a call started and ended. For internet sessions this is when a device or account connects to a data network and ends when it disconnected – those events may be a few hours to several days, weeks, or longer apart, depending on the design and operation of the service in question.
5. The type of a communication and relevant service used in connection with a communication	The following: a) the type of communication; Examples: Voice, SMS, email, chat, forum, social media. b) the type of the relevant service; Examples: ADSL, Wi-Fi, VoIP, cable, GPRS, VoLTE, LTE. c) the features of the relevant service that were, or would have been, used by or enable for the communication. Examples: call waiting, call forwarding, data volume usage.	The type of communication means the form of the communication (for example voice call vs. internet usage). The type of the relevant service (5(b)) provides more technical detail about the service. For example, for a mobile messaging service, whether it is an SMS or MMS. Data volume usage, applicable to internet access services, refers to the amount of data uploaded and downloaded by the subscriber. This information can be measured for each session, or in a way applicable to the operation and billing of the service in question, such as per day or per month. Note: This item will only apply to the service provider operating the relevant service: see paragraph 187A(4)(c).
6. The location of equipment or a line used in connection with a communication	The following in relation to the equipment or line used to send or receive the communication: a) the location of the equipment or line at the start of the communication; b) the location of the equipment or line at the end of the communication. Examples: Cell towers, Wi-Fi hotspots.	Location records are limited to the location of a device at the start and end of a communication, such as a phone call or Short Message Service (SMS) message. For services provided to a fixed location, such as an ADSL service, this requirement can be met with the retention of the subscriber's address. Paragraph 187A(4)(e) of the Bill provides that location records are limited to information that is used by a service provider in relation to the relevant service. This would include

Matters to which information must relate	Data set	Explanation and examples
		information such as which cell tower, Wi-Fi hotspot or base station a device was connected to at the start and end of communication. Service providers are not required to keep continuous, real-time or precise location records, such as the continuous GPS location of a device. These limitations seek to ensure that the locations records to be kept by service providers do not allow continuous monitoring or tracking of devices.

Annexure B – Case Studies

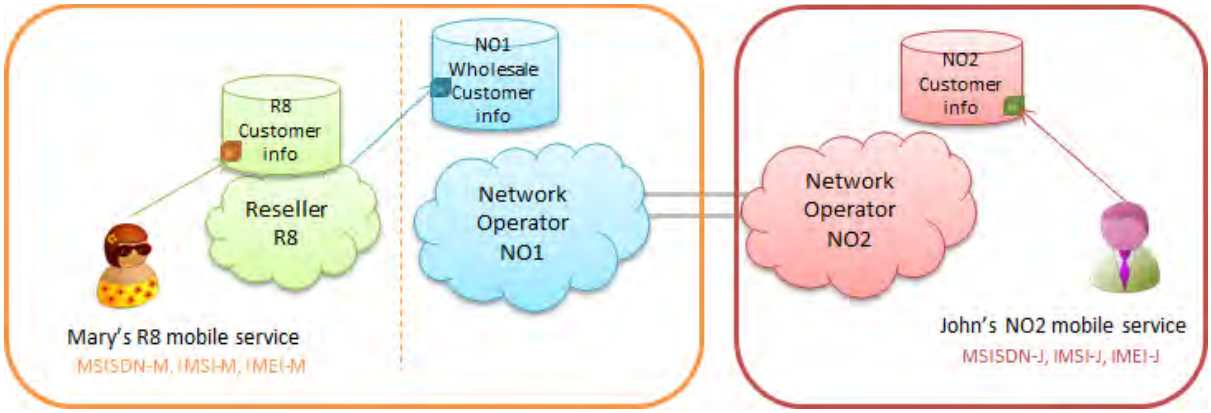
Data retention obligations vary across industry. The six kinds of information to be collected are defined and detailed in supporting material, the exact data that maps to those kinds of information depends on what technologies are used in delivering each particular service. The data available to a provider for retention purposes will vary depending on the particular role the provider has in delivering a particular service. Whether a provider is a retailer selling its own communications services, reselling another provider's services, or a wholesaler selling services to another provider to resell, it is critical to understand each provider's data retention obligations (see 'step 3' of the flow chart 'Sequence for Applying Data Retention Provisions').

The following scenario is intended to be read together with the accompanying flow chart, matrix and guidance materials.

Scenario 1 – Mobile Virtual Network Operator mobile call example

In this scenario, there are three providers involved, including:

- R8 (coloured green) is a mobile virtual network operator (MVNO), providing retail mobile services to its customers. R8 is a reseller, buying mobile services provided by network operator NO1.
- NO1 (coloured blue) is a mobile network operator who wholesales mobile services. R8 is NO1's wholesale customer.
- NO2 (coloured red) is also a mobile network operator who both operates and retails mobile services.



- Mary has a subscription for a mobile service provided by R8. R8 has Mary's customer details from when she signed up and bills Mary monthly, from billing files originated from NO1.
- John has a subscription for a mobile service provided by NO2. NO2 has John's customer details from when he signed up and bills John monthly using data created by its own network.

To understand how data retention obligations apply to each provider the relevant provisions must be applied in order. The flow chart makes clear the correct sequence for applying sections and that certain provisions need to be applied to each relevant service independently.

In this instance, R8, NO1 and NO2 are either carriers or carriage service providers, meaning they have data retention obligations. Each of them also offers at least one relevant service, noting they may also offer other relevant services beyond this scenario. Each provider needs to consider only the obligations that apply to its relevant service—not the totality of the service collectively offered by all providers.

In this scenario, R8's relevant service is coloured green, NO1's relevant service is coloured blue and NO2's relevant service is coloured red. The concept of data that is 'visible' to each provider is a helpful way of understanding the boundaries of each provider's relevant service.

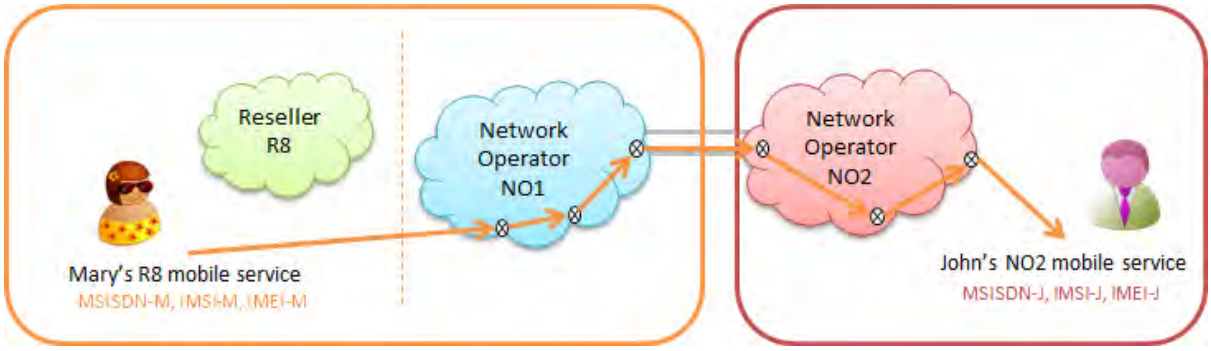
The first element of the data set is subscriber information (Item 1), which is applied generally rather than to sessions.

Retention of subscription information

Data set	R8	NO1	NO2
Item 1. The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service	Mary's subscriber details (address, financial records, subscription type, payment methods), MSISDN-M, IMSI-M. R8 also has IMEI-M as in this case R8 sold Mary her phone.	MSISDN-M and IMSI-M of the service being billed to R8, whether it is an active account and the date of activation.	John's subscriber details (address, financial records, subscription type, payment methods), MSISDN-J, IMSI-J, and IMEI-J

Transaction 1 – Mary calls John

Before the data set can be applied to particular communications-scenarios, step 4 of the flow chart requires the definition of "communications" or "sessions" to be considered for each provider's relevant service. In this scenario, the relevant communications are calls on the network. Therefore, when applying the data set, data that does not relate to calls does not need to be retained. For example, NO2 is not required to retain location information that is not connected with the start and end of John's communications, such as location updates. R8's relevant service does not have transactional information so R8 has no obligations beyond the subscriber data described above.



In the above call-scenario, Mary's mobile service is the *source* (Item 2) of the communication for all facilitating parties – R8, NO1 and NO2. However, as R8 does not undertake the routing of this communication, any data R8 retains will be as a result of the billing information it has about Mary. NO1 and NO2 will both have data on the call. NO1 will have Mary's MSISDN, IMSI and IMEI. NO2 will have Mary's MSISDN.

Similarly, John's mobile service is the *destination* (Item 3) of the communication for all facilitating parties. Again, as R8 does not route this communication, any data R8 retains will be as a result of the billing information it has about Mary. Again, NO1 and NO2 will both have data on the call. NO1 will have John's MSISDN and NO2 will John's MSISDN, IMSI and IMEI.

The *duration* (Item 4) of the call will be recorded by both NO1 and NO2. Once more, R8 will have retained this only as a result of any billing information they have on Mary.

The *type of communication or service used* (Item 5) is retained by both NO1 and NO2. In this particular example, both NO1 and NO2 would retain the communication since it was a voice communication over an LTE network. R8 has no obligation to record this information.

With respect to the sixth category of the information, *location (Item 6)* , NO1 would retain the cell tower location information for Mary's mobile at the start and end of Mary's call to John, NO2 would retain the cell tower location information for John's mobile at the start and end of Mary's call to John, and R8 has no obligation to record this information.

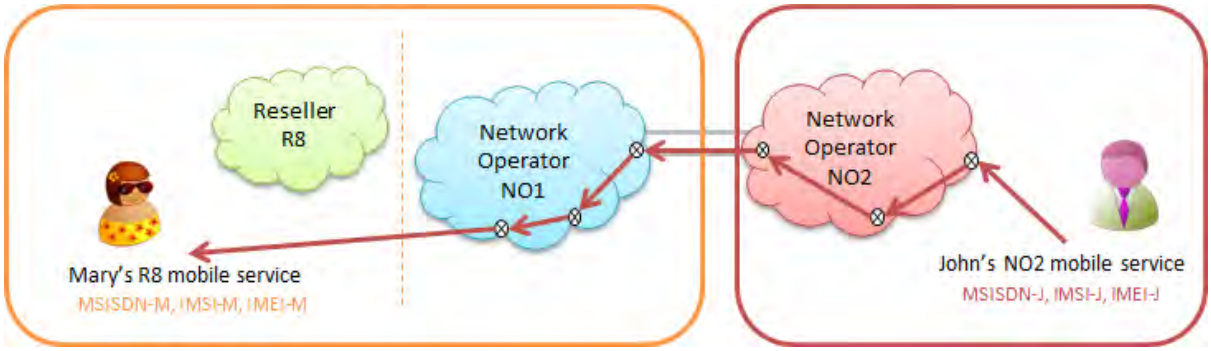
The obligation to "create information" in section 187A(6) of the Act only applies to data about particular communications on a relevant service offered by a provider that the provider is required to retain, consistent with the above analysis. For example, NO1 does not have to create (or obtain from NO2) information about John's cell tower location because that information relates to NO2's relevant service. However, if NO1 operated its network and billing systems in such a way that it does not collect the duration of Mary's call, NO1 would be required to create that information.

Retention of transactional information – Mary calls John

Data set	R8*	NO1	NO2
Item 2. The source of a communication	*(Mary's MSISDN*)*	Mary's MSISDN, IMSI, IMEI	Mary's MSISDN
Item 3. The destination of a communication	*(John's MSISDN*)*	John's MSISDN	John's MSISDN, IMSI, IMEI
Item 4. The date, time and duration of a communication, or of its connection to a relevant service	*(date, time and duration*)*	date, time and duration	date, time and duration
Item 5. The type of a communication, or of a relevant service used, in connection with a communication	-	LTE, voice	LTE, voice
Item 6. The location of equipment, or a line, used in connection with a communication	-	Mary's cell tower information at the start and end of communication	John's cell tower information at the start and end of communication

** Note: As R8 does not route this communication, any data retained will be as a result of the billing information they have on their customer, Mary, held under is subscriber information (Item 1).*

Transaction 2 - John calls Mary



R8 does not have visibility of this communication and hence has no obligation to retain any data for it. The obligations fall only on NO1 and NO2.

In this case, John's mobile service is the *source* (Item 2) of the communication. NO1 and NO2 will both have data on the call. NO1 will have John's MSISDN, while NO2 will have John's MSISDN, IMSI and IMEI.

Similarly, Mary's mobile service is the *destination* (Item 3) of the communication. Again, NO1 and NO2 will both have data on the call. NO1 will have Mary's MSISDN, IMSI and IMEI while NO2 will have Mary's MSISDN.

The *duration* (Item 4) of the call will be recorded by both NO1 and NO2.

The *type of communication or service used* (Item 5) is retained by both NO1 and NO2. In this scenario, both NO1 and NO2 would retain the communications since it was a voice communication over an LTE network.

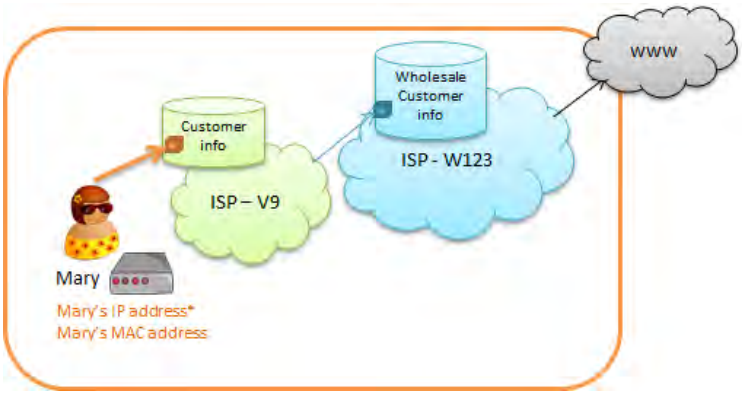
With respect to the sixth category of the information, *location*, NO1 would retain the cell tower location information for Mary's mobile at the start and end of John's call to Mary, NO2 would retain the cell tower location information for John's mobile at the start and end of John's call to Mary.

Retention of transactional information – John calls Mary

	R8[#]	NO1	NO2
Item 2. The source of a communication	-	John's MSISDN	John's MSISDN, IMSI, IMEI
Item 3. The destination of a communication	-	Mary's MSISDN, IMSI, IMEI	Mary's MSISDN
Item 4. The date, time and duration of a communication, or of its connection to a relevant service	-	date, time and duration	date, time and duration
Item 5. The type of a communication or of a relevant service used in connection with a communication	-	LTE, voice	LTE, voice
Item 6. The location of equipment, or a line, used in connection with a communication	-	Mary's cell tower information at the start and end of communication	John's cell tower information at the start and end of communication

[#] *Note: R8 will not have any information on this transaction.*

Scenario 2 – Internet Access Service with Reseller and Wholesale ISPs



In this scenario, Mary has a fixed internet subscription with the retail ISP provider V9.

- V9 is a virtual ISP (reseller) who buys their internet access service from the Wholesale ISP "W123" (wholesaler).
- V9 has Mary's customer details from when she signed up for her broadband service, including her contact number, email address, billing address, residential address, and financial details of how she pays for her service.
- V9 provided Mary with the router for her internet connection, so V9 has the MAC address of the device.
- W123 also has Mary's residential address, required to connect Mary's internet access service.

This scenario should be read in conjunction with the flowchart. The flow chart makes clear the correct sequence for applying sections and that certain provisions need to be applied to each relevant service independently.

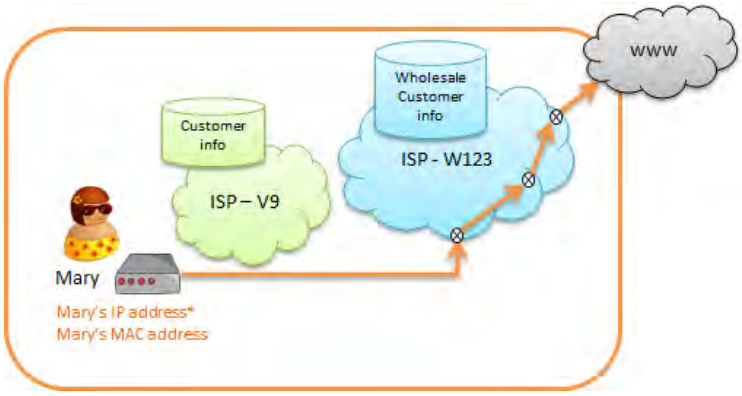
In this scenario V9 and W123 have data retention obligations as they are either a carrier, carriage service provider or internet service provider. The relevant service being considered for both parties is internet access. V9's relevant service is coloured green and W123's relevant service is coloured blue. The concept of data that is "visible" to each provider is a helpful way of understanding the boundaries of each provider's relevant service.

The first element of the data set is subscriber information (Item 1), which is applied generally rather than to sessions.

Retention of subscription information

Data set	V9	W123
Item 1. The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service	Mary's subscriber details (address, financial records, subscription type and payment methods). Details about the connection, such as date connected and technology deployed (e.g. ADSL). Details about the subscription, such as monthly allowance and usage, MAC address of the customer equipment (e.g. ADSL modem).	Details of V9 and the services being resold by V9. V9's address (any and all of physical, billing, postal) and contact details, contract details and details of services provided in a wholesale capacity. Additionally, some connection details about Mary to enable the service, such as DSLAM details for an ADSL connection and physical address.

Transaction – Mary accesses the internet



Before the data set can be applied to particular scenarios, step 4 of the flow chart requires the definition of "communications" or "sessions" to be considered for each service provider's relevant service. In this scenario, it is the definition of session that is relevant. Therefore, when applying the data set, data that does not relate to sessions does not need to be retained. For example, time stamps and data volume usage will relate to the session.

In this scenario, Mary's router's IP address is the *source* (Item 2) of the session for all parties – V9 and W123. If network address translation (NAT) was used to assign a public IP address to Mary's private IP address, W123 would also need to keep the NAT information (public IP address and port number). As V9 does not undertake the routing of this communication, any data V9 retains will be as a result of the billing information it has about Mary's usage of the service. W123 will have data on the session, as well as the MAC address used by the service.

No *destination* (Item 3) IP data should be retained in association with an internet access service because of the exclusion in s187(4)—see step 3c of the flow chart. (To avoid any doubt, some services that Mary makes use of on the internet may have their own data retention obligations and the obligations go to the provider of those other, relevant services. This is not necessarily the same as the provider of the internet access service.)

The *duration* (Item 4) of the session will be recorded by W123. To the extent that V9 has this information, it will have retained this only as a result of any billing information provided by W123 for Mary.

The *type of communication or service used* (Item 5) is retained by W123. In this scenario, W123 would retain the type of service since it was an internet access service, including details of the technology enabling that internet access service (e.g. ADSL).

With respect to the sixth category of the information, *location* (Item 6), W123 would retain and associate Mary's physical (i.e. fixed service) address to the session. W123 has this address as they connected her ADSL service but may not have her name. While V9 also has this address, it does not share the obligation to retain session data.

Retention of transactional information – Mary accesses the Internet

Data set	V9	W123
Item 2 .The source of a communication	Typically nil.	IP address(es) allocated to the service for the session (this is likely to be dynamically assigned by W123.) MAC address used
Item 3. The destination of a communication	Excluded.	Excluded.
Item 4. The date, time and duration of a communication, or of its connection to a relevant service	Typically nil.	Date, time and duration of the session.
Item 5. The type of a communication, or of a relevant service, used in connection with a communication	Typically nil.	Internet usage. Technology providing the relevant service (e.g. ADSL). Data volume usage.
Item 6. The location of equipment, or a line, used in connection with a communication	Typically nil.	Home address of the service.

Annexure C – Service Type Matrices

The series of tables provides a guide to the kinds of information that should be typically kept for different service types. The precise data any individual service provider will need to keep depends on a number of factors, including the relationship to the end-user of the relevant service, the relationship to the network operator and the data available from the underlying technologies.

The tables describe three broad categories of service provider in order to offer guidance on the kinds of data set information typically available for different service types. Note that a single service provider may offer a number of service types across different categories – for example, being a retailer for some services and a wholesaler for others.

The tables should be read in conjunction with the additional guidance materials and examples.

Data Set		**Voice and Video type services** such as payphones, traditional telephony, VoIP, voicemail services, video conferencing, etc.		
		CSP Retailer ☑ *Direct relationship with end-user* ☑ *Run the service*	**Reseller** ☑ *Direct relationship with end-user* ☒ *Run the service*	**Wholesaler** ☒ *Direct relationship with end-user* ☑ *Run the service*
1	The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service	Any information for a relevant service that is: Customer details inclusive of name(s), address (any and all of physical, service, billing, postal, directory), other contact details, billing records, payment or financial details, details of services or devices provided.	Any information for a relevant service that is: Customer details inclusive of name(s), address (any and all of physical, service, billing, postal, directory), other contact details, billing records, payment or financial details, services or devices provided. Billing records are also to be retained, however, are not required in order to create details for Data Sets below.	Any information for a relevant service that is: Details of the reseller service provider and the services being sold. Typically including name, address and contact details, contract details and details of services provided in a wholesale capacity.
2	The source of a communication	Identifier such as the telephone number of the service making the call, including the IP address(es) and ports if IP telephony. The MSISDN, IMSI, IMEI or other device identifier, where available. Details for each of these where there are multiple parties to the communication, such as teleconferencing.	Typically nil	Identifier such as the telephone number of the service making the call, including the IP address(es) and ports if IP telephony. In some cases this may be network routing numbers. The MSISDN, IMSI, IMEI or other device identifier, where available. Details for each of these where there are multiple parties to the communication, such as teleconferencing.
3	The destination of a communication	Identifier such as the telephone number of the service receiving the call, including the IP address(es) and ports if IP telephony. The MSISDN, IMSI, IMEI or other device identifier, where available. Details for each of these where there are multiple parties.	Typically nil	Identifier such as the telephone number of the service receiving the call, including the IP address(es) and ports if IP telephony. The MSISDN, IMSI, IMEI or other device identifier, where available. Details for each of these where there are multiple parties.
4	The date, time and duration of a communication, or of its connection to a relevant service	The date, time and duration of a call, including details of time zone.	Typically nil	The date, time and duration of a call, including details of time zone.

Data Set		Voice and Video type services such as payphones, traditional telephony, VoIP, voicemail services, video conferencing, etc.		
		CSP Retailer ☑ *Direct relationship with end-user* ☑ *Run the service*	**Reseller** ☑ *Direct relationship with end-user* ☒ *Run the service*	**Wholesaler** ☒ *Direct relationship with end-user* ☑ *Run the service*
5	The type of a communication or of a relevant service used in connection with a communication	Details of call services used such as call waiting, call forwarding or voice mail used. Details of type of service such as landline, mobile, nomadic, satellite or OTT telephony service. Details of the type of communication – for example, an LTE voice or video type of communication.	Typically nil	Details of call services used such as call waiting, call forwarding or voice mail used. Details of type of service such as landline, mobile, nomadic, satellite or OTT telephony service. Details of the type of communication – for example, an LTE voice or video type of communication.
6	The location of equipment, or a line, used in connection with a communication	Location (physical address, service address, latitude:longitude, logical address) of landline, payphone, cell tower, Wi-Fi hotspot or other point of connection to the network at the start and end of call.	Typically nil	Location (physical address, service address, latitude:longitude, logical address) of landline, payphone, cell tower, Wi-Fi hotspot or other point of connection to the network at the start and end of call.

Dataset		Messaging type services such as email, chat, SMS, IM, voicemail, MMS, etc.		
		CSP Retailer ☑ *Direct relationship with end-user* ☑ *Run the service*	**Reseller** ☑ *Direct relationship with end-user* ☒ *Run the service*	**Wholesaler** ☒ *Direct relationship with end-user* ☑ *Run the service*
1	The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service	Any information for a relevant service that is: Customer details inclusive of name(s), address (any and all of physical, service, billing, postal, directory), other contact details, billing records, payment or financial details, details of services or devices provided.	Any information for a relevant service that is: Customer details inclusive of name(s), address (any and all of physical, service, billing, postal, directory), other contact details, billing records, payment or financial details, services or devices provided. Billing records are also to be retained, however, are not required in order to create details for Data Sets below.	Any information for a relevant service that is: Details of the reseller service provider and the services being sold. Typically including name, address and contact details, contract details and details of services provided in a wholesale capacity.
2	The source of a communication	The service identifier such as the sending e-mail address, telephone number (SMS), chat name, IM address, including the IP address(es) and ports. The IMSI, IMEI, MAC address or other device identifier, where available.	Typically nil	The service identifier such as the e-mail address, telephone number (SMS), chat name, IM address, including the IP address(es) and ports. The IMSI, IMEI, MAC address or other device identifier, where available.

Dataset		Messaging type services such as email, chat, SMS, IM, voicemail, MMS, etc.		
		CSP Retailer ☑ *Direct relationship with end-user* ☑ *Run the service*	**Reseller** ☑ *Direct relationship with end-user* ☒ *Run the service*	**Wholesaler** ☒ *Direct relationship with end-user* ☑ *Run the service*
3	The destination of a communication	The service identifier of the receiving party(ies), such as destination e-mail address(es), IM, chat or telephone number (SMS) , including the IP address(es) and port(s). Details for each of these where there are multiple parties to the message, such as cc: and bcc: for e-mail. Destination details where a message is being forwarded, such as an SMS or another voicemail box.	Typically nil	The service identifier of the receiving party(ies), such as destination e-mail address(es), IM, chat or telephone number (SMS) , including the IP address(es) and port(s). Details for each of these where there are multiple parties to the message, such as cc: and bcc: for e-mail. Destination details where a message is being forwarded, such as an SMS or another voicemail box.
4	The date, time and duration of a communication, or of its connection to a relevant service	The date and time the message was sent, including details of time zone.	Typically nil	The date and time the message was sent, including details of time zone.
5	The type of a communication or of a relevant service used in connection with a communication	Detail of the service used, such as SMS, chat, IM, voicemail, e-mail, etc. Details as to whether the communication was delivered over fixed or mobile broadband, satellite or other services.	Typically nil	Detail of the service used, such as SMS, chat, voicemail, IM, e-mail, etc. Details as to whether the communication was delivered over fixed or mobile broadband, satellite or other services.
6	The location of equipment, or a line, used in connection with a communication	Where available, physical and logical location of fixed broadband, cell tower, Wi-Fi hotspot or other point of connection to the network at the start and end of call.	Typically nil	Where available, physical and logical location of fixed broadband, cell tower, Wi-Fi hotspot or other point of connection to the network at the start and end of call.

Dataset		Internet service type services such as mobile internet, fixed broadband, satellite broadband, etc.		
		CSP Retailer ☑ *Direct relationship with end-user* ☑ *Run the service*	**Reseller** ☑ *Direct relationship with end-user* ☒ *Run the service*	**Wholesaler** ☒ *Direct relationship with end-user* ☑ *Run the service*
1	The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service	Any information for a relevant service that is: Customer details inclusive of name(s), address (any and all of physical, service, billing, postal, directory), other contact details, billing records, payment or financial details, details of services or devices provided.	Any information for a relevant service that is: Customer details inclusive of name(s), address (any and all of physical, service, billing, postal, directory), other contact details, billing records, payment or financial details, services or devices provided. Billing records are also to be retained, however, are not required in order to create details for Data Sets below.	Any information for a relevant service that is: Details of the reseller service provider and the services being sold. Typically including name, address and contact details, contract details and details of services provided in a wholesale capacity.

Dataset		Internet service type services such as mobile internet, fixed broadband, satellite broadband, etc.		
		CSP Retailer ☑ *Direct relationship with end-user* ☑ *Run the service*	**Reseller** ☑ *Direct relationship with end-user* ☒ *Run the service*	**Wholesaler** ☒ *Direct relationship with end-user* ☑ *Run the service*
2	The source of a communication	Identifiers of a related account at the commencement of a session such as IP address and MAC for fixed broadband, or IP address, port and IMEI for mobile data.	Typically nil	Identifiers of a related account at the commencement of a session such as IP address and MAC for fixed broadband, or IP address, port and IMEI for mobile data.
3	The destination of a communication	Nil for Internet Access Services (IAS)	Typically nil	Nil for Internet Access Services (IAS)
4	The date, time and duration of a communication, or of its connection to a relevant service	Date and time of communication or session beginning and end, including time zones.	Typically nil	Date and time of communication or session beginning and end, including time zones.
5	The type of a communication or of a relevant service used in connection with a communication	Details of type of service including the type of communications (e.g. data) the type of service (e.g. mobile, Wi-Fi, Satellite, ADSL), and features used (e.g. volume usage)	Typically nil	Details of type of service including the type of communications (e.g. data) the type of service (e.g. mobile, Wi-Fi, Satellite, ADSL), and features used (e.g. volume usage)
6	The location of equipment, or a line, used in connection with a communication	Location of service, such as physical address for fixed services, cell tower for mobiles, Wi-Fi access point or other relevant location.	Typically nil	Location of service, such as physical address for fixed services, cell tower for mobiles, Wi-Fi access point or other relevant location.

Dataset		Data Link type services such as point to point service, SDH, Dark Fibre, ISDN, MPLS		
		CSP Retailer ☑ *Direct relationship with end-user* ☑ *Run the service*	**Reseller** ☑ *Direct relationship with end-user* ☒ *Run the service*	**Wholesaler** ☒ *Direct relationship with end-user* ☑ *Run the service*
1	The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service	Any information for a relevant service that is: Customer details inclusive of name(s), address (any and all of physical, service, billing, postal, directory), other contact details, billing records, payment or financial details, details of services or devices provided. Details of end points, such as physical addresses. Details of the type of relevant service such as, for example, ISDN, SDH, Point-to-Point. The date that the service was established and dates for any subsequent changes to the service such as, for example, installation dates and dates when substantial changes are made to the service.	Any information for a relevant service that is: Customer details inclusive of name(s), address (any and all of physical, service, billing, postal, directory), other contact details, billing records, payment or financial details, services or devices provided. Details of the type of relevant service such as, for example, ISDN, SDH, Point-to-Point. The date that the service was established and dates for any subsequent changes to the service such as, for example, installation dates and dates when substantial changes are made to the service.	Any information for a relevant service that is: Details of the reselling service provider and the services being sold. Typically including name, address and contact details, contract details and details of services provided in a wholesale capacity. Details of the type of relevant service such as, for example, ISDN, SDH, Point-to-Point. The date that the service was established and dates for any subsequent changes to the service such as, for example, installation dates and dates when substantial changes are made to the service.

Dataset		Data Link type services such as point to point service, SDH, Dark Fibre, ISDN, MPLS		
		CSP Retailer ☑ *Direct relationship with end-user* ☑ *Run the service*	**Reseller** ☑ *Direct relationship with end-user* ☒ *Run the service*	**Wholesaler** ☒ *Direct relationship with end-user* ☑ *Run the service*
2	The source of a communication	Typically nil	Typically nil	Typically nil
3	The destination of a communication	Typically nil	Typically nil	Typically nil
4	The date, time and duration of a communication, or of its connection to a relevant service	Typically nil	Typically nil	Typically nil
5	The type of a communication or of a relevant service used in connection with a communication	Typically nil	Typically nil	Typically nil
6	The location of equipment, or a line, used in connection with a communication	Typically nil	Typically nil	Typically nil

Annexure D – Glossary

ACMA	Australian Communications and Media Authority
AFP	Australian Federal Police
AGD	Attorney-General's Department
ASIO	Australian Security Intelligence Organisation
CAC	Communications Access Co-ordinator
C/CSP	Carriers and Carriage Service Providers
CSP	Carriage Service Provider
ETSI	European Telecommunications Standards Institute
EUDRD	European Union Data Retention Directive
IP	Internet Protocol
IPTV	Internet Protocol television
ISP	Internet Service Provider
IWG	Data Retention Implementation Working Group
MAC	Media Access Control
NAT	Network Address Translation
OTTs	Over-the-top services
PJCIS	Parliamentary Joint Committee on Intelligence and Security
PwC	PricewaterhouseCoopers
Report	Report 1 of the Data Retention Implementation Working Group
TIA Act	*Telecommunications (Interception and Access) Act 1979*
VoIP	Voice over Internet Protocol
Wi-Fi	Local area wireless technology