Data Retention Bill – Proposed data set

The Australian Government has introduced a Bill to oblige telecommunications providers to retain a limited set of telecommunications data ('metadata') for two years.

It is not the content or substance of a communication and it is not a person's web-browsing history. Agencies will continue to need to obtain a warrant to access the content of a communication.

The categories of data that industry will be asked to retain is set out in the legislation. The categories of data are based closely on the European Union Data Retention Directive. Regulations will provide further details about what is to be collected and greater technical specificity under each of these categories. This will enable flexibility as technology changes and provide more certainty and consistency for industry. The regulations will also limit the retention of subscriber information described in item 1 (c)-(f) to two years from creation of that data.

The draft set has been released publicly with the Bill and referred to the Parliamentary Joint Committee on Intelligence and Security for review and public consultation. There will also be ongoing consultation and review with a joint government/industry Expert Working Group, which has been set up to settle implementation, the data set and funding of the scheme.

Kinds of information to be kept

Matters to which information must relate	**Draft 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 service, or to any related 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;	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 person's identity or link a service or account to a person. 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 allocated to an internet access account or service. This category further includes billing and payment information. This can be a valuable source of information for law enforcement agencies. For example, even if someone has lied about other identifying details, it is more difficult to falsify 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. Information about metrics relating to the relevant service, such as available bandwidth, or historic aggregate upload and download volumes, is useful in law

Matters to which information must relate	Draft data set	Explanation and examples
	(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; (f) any information about metrics of the relevant service or a related account, service or device.	enforcement and national security investigations. For example, it allows agencies to better allocate resources in support of warrants where more intrusive surveillance is justified. For instance, if a suspect regularly downloads large volumes of information, agencies may need to assign additional system resources when provisioning a warrant.
2. The source of a communication	Any identifiers of a related account, service or device from which the communication has been sent by means of the relevant service.	The source of a communication includes the phone from which a call was made, the account from which an email was sent or the IP address allocated to a person connected to the internet.
3. The destination of a communication	Any 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.	The destination of a communication is the recipient. For example, destination includes the phone number that received a call or SMS. This will include destinations for online services, such as the user name, number and/or IP address of the recipient of a Voice over IP (VoIP) call. 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 person has browsed.
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): (a) the start of the communication; (b) the end of the communication; (c) the connection to the relevant service; (d) 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 – this may last from a few hours to several days.
5. The type of communication or 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 enabled for the communication. Examples: call waiting, call forwarding, bandwidth allowances.	The type of communication means the form of the communication (for example voice call vs. internet usage). The type of the relevant service provides more technical detail about the service. For example, for a mobile voice service, whether it is a GPRS or VoLTE service. Note: This item will only apply to the service provider operating the relevant service: see paragraph 187A(4)(c) of the Act.

Matters to which information must relate	Draft data set	Explanation and examples
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.	Location records will be limited to the location of a device at the start and end of a communication, such as a phone call or SMS message. Paragraph 187A(7) of the Bill provides that two or more communications that together constitute a single communications session are taken to be a single communication. In relation to internet access sessions, this means that service providers will only be required to keep location records at the start and end of a session, which can last from a few hours to a several days. Paragraph 187A(4)(e) of the Bill provides that locations records are limited to information that is used by a service provider in relation to the relevant service. This would include information such as which cell tower, Wi-Fi hotspot or base station a device was connected to at the start and end of communication. As a result of the above, the location records to be kept by service providers will not allow continuous monitoring or tracking of devices. Precise or real-time location information, such as a GPS location is also not part of data retention.