Capability/Data, - Authorisation, Collection Reporting and Oversight

Name of Capability/Data	What data is obtained	How request is made	What is the legal authority underpinning request	Authorising Officer	Qualifying Legal Threshold	Who request is served on (if anyone)	Duration/Period of authority:	Data Retention Timeframes	Reporting and Oversight
Metadata	The subscriber information including name, address or contact details. Information about accounts, telecommunications devices or other relevant services. Contract information. Billing or payment information. Source of communication Destination of communication Date, time and duration of communication Type of communication (ie voice, SMS) Location of equipment when communication is made.	Method of requests varies depending on the request.	*Telecommunication (Interception and Access) Act 1979* s178 s179 s178A	Members authorised under s5AB(1) being Superintendent and above	Necessary for the enforcement of the criminal law. Necessary for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue Necessary for the purposes of finding a person who the AFP, or a Police Force of a State, has been notified is missing.	Telecommunications provider.	N/A	Varies depending on the provider.	Annual report to AGD
Integrated Public Number Database (IPND) *The reliability of the results is dependent on the timely entry of data by the individual carriers*	Subscriber information Date service connected / disconnected Type of service	Requests are actioned centrally within TID and via an online portal managed by Telstra.	*Telecommunication (Interception and Access) Act 1979* s178 s179 s178A	Members authorised under s5AB(1) being Superintendent and above	Necessary for the enforcement of the criminal law. Necessary for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue Necessary for the purposes of finding a person who the AFP, or a Police Force of a State, has been notified is missing.	N/A	N/A	Varies depending on the provider.	Annual report to AGD
Call Charge Records (CCR)	Provides details of outgoing phone calls made by a targeted phone service during a nominated period.	Requests are actioned centrally within TID	*Telecommunication (Interception and Access) Act 1979* s178 s179 s178A	Members authorised under s5AB(1) being Superintendent and above	Necessary for the enforcement of the criminal law. Necessary for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue Necessary for the purposes of finding a person who the AFP, or a Police Force of a State, has been notified is missing.	Telecommunications provider	N/A	Varies depending on the provider.	Annual report to AGD
Reverse CCR	Provides details of all incoming calls to a nominated target phone number.	Requests are actioned centrally within TID	*Telecommunication (Interception and Access) Act 1979* s178 s179 s178A	Members authorised under s5AB(1) being Superintendent and above	Necessary for the enforcement of the criminal law. Necessary for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue Necessary for the purposes of finding a person who the AFP, or a Police Force of a State, has been notified is missing.	Telecommunications provider	N/A	Varies depending on the provider.	Annual report to AGD
Subscriber Check	Provides details on the customer name, address, billing address, service number, connection/disconnection information.	Requests are actioned centrally within TID	*Telecommunication (Interception and Access) Act 1979* s178 s179	Members authorised under s5AB(1) being Superintendent and above	Necessary for the enforcement of the criminal law. Necessary for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue	Telecommunications provider	N/A	Varies depending on the provider.	Annual report to AGD

Name of Capability/Data	What data is obtained	How request is made	What is the legal authority underpinning request	Authorising Officer	Qualifying Legal Threshold	Who request is served on (if anyone)	Duration/Period of authority:	Data Retention Timeframes	Reporting and Oversight
Prospective Data Call Associated Data (CAD) Location Based Services – SEEK (Telstra), LBS (Optus)	Source of communication Destination of communication Date, time and duration of communication Type of communication (ie voice, SMS) Location of equipment when communication is made.	2 options - physically signed and scanned or electronically approved and emailed	*Telecommunication (Interception and Access) Act 1979* s180	Members authorised under sSAB(1) being Superintendent and above	An offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years.	Telecommunications provider	Maximum of 45 days	N/A	Annual report to AGD
TI Service Warrant TI Device Warrant Issued under s46	Call content Source of communication Destination of communication Date, time and duration of communication Type of communication (ie voice, SMS) Location of equipment when communication is made.	Authorised warrant is scanned and emailed to TID TID faxes warrant to the carrier together with a cover letter.	*Telecommunication (Interception and Access) Act 1979* Part 2-5	Warrant can be authorised by an Eligible Judge or Nominated AAT member	The offence must be considered a 'serious offence' which is an offence punishable by imprisonment for at least 7 years.	Telecommunications provider	Maximum of 90 days	N/A	Annual report to AGD Inspected by the Commonwealth Ombudsman biannually.
TI Named Person Warrant Issued under s46A	Call content Source of communication Destination of communication Date, time and duration of communication Type of communication (ie voice, SMS) Location of equipment when communication is made.	Authorised warrant together with signed notifications for each intercepted service (or device) is scanned and emailed to TID TID faxes warrant and notification to the carrier together with a cover letter.	*Telecommunication (Interception and Access) Act 1979* Part 2-5	Warrant can be authorised by an Eligible Judge or Nominated AAT member Notifications are authorised by Commander level and above.	The offence must be considered a 'serious offence' which is an offence punishable by imprisonment for at least 7 years.	Telecommunications provider	Maximum of 90 days	N/A	Annual report to AGD Inspected by the Commonwealth Ombudsman biannually.
TI B-Party Warrant Issued under s46 Interception of a service where it is believed the target will make contact ie the service owner is not being investigated.	Call content Source of communication Destination of communication Date, time and duration of communication Type of communication (ie voice, SMS) Location of equipment when communication is made.	Authorised warrant is scanned and emailed to TID TID faxes warrant to the carrier together with a cover letter.	*Telecommunication (Interception and Access) Act 1979* Part 2-5	Warrant can be authorised by an Eligible Judge or Nominated AAT member	The offence must be considered a 'serious offence' which is an offence punishable by imprisonment for at least 7 years.	Telecommunications provider	Maximum of 45 days	N/A	Annual report to AGD Inspected by the Commonwealth Ombudsman biannually.
International Mobile Equipment Identity (IMEI) – Unique handset identifier	Regardless of SIM card used in mobile device – Call content Source of communication Destination of communication Date, time and duration of communication Type of communication (ie voice, SMS) Location of equipment when communication is made.	Authorised warrant is scanned and emailed to TID TID faxes warrant to the carrier together with a cover letter.	*Telecommunication (Interception and Access) Act 1979* Part 2-5	Warrant can be authorised by an Eligible Judge or Nominated AAT member	The offence must be considered a 'serious offence' which is an offence punishable by imprisonment for at least 7 years.	Telecommunications provider	Maximum of 90 days	N/A	Annual report to AGD Inspected by the Commonwealth Ombudsman biannually.
International Mobile Subscriber Identity (IMSI) – Unique SIM card identifier	Regardless of handset used – Call content Source of communication Destination of communication Date, time and duration of communication Type of communication (ie voice, SMS) Location of equipment when communication is made.	Authorised warrant is scanned and emailed to TID TID faxes warrant to the carrier together with a cover letter.	*Telecommunication (Interception and Access) Act 1979* Part 2-5	Warrant can be authorised by an Eligible Judge or Nominated AAT member	The offence must be considered a 'serious offence' which is an offence punishable by imprisonment for at least 7 years.	Telecommunications provider	Maximum of 90 days	N/A	Annual report to AGD Inspected by the Commonwealth Ombudsman biannually.
Preservation Notices Historic	All stored communications held by the carrier relating to the person or service of interest at the time the notice is received by the carrier.	Authorised preservation notice is scanned and emailed to TID TID faxes preservation notice to the carrier together with a cover letter.	*Telecommunication (Interception and Access) Act 1979* Domestic Preservation Notices under s107H	Historic preservation notices can be authorised by any sworn member.	The offence must be considered a 'serious offence' which is an offence punishable by imprisonment for at least 7 years, or a 'serious contravention' punishable by imprisonment for at least 3 years.	Telecommunications provider	Stored communications are held for 90 days	Varies depending on the provider.	Annual report to AGD Inspected by the Commonwealth Ombudsman annually.

Name of Capability/Data	What data is obtained	How request is made	What is the legal authority underpinning request	Authorising Officer	Qualifying Legal Threshold	Who request is served on (if anyone)	Duration/Period of authority:	Data Retention Timeframes	Reporting and Oversight
Preservation Notices Ongoing	All stored communications held by the carrier relating to the person or service of interest at the time the notice is received by the carrier as well as any new communications received until the end of the 29th day of the carrier receiving the notice.	Authorised preservation notice is scanned and emailed to TID TID faxes preservation notice to the carrier together with a cover letter.	*Telecommunication (Interception and Access) Act 1979* Domestic Preservation Notices under s107H	Ongoing preservation notices can be authorised by Superintendent or above, or a member acting in that position who holds a declaration of rank.	The offence must be considered a 'serious offence' which is an offence punishable by imprisonment for at least 7 years, or a 'serious contravention' punishable by imprisonment for at least 3 years.	Telecommunications provider	Stored communications are held for 90 days	Varies depending on the provider.	Annual report to AGD Inspected by the Commonwealth Ombudsman annually.
Stored Communications	All stored communications held by the carrier relating to the person or service of interest at the time the notice is received by the carrier.	Authorised warrant is scanned and emailed to TID TID faxes warrant to the carrier together with a cover letter.	*Telecommunication (Interception and Access) Act 1979* s116	Warrant can be authorised by an Eligible Judge or Nominated AAT member	The offence must be considered a 'serious offence' which is an offence punishable by imprisonment for at least 7 years.	Telecommunications provider	A stored communications warrant remains in force until: • It is first executed; or • 5 days after the date of issue.		
Surveillance Device Warrant: Listening Device Optical Device Data Device Tracking Device	Audio Visual Data Location information	Authorised warrant is scanned and emailed to TID Case officer liaises with TCD and TSO to commence surveillance	*Surveillance Devices Act 2004* Warrant issued under s16	Warrant can be authorised by an Eligible Judge or Nominated AAT member	The offence must be considered a 'relevant offence' which is an offence punishable by imprisonment for at least 3 years.	N/A	Maximum of 90 days however can be extended.	N/A	Annual report to AGD Inspected by the Commonwealth Ombudsman biannually.
Tracking Device Authorisation	Location information	Tracking Device Authorisation is scanned and emailed to TID Case officer liaises with TCD and TSO to commence surveillance	*Surveillance Devices Act 2004* Tracking Device Authorisation issued under s39	Tracking Device Authorisations can be authorised by Commander level and above.	The offence must be considered a 'relevant offence' which is an offence punishable by imprisonment for at least 3 years.	N/A	Maximum of 90 days.	N/A	Annual report to AGD Inspected by the Commonwealth Ombudsman biannually.
Tactical Wireless	Location information	Tracking Device Authorisation is scanned and emailed to TID Case officer liaises with TCD and TSO to commence surveillance	*Surveillance Devices Act 2004* Tracking Device Authorisation (TDA) issued under s39	TDA's can be authorised by Commander level and above.	The offence must be considered a 'relevant offence' which is an offence punishable by imprisonment for at least 3 years.	N/A	Maximum of 90 days	N/A	Annual report to AGD Inspected by the Commonwealth Ombudsman biannually.