E

Appendix E – Framework for Access to Communications in Australia

	Disclosure of Historic Non-Content Data	Prospective Disclosure Non-Content Data	Stored Communications	Telecommunications Interception
What type of information	Information about communications (but not the content of the communications themselves). The information is created in the course of a carrier's business and is in existence	The same information as historic non-content data. However, rather than authorising the disclosure of information in the carrier's possession, the authorisation enables the additional disclosure of	Stored communications are 'communications' that are stored on the equipment of carriers, are accessible by the intended recipient of the communication and can only be accessed with the	Telecommunications interception is the real-time copying or recording of information that is passing over a telecommunications system. It can be by way of a fixed landline, mobile communication or

	Disclosure of Historic Non-Content Data	Prospective Disclosure Non-Content Data	Stored Communications	Telecommunications Interception
	at the time the disclosure is authorised. It includes details about subscribes and billing and assists agencies establish who uses a service, the parties to a communication, when it was sent and received and sometimes their location.	information which comes into existence for an ongoing period.	assistance of the employee of a carrier. These communications include sent emails and sms messages as well as voicemail messages.	communications via computer networks.
Threshold for access	Either: • Security (as defined in the ASIO Act) • the enforcement of the criminal law • the enforcement of a law imposing a pecuniary penalty, or • the protection of the public revenue	Either: • Security, or • The investigation of an offence with a penalty of at least three years' imprisonment	Either: • Security, or • An offence for which telecommunications interception is available, • An offence with a penalty of at least three years' imprisonment, • An offence with a penalty of 180 penalty units for an individual, or 900 penalty units for a body corporate	Either: • Security, or • A 'serious offence', in section 5D of the Interception Act. They generally carry a penalty of at least seven years' imprisonment, however there are exceptions. Offences are included within the regime on a case-by-case amendment

	Disclosure of Historic Non-Content Data	Prospective Disclosure Non-Content Data	Stored Communications	Telecommunications Interception
Who can access it	An 'enforcement agency', as defined in section 5 of the Interception Act (an agency with the above functions). These can be Federal, State or Local Government agencies.	ASIO, or a 'criminal law enforcement agency', as defined in the Interception Act. There are both Federal and State criminal law enforcement agencies.	ASIO, or an enforcement agency.	ASIO and 16 other Commonwealth and State agencies. Commonwealth agencies are defined in the Act and State agencies are authorised by a declaration made by the Attorney-General.
How can it be accessed	The agency provides an authorisation to the carrier that holds the information authorising the disclosure of the information. For ASIO, authorisations can be made by the Director-General, Deputy Director-General or an employee authorised by the Director-General. For enforcement agencies, authorisations can be made by a person in a	The agency provides an authorisation to the carrier that holds the information authorising the disclosure of the information. For ASIO, authorisations can be made by the Director-General, Deputy Director-General or an authorised employee at the equivalent level of SES Band 2. For criminal law enforcement agencies,	An enforcement agency must apply to a Federal Judge or Magistrate, or a Nominated AAT Member for a warrant which authorises access to any stored communications held by the carrier that relate to the person named in the warrant. ASIO obtain access to stored communications as part of their telecommunications interception warrants. They do not have a	Telecommunications interception is authorised by way of a warrant. Warrants for law enforcement agencies are issued by a Judge of a Federally-created court that has consented to issue warrants. Warrants for ASIO are issued by the Attorney-General.

	Disclosure of Historic Non-Content Data	Prospective Disclosure Non-Content Data	Stored Communications	Telecommunications Interception
	management position or management office authorised by the agency head.	authorisations can be made by a person in a management position or management office authorised by the agency head.	separate means of access.	
Set out in	Interception Act – Chapter 4	Interception Act – Chapter 4	Interception Act – Chapter 3	Interception Act – Chapter 2