Data Retention Amendments

Telecommunications (Interception and Access) Act 1979

Came into force: 13 October 2015

Summary

- New requirements for ACLEI authorised officers
  - Authorisation thresholds
  - Journalist warrants
  - Ombudsman oversight
  - Reporting Requirements

The Data Set

- Carriers and ISPs must retain **six** kinds of information for **two years** (unless exempted):
  1. **Subscriber** and other relevant service-level account information
  2. **Source** of a communication
  3. **Destination** of a communication (not applicable to internet access service providers)
  4. The **date**, **time** and **duration** of a communication
  5. The communication **type**
  6. The **location** of communication equipment

What Changes?

(1) New threshold for accessing telecommunications data under s 178 and s 180 of the TIA Act

(2) New Journalist Information Warrants

(3) New record-keeping and reporting requirements

(4) New oversight: inspections by Cth Ombudsman

When? 13 October 2015

Issuing Authorisations

- ACLEI positions designated as 'authorising officers' under s5AB(1) of the TIA Act:
  - Executive Director
  - Director Intelligence
  - Director Investigations
  - Directory Sydney Taskforce
- s178 – authorise disclosure of **existing information**
  - Subscriber checks, IPND, call charge records
  - Other information
- s180 – authorise disclosure of **prospective information**
  - Call-associated Data (CAD), Location Based Service (LBS)

Existing requirements

- s178 - You must be satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law
- ss178A, 179 - reasonably necessary missing person/pecuniary penalty
- s180 – You must be satisfied that the disclosure is reasonably necessary for the investigation of a "serious offence" or a Cth/State/Territory law that is punishable by imprisonment for at least 3yrs.

Privacy Considerations: s 180F

- **Before** making an authorisation you must be satisfied on reasonable grounds that any interference with the privacy of any person(s) is justifiable and proportionate, having regard to:
  - (aa) the gravity of any conduct in relation to which the authorisation is sought, including:
    - The seriousness of the offence/pecuniary penalty/public revenue/missing person;
  - The likely relevance and usefulness of the information; and
  - The reason for the disclosure.
- Authorisations must include a statement that you are satisfied as to the matters in s 180F
- Records **must** be kept to demonstrate that authorisations were properly made

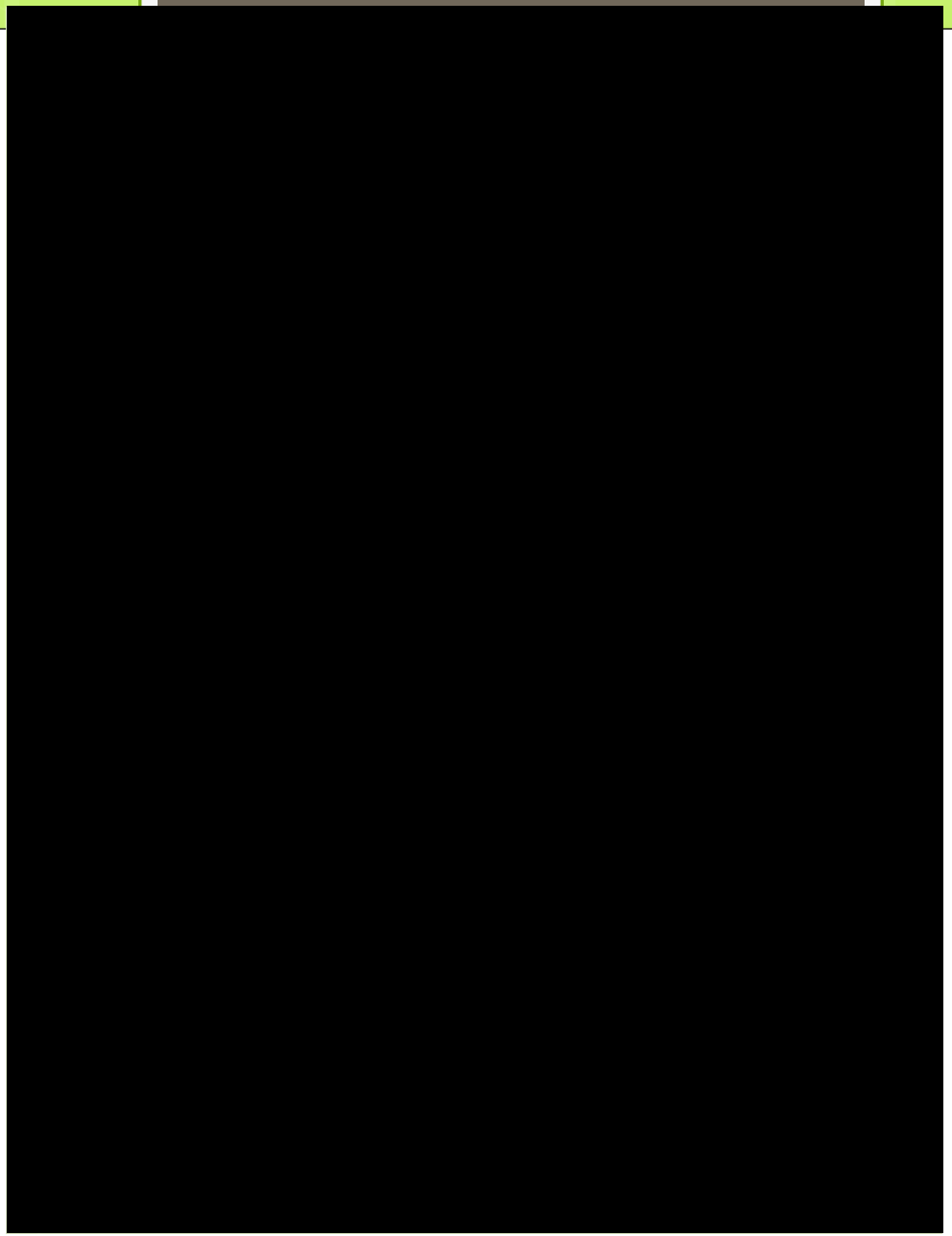
ACLEI's Approach

- ☞ **NEW TEMPLATES** for s 178 and 180 Requests
- Investigating officers will also need to complete an accompanying minute (there is a template for this too)
  - Grounds which justify the granting of an authorisation (i.e. reasonably necessary criminal law/serious offence/pecuniary penalty/missing person)
  - Address the privacy considerations – sufficient information to justify any privacy interference

Template - Internal Minute (1/3)

Template - Internal Minute (3/3)

Request Template– to service providers



Ombo Oversight: Section 178 and 180 record keeping

- 186A: Obligation to keep records in relation to Authorisations made under section 178 and 180:
  - Each Authorisation
  - Whether Authorisation/Revocation was properly made
  - Use and Disclosure of information obtained under Authorisation
  - Evidentiary Certificates

Use and disclosure of data

- Still the same: Data can be lawfully used or disclosed when “reasonably necessary for the enforcement of the criminal law”
- What **has** changed is the need to keep records (“documents or other materials”) when this occurs
- The Ombudsman will inspect these records
- Ombudsman has indicated we do not need to record use once we have disclosed to an external agency.

Data sent to ACLEI by mistake

- Follow same process as for TI content i.e. product is quarantined and a record is made of this information to enable self-disclosure to the Commonwealth Ombudsman inspectors at inspection time.

Journalist Information Warrants

- You must **not** authorise the disclosure of information (under s 178 or s 180) relating to a particular person if:
  - You know or reasonably believe that they are a journalist or the employee of a journalist; and
  - The purpose of making the authorisation is to identify a journalist source

- **Key point: If the purpose of a request is to identify a journalist's source, you must obtain a Journalist Information Warrant**

Journalist Information Warrants

- Warrants are issued by a nominated AAT member or eligible judge to officers who are eligible to apply for interception warrants
- Public Interest Advocates are able to make submissions to an issuing authority on behalf of a journalist

Other Requirements:

- IC must as soon as practicable provide to the Ombudsman.
  - A copy of the journalist information warrant
- IC may revoke a journalist warrant and must do so if satisfied that the grounds on which the warrant was issued to the agency have ceased to exist.
- Annual reporting obligations

Administrative Procedures

- [redacted] – all records from each authorisation, whether successful or not, are to be given to [redacted] for filing.

Full extent of Ombo oversight: record keeping

- Preservation notices
- Stored communication warrants and supporting documents
- Telecommunications data authorisations
- Revocation notices
- Requests for mutual assistance in relation to TI material
- A range of procedural documents showing that authorisations properly made, access to TI material lawful, disclosure of TI material lawful
- Evidentiary certificates
- Documents identifying authorised officers
- Annual reports
- Material for Journo Info Warrants and related PIA materials

New Reporting Requirements: Annual Report

- Currently we only report the number of authorisations issued for the year
- New reporting requirements
  - Offences and other matters for which authorisations were made (there is a 'bribery or corruption' category)
  - The age of data sought under an authorisation
  - Number of authorisations for 'subscriber' information
  - Number of authorisations for 'traffic' information
  - Number of journalist information warrants
  - Costs incurred – data authorisations

Additional Record Keeping: 2020 Review

- Parliamentary Joint Committee on Intelligence and Security to review the data retention scheme, commencing in 2019 and concluding in 2020.
- All oversight and annual report documents must be kept until the conclusion of the review.
- Will need to keep additional information which will help the PJCIS test the effectiveness of the whole scheme. AGD still deciding what this information should be.