

# **COMMUNICATIONS DATA**

Metadata created as a result of a communication. It includes subscriber information; source and destination; date, time and duration; type of communication; type of service used



#### DATA: AUTHORISATIONS, NOT WARRANTS

## 2 types of authorisations

- Existing: data which already exists at the time the authorisation is given
- Prospective: data which comes into existence during the period for which the authorisation is in force. Single authorisation may also authorise existing data.

#### 'Authorised officers' can issue authorisations

- Section 5AB authorised officers
- EDs, Director Intel, Investigations, Sydney

### Thresholds

Higher threshold for prospective than existing



### DATA: AUTHORISATION THRESHOLDS

Existing Data	Prospective Data
Disclosure is reasonably necessary for the enforcement of the criminal law (s 178)	Disclosure is reasonably necessary for the investigation of a serious offence, or a 3-year offence (s 180)
AND	AND
Privacy considerations (s 180F)	Privacy considerations (s 180F)



#### DATA: PRIVACY CONSIDERATIONS

The authorised officer must be satisfied on reasonable grounds that any interference with the privacy of any person(s) is justifiable and proportionate, having regard to:

- the gravity of any conduct in relation to which the authorisation is sought, including the seriousness of the offence
- ■The likely relevance and usefulness of the information; and
- •The reason for the disclosure.

Authorisations must include a statement section 180F is satisfied.

Records must be kept to demonstrate that authorisations were properly made.



#### DATA: AUTHORISATION PROCESS

1. Complete an internal authorisation request and get it approved by an authorised officer

2. Authorised officer will produce an external minute to the carrier (unless it is an IPND check, in which case the Director Strategic Intel executes this)

3. For existing data, the case officer will liaise with the carrier. For prospective, the Assistant Director Operation Support will do so via the AFP.

4. ACLEI receives the



#### DATA: USE AND DISCLOSURE

Offence

- Disclosing the data itself (ss 276, 277 TA)
- Disclosing information which would reveal the existence of a data authorisation ( s 181B TIA Act)

**Exemptions** 

- Disclosure or use is for the purpose of the relevant authorisation, revocation or notification
- Disclosure or use is reasonably necessary for the enforcement of the criminal law (s 181B)

Who?

 No limitation on who may receive information