

Overview

MinterEllison

3

Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)

'to facilitate access to communications and data, for the purpose of disrupting and investigating criminal activity and threats to national security'

achieves this by
enabling lawful access
via



Decryption
(Schedule 1)

and



Access where data
is not encrypted
(Schedules 2-5)

4



Schedule 1 Industry Assistance

MinterEllison

Provides for industry assistance (voluntary or ordered) to do 'listed acts or things' including:

- Removing electronic protection
- Providing technical information
- Formatting information
- Facilitating access to devices
- *and other things*

Amends

- *Telecommunications Act 1997*
- *Criminal Code Act 1995*

Enforcement

- Criminal & Civil

Executed by

- ASIO, ASD, ASIS *and*
- 'interception agencies'

5

SAFEGUARDS

- The introduction of '*systemic weakness*' or '*systemic vulnerability*' is prohibited, including lessening the effectiveness of encryption / authorisation
- An underlying TIA warrant or authorisation required to access data
- Core interception and data retention will not be extended
- Industry must be consulted about new capabilities
- Any request/notice must be reasonable, proportionate, practicable & technically feasible
- Information is protected

6



Schedule 2 Computer Access Warrants

MinterEllison

Expands the powers available under *computer access warrants*:

- to *interception agencies*
- removes requirement to identify service or person
- allows remote collection of data
- may remove things from premises
- concealment upon expiry of warrant
- provides for use of force
- increased penalties
- redefines 'computer'
- introduces assistance orders

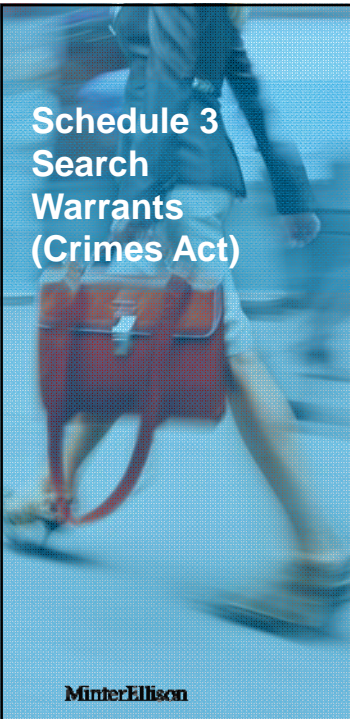
Amends

- *ASIO Act 1979*
- *TIA Act 1979*
- *Surveillance Devices Act 2004*
- *Mutual Assistance in Criminal Matters Act 1987*

Safeguards

- Matters to be considered
- Relevant offence
- Appropriate undertakings
- Reporting & record keeping

7



Schedule 3 Search Warrants (Crimes Act)

MinterEllison

Amends the search warrant framework to enhance the ability to collect evidence:

- *Access to account based data (eg Gmail, Facebook, any user id)*
- person based warrants
- *assistance orders* in the ordinary search of a person
- remove and conceal
- increased penalties

Amends

- *Crimes Act 1914*

Safeguards

- Independent (judiciary) approval is required
- Interference not authorised
- Thresholds apply

8



**Schedule 4
Search
Warrants
(Customs Act)**

**Schedule 5
ASIO
Assistance
Powers**

MinterEllison

Schedule 4 - Customs

- Aligns Customs search warrants and action to the *Crimes Act 1914* (as amended by Schedule 3)
- Person based warrants (assistance orders)

Safeguards

- as per Schedule 3

Schedule 5 - ASIO

- Civil liability protections for voluntary assistance
- Assistance requests (overlap between Schedule 1 TAR)

Safeguards

- AG must be satisfied collection is important to national security

9

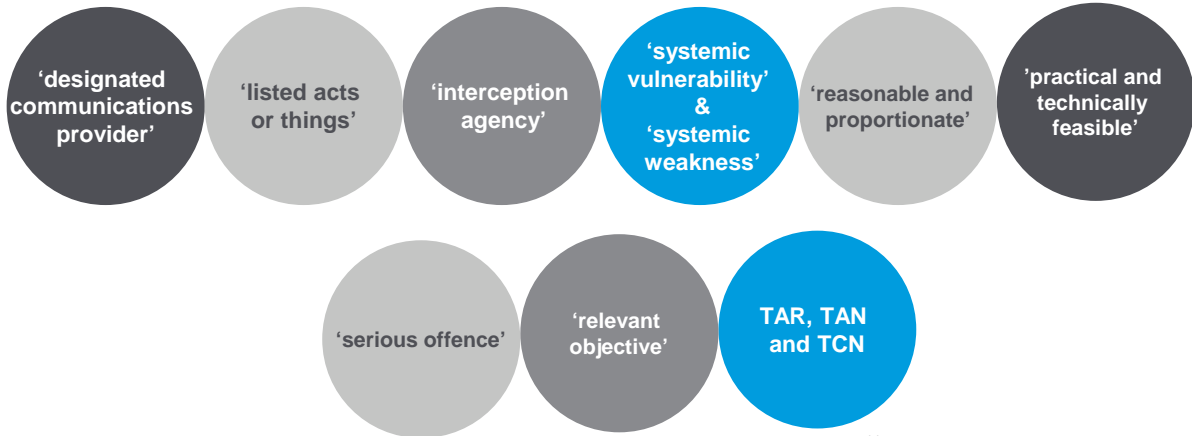


Key terms

MinterEllison

10

Key Terms



11

S 317C

'Designated Communications Provider'

- Carriage or carriage service providers and their intermediaries,
- Electronic service providers and their ancillary service providers,
- Person who manufactures, supplies, installs, operates a facility, and similarly for components likely to be used in a facility,
- Person who manufactures, supplies, installs or maintains customer equipment, and similarly for components used in customer equipment,
- *Constitutional corporations* who manufacture, supply, install, maintain equipment, or software installed on a device that can connect to a network in Australia.

12

S 317E
'listed acts or things'

- Removing electronic protection,
- Providing technical information,
- Installing, maintaining, modifying, developing, testing or using software or equipment,
- Reformatting information,
- Facilitating access to any of the eligible activities of the DCP,
- Facilitating the modification of any characteristics of the DCP,
- Facilitating substitution of a service provided by a DCP,
- An act or thing done to conceal the fact that any thing has been done covertly.

13

S 317B
'interception agency'

- Australian Federal Police,
- Australian Crime Commission,
- Any State or Territory Police Force
- In addition to:
 - ASIO
 - Australian Secret Intelligence Service
 - Australian Signals Directorate

14

‘serious
Australian
offence’

‘relevant
objective’

- An offence punishable by 3 more more years imprisonment
 - Tax evasion, theft, bankruptcy, directors duties
- Safeguarding national security
- Interests of Australia's national economic well being
- Interests of Australia's foreign relations
- Serious Australian or foreign offences

15

Schedule 1 Requests & Notices

- **Technical Assistance Request (TAR):** a request for a DCP to *voluntarily* do acts or things
- **Technical Assistance Notice (TAN):** *requiring* a DCP to do acts or things
- **Technical Capability Notice (TCN):** *requiring* a DCP *to build a new capability*

To assist the issuing agency perform functions that related to:

- Enforcing serious criminal laws of Australia or of a foreign country, or
- Australia's foreign relations, national economic well-being or national security, or
- Matters that facilitate or are ancillary to such matters

s 317ZB

Prohibition on building:
systemic weaknesses &
systemic vulnerabilities

MinterEllison

- A notice *must not* have the effect of requiring a designated communications provider to implement or build a *systemic weakness*, or a *systemic vulnerability*, into *a form of electronic protection*, and must not prevent the provider from rectifying such a weakness or vulnerability.
- Any act or thing that would likely create a *material risk* that otherwise secure information held by any other person can be accessed by an unauthorised third party.
- *Does not apply* to actions that weaken a form of electronic protection on a particular device.

17

s 317ZAA

Matters to be considered in assessing
'reasonable and proportionate'

MinterEllison

- A request or notice *must not* be given unless the requirements are *reasonable and proportionate* and compliance with the notice is *practicable and technically feasible*.
- Matters to be considered in assessing *reasonable and proportionate*
 - Interests of national security,
 - Legitimate interests of the DCP,
 - Availability of other means to achieve the purpose,
 - Legitimate expectations of the Australian community, and
 - Other relevant matters (S 317ZAA).
- No guidance for *practicable and technically feasible*, however notices require prior consultation (although no merit review).

18



Compliance and enforcement

- **Schedule 1 Notices**
 - S 317ZB Failure to comply with notices
 - \$10 million body corporate, \$50,000 individuals
 - S 317ZF Unauthorised disclosure of information
 - Maximum penalty - 5 years imprisonment
- **Schedule 2 - 5 Assistance orders**
 - Failure to comply
 - Maximum penalty - 5 or 10 years imprisonment and/or
 - Fine of \$63,000 or \$126,000 (\$315,000 or \$630,00 for corporations)



Relevant matters



Frequently asked questions

MinterEllison



- Does the Act put organisations in breach of GDPR?
- Can an employee with access to systems and capability be compelled without alerting their employer?
- Does the Act only apply to companies located in Australia?
- What about warrant canaries?

21



Comparisons

MinterEllison



- UK Investigatory Powers Act 2016
- NZ Telecommunications (Interception Capability and Security) Act 2013
- Australia the default Five Eye jurisdiction?

22

Crypto Wars

- 1990's encryption export restrictions
 - Clipper chip & key escrow
 - Netscape 'international edition'
- What happened after controls were lifted?
- *'encryption is more about keeping the bad guys out than letting the good guys in'*
- Secrets are hard to keep



MinterEllison

23

Concluding comments

- The Act introduces more capability for agencies to disrupt and investigate criminal activity
- The use of industry assists agencies keep up with the range of technology used to facilitate criminal activity
- The Act may be drafted more broadly than required to meet its objectives
- Safeguards and accountability mechanisms could be strengthened

MinterEllison

24

Thank you



Associate

T +61 2 9921 4811

M +61 421 865 841

EMAIL kit.loyd@minterellison.com

MinterEllison

25



26