Australian Government | acma

Australian Communications and Media Authority

Telecommunications law enforcement and national security obligations: Monitoring industry performance

DECEMBER 2020

Canberra
Red Building
Benjamin Offices
Chan Street
Belconnen ACT

PO Box 78
Belconnen ACT 2616

T +61 2 6219 5555
F +61 2 6219 5353

Melbourne
Level 32
Melbourne Central Tower
360 Elizabeth Street
Melbourne VIC

PO Box 13112
Law Courts
Melbourne VIC 8010

T +61 3 9963 6800
F +61 3 9963 6899

Sydney
Level 5
The Bay Centre
65 Pirrama Road
Pyrmont NSW

PO Box Q500
Queen Victoria Building
NSW 1230

T +61 2 9334 7700 or 1800 226 667
F +61 2 9334 7799

Contents

Overview

This is a report for 2019–20 from the Australian Communications and Media Authority (ACMA) about:

- the operation of Part 14 (national interest matters) of the *Telecommunications Act 1997* (the Telecommunications Act) and the associated compliance costs[1]
- the costs of complying with Part 5-1A (data retention) of the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

We are required to report on these matters under subsection 105(5A) of the Telecommunications Act.

This report includes information about:

- how carriers, carriage service providers and carriage service intermediaries (telcos) support and assist law enforcement and national security agencies by:
  - providing reasonably necessary assistance
  - suspending carriage services in an emergency
  - developing, installing and maintaining interception capabilities
  - complying with the data retention regime.
- the costs of complying with Part 5-3 (interception capability) of the TIA Act.

[1] Under subsection 105(5B) of the Telecommunications Act, the ACMA is not required to monitor or report on the operation of the sections of Part 14 amended by the *Telecommunications and Other Legislation Amendment Act 2017*. This means the ACMA is not required to report on the matters set out in section 315J, which relate to the telecommunications sector security reforms.

Support for law enforcement and national security agencies

Among other matters, Part 14 of the Telecommunications Act requires telcos to do their best to prevent telecommunications networks and facilities from being used to commit offences. Telcos must also help law enforcement and national security agencies where reasonably necessary for specific purposes. Telcos may also suspend the supply of a service in an emergency if requested to do so by a senior police officer under Part 14 of the Telecommunications Act.

The Department of Home Affairs reports on the matters set out in section 315J of the Telecommunications Act, which relate to the telecommunications sector security reforms.

Reasonably necessary assistance

Telcos must provide law enforcement and national security agencies with reasonably necessary assistance under subsections 313(3) and (4) of the Telecommunications Act. This usually involves providing information about consumers and their communications, for the purposes of:

- enforcing the criminal law
- enforcing laws that impose a pecuniary penalty
- assisting the enforcement of the criminal laws in force in a foreign country
- protecting the public revenue
- safeguarding national security.

We may assess compliance with section 313 of the Telecommunications Act through compliance assessments or investigations, undertaken in response to:

- a referral from the Department of Home Affairs
- complaints from law enforcement agencies.

In 2019–20, we did not receive any complaints or referrals[2] to investigate telco non-compliance with obligations under subsections 313(3) or (4) of the Telecommunications Act.

Cost of providing assistance

If a telco is required to give help to a law enforcement or national security agency under subsections 313(3) or (4) of the Telecommunications Act, it must do so on the basis that it does not profit from, or bear the cost of, that help.[3] Telcos provide such assistance on the terms and conditions agreed with the relevant Commonwealth, state or territory authority.

[2] Referrals would usually come from the Communications Access Co-ordinator located within the Department of Home Affairs as it is the central liaison point between telcos and law enforcement and national security agencies.

[3] Section 314 of the Telecommunications Act.

Lawful disruption of online services

Subsection 313(3) enables Australian and state and territory government agencies to request telcos that are internet service providers to provide assistance as reasonably necessary to disrupt access to illegal online services by blocking access to websites in connection with any of the purposes set out in paragraph 313(3)(c)–(e) of the Telecommunications Act.

In making requests, Australian government agencies[4] are expected to follow the whole-of-government guidelines released in June 2017 – Guidelines for the use of section 313(3) of the Telecommunications Act by government agencies for the lawful disruption of access to online services.[5]

In 2019–20, 2 agencies reported using subsection 313(3) of the Telecommunications Act to disrupt online services. This resulted in 8 requests to telcos and 67 websites blocked.

The ACMA is one of these agencies and made 7 requests to telcos in 2019–20, resulting in 66 illegal off-shore gambling websites being blocked.

Emergency suspension of carriage services

Under section 315 of the Telecommunications Act, a senior officer of a police force or service[6] can request the suspension of a carriage service if they have reasonable grounds to believe there is an imminent threat to someone's life or health. Telcos reported the suspension of 17 carriage services in 2019–20, a decrease of 47% from 32 carriage services suspended in 2018–19.

Interception capability costs

The content of telecommunications is protected in Australia.

It is a criminal offence under the TIA Act to intercept or access communications passing over a telecommunications system without the knowledge of those involved in that communication. Only law enforcement and national security agencies can authorise interception with a warrant issued under the TIA Act.

Chapter 5 of the TIA Act requires telcos to develop, install and maintain an interception capability, so that their networks, facilities and carriage services can be intercepted if presented with an interception warrant under paragraph 313(7)(a) of the Telecommunications Act.

Under section 207 of the TIA Act, telcos are responsible for the capital and ongoing costs of providing an interception capability.

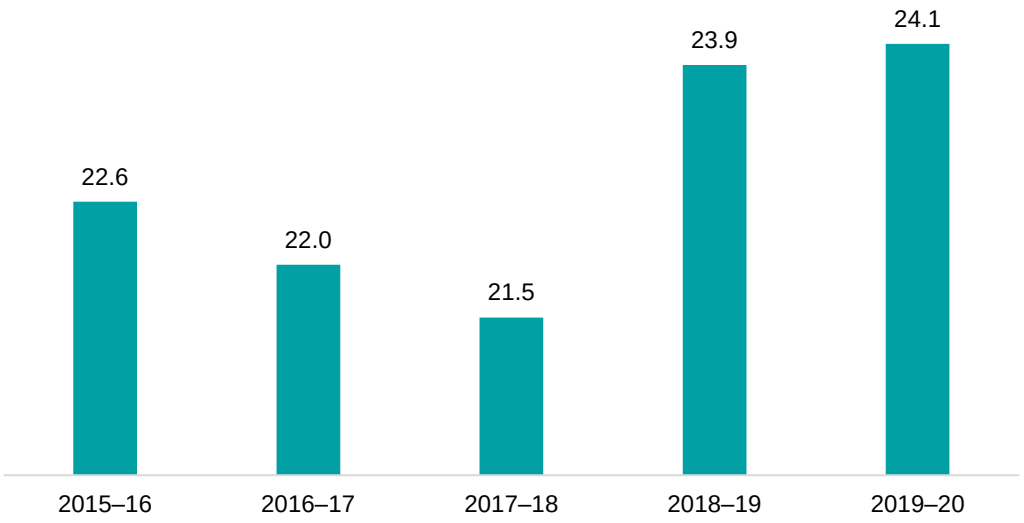
In 2019–20, telcos reported the cost of providing interception capability as approximately $24.1 million, an increase of 0.8% from 2018–19 (Figure 1).

[4] State and territory government agencies are encouraged to follow the guidelines.

[5] www.communications.gov.au/documents/guidelines-use-section-3133-telecommunications-act-1997-government-agencies-lawful-disruption-access.

[6] That is, a commissioned officer of the force or service who holds a rank not lower than the rank of Assistant Commissioner.

Figure 1: Cost of providing interception capabilities ($ million)



Source: Telco industry data request.

Data retention

Since 13 October 2015, telcos have been required to comply with data retention obligations under Part 5-1A of the TIA Act. Telcos are required to retain specific telecommunications data relating to the services they offer for at least 2 years. Telcos can apply to the Communications Access Co-ordinator (through the Department of Home Affairs) for an exemption or variation to the data retention obligations. We have a role in enforcing these obligations.[7]

Cost of complying with data retention obligations

Table 1 sets out telcos' costs (administrative[8] and substantive[9]) of complying with the data retention obligations. It also sets out the costs telcos recovered from criminal law enforcement agencies for responding to requests for data. The recovered costs partially offset the administrative costs reported.

Table 1: Reported cost of complying with the data retention obligations and costs recovered from criminal law enforcement agencies

Financial year	Data retention compliance cost	Costs recovered from criminal law enforcement agencies
2015–16	$44,426,132.06	$9,412,132.06
2016–17	$119,793,739.83*	$9,829,783.17
2017–18	$35,355,577.00	$12,515,681.00
2018–19	$17,453,069.00	$7,443,035.00
2019–20	$21,246,398.52	$11,165,966.50

**The TIA Act allowed approved telcos to implement compliance with data retention obligations over a 2-year period, leading to more costs being incurred during the 2016–17 reporting period.*

Note: The data represents the administrative and substantive compliance costs reported to us by telco industry participants. Industry participants were permitted to report on behalf of subsidiary organisations.

Source: Telco industry data request.

Telco costs increased by 22% from the previous year, while costs recovered from criminal law enforcement agencies increased by 50%.

Data retention compliance and enforcement

The Department of Home Affairs did not refer any telcos to us for failing to comply with data retention obligations in 2019–20.

Telcos can apply to us in writing to seek a review of a decision made by the Department of Home Affairs in relation to a data retention exemption or variation. We did not receive any requests to review an exemption or variation decision in 2019–20.

[7] Compliance with data retention obligations is a carrier licence condition and service provider rule under the Telecommunications Act.

[8] Administrative costs are costs incurred by regulated entities primarily to demonstrate compliance with the regulation (for example, making, keeping, and providing records).

[9] Substantive compliance costs are the costs incurred to deliver the regulated outcomes being sought (for example, plant, equipment and employee training).