Australian Government

acma

Australian Communications and Media Authority

Telcos and law enforcement:
Monitoring industry performance

DECEMBER 2022

acma.gov.au

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
F +61 2 9334 7799

Contents

Overview

Each year, the Australian Communications and Media Authority (ACMA) must prepare a report under subsection 105(5A) of the *Telecommunications Act 1997.* It looks at actions taken in the telecommunications industry to assist law enforcement and national security agencies (agencies) and prevent telecommunications networks and facilities from being used to commit offences. The report must include information about the:

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

This 2021–22 report includes information about how carriers, carriage service providers and carriage service intermediaries (telcos) support and assist agencies by:

- providing assistance
- disclosing telecommunications data
- suspending carriage services in an emergency
- developing, installing and maintaining interception capabilities
- complying with the data retention regime.

It also looks at the costs for telcos of complying with Part 5-3 (interception capability) of the TIA Act.

Consistent with our obligation to do our best to prevent telecommunications networks and facilities being used in the commission of offences[2], this 2021–22 report also includes information about the following ACMA activities:

- disruption of certain online services with the assistance of telcos
- combating phone scams (including mobile number fraud).

[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 of the Telecommunications Act that relate to the telecommunications sector security reforms.
[2] This requirement is set out in subsection 312(1) of the Telecommunications Act.

Support for agencies

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 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 annually on the telecommunications sector security reforms and the Attorney-General's Department on the operation of the TIA Act.[3]

Assisting agencies

Telcos must assist agencies under subsections 313(3) and (4) of the Telecommunications Act. This usually involves providing information about consumers and their communications to:

- enforce criminal law
- enforce laws that impose a pecuniary penalty
- assist the enforcement of the criminal laws in force in a foreign country
- assist the investigation and prosecution of:
  - crimes within the jurisdiction of the ICC (within the meaning of the *International Criminal Court Act 2002*)
  - tribunal offences (within the meaning of the *International War Crimes Tribunals Act 1995*)
- protect public revenue
- safeguard national security.

The ACMA can investigate and take enforcement action if telcos fail to comply with obligations under Part 14 of the Telecommunications Act. We usually become aware of compliance issues through complaints or referrals, but we can also initiate our own enquiries and investigations.

We did not receive any complaints about telco compliance with subsections 313(3) or (4) of the Telecommunications Act from agencies, or conduct any investigations about telco compliance with Part 14 of the Telecommunications Act in 2021–22.

Disclosing telecommunications data

Telcos assist agencies under subsection 313(3) (in association with paragraphs 313(7)(d) and (e)) of the Telecommunications Act by giving effect to agency authorisations under the TIA Act and disclosing telecommunications data under section 280 of the Telecommunications Act.[4]

[3] These requirements are set out in section 315J of the Telecommunications Act. Up until 1 July 2022, the Department of Home Affairs was responsible for reporting on all these matters.
[4] Section 280 of the Telecommunications Act deals with authorisations by or under law.

Telecommunications data is often the first source of information for agency investigations.[5] It can help agencies to eliminate potential suspects and support applications for more intrusive investigative tools, including interception warrants.

In 2021–22, surveyed telcos reported 748,903 disclosures of telecommunications data under section 280 of the Telecommunications Act and the TIA Act (see Table 1).

Table 1: Disclosures of telecommunications data, 2021–22

Reason for disclosure	(Sub)section	Number of disclosures, 2021–22
Under the Telecommunications Act		
Authorised by or under law	280	5,483*
Under the TIA Act		
Voluntary disclosure	177	93
Authorisations for access to existing information or documents – enforcement of the criminal law	178	512,062
Authorisations for access to existing information or documents – locating missing persons	178A	3,051
Authorisations for access to existing information or documents – enforcement of a law imposing pecuniary penalty or protection of the public revenue	179	767
Authorisations for access to prospective information or documents	180	227,386
Enforcement of the criminal law of a foreign country (existing information)	180A	60
Enforcement of the criminal law of a foreign country (prospective information)	180B	1
Total		**748,903****

** The total number of disclosures under section 280 of the Telecommunications Act includes disclosures made to agencies and other entities.*

***The total number of disclosures of personal information under Part 13 of the Telecommunications Act and Chapter 4 of the TIA Act by telcos in 2021–22 is also published in the ACMA's annual report.*

Source: Telco industry data request.

Cost of providing assistance

If a telco is required to give help to an 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.[6] Telcos provide such assistance on the terms and conditions agreed with the relevant Commonwealth, state or territory authority.

[5] Telecommunications data is information about a communication, such as the phone numbers of people who called one another, the duration of the call, the email address from which a message was sent and the time the message was sent – but not the content of the communication.

[6] Subsection 314(2) of the Telecommunications Act.

Emergency suspension of carriage services

Under section 315 of the Telecommunications Act, a senior officer of a police force or service[7] 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 31 carriage services in 2021–22. There were 32 suspensions reported in 2020–21.

Interception capability costs

The content of telecommunications is protected in Australia.

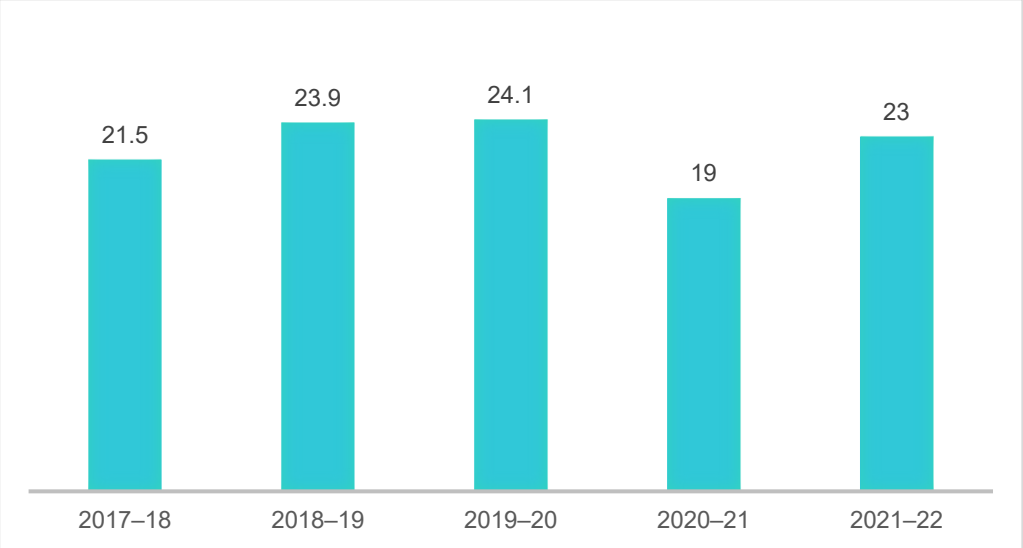
It is a criminal offence under the TIA Act to intercept or access communications passing over a telecommunications system without the knowledge of those involved in that communication. Communications can only be intercepted by agencies that have been issued a warrant under the TIA Act.

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, the provision of interception services, including services in executing an interception warrant under the TIA Act, is a form of assistance for the purposes of section 313.

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

In 2021–22, surveyed telcos reported the cost of providing interception capability as approximately $23 million, an increase of 21% from 2020–21 (see Figure 1).

Figure 1: Cost of providing interception capabilities ($ million), 2017–18 to 2021–22



Source: Telco industry data request.

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

Data retention regime

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. There is also a requirement to protect the confidentiality of information by encrypting the information and protecting the information from unauthorised interference or unauthorised access. This is known as the data retention regime.

Access to data is central to almost all serious criminal and national security investigations.[8] The data retention regime ensures agencies can lawfully access telecommunications data, subject to strict controls.

Section 187AA of the TIA Act outlines the information telcos must retain, including:

- the subscriber of, and accounts, services, telecommunications devices and other relevant services relating to the relevant service
- the source and destination of communications
- the date, time and duration of a communication, or of its connection to a relevant service
- the type of a communication or of a relevant service used in connection with a communication
- the location of equipment or a line used in connection with a communication.

Compliance with the data retention regime is a carrier licence condition and service provider rule under the Telecommunications Act. We are not aware of any failures to comply with the data retention regime and did not undertake any data retention regime compliance investigations in 2021–22.

Telcos can apply to the Communications Access Co-ordinator (CAC – through the Attorney-General's Department[9]) for an exemption or variation to the data retention regime obligations.

Telcos can apply to the ACMA in writing to seek a review of a decision made by the CAC in relation to a data retention regime exemption or variation.

We did not receive any requests to review an exemption or variation decision in 2021–22.

[8] Department of Home Affairs, Data retention obligations, Department of Home Affairs website, 2020, accessed 29 October 2021.
[9] Up until 1 July 2022, the CAC was within the Department of Home Affairs.

Cost of complying with data retention regime obligations

Table 2 sets out surveyed telcos' costs (administrative and substantive[10]) of complying with the data retention regime obligations. It also sets out the costs surveyed telcos recovered from criminal law enforcement agencies for responding to requests for data. The recovered costs partially offset the administrative costs reported.

Table 2: Reported cost of complying with the data retention regime obligations and costs recovered from criminal law enforcement agencies

Financial year	Data retention regime compliance cost	Costs recovered from criminal law enforcement agencies
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
2020–21	$25,262,114.03	$13,385,407.50
2021–22	$28,136,658.54	$14,228,772.50

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

Source: Telco industry data request.

Telco costs for 2021–22 increased by 11% from the previous year, while costs recovered from criminal law enforcement agencies increased by 6%. During the reporting period, 11% of surveyed telcos recovered costs from criminal law enforcement agencies. Those telcos were responsible for over 80% of the 2021–22 compliance costs.

[10] Administrative costs are those incurred by regulated entities primarily to demonstrate compliance with the regulation (for example, making, keeping, and providing records). Substantive compliance costs are those incurred to deliver the regulated outcomes being sought (for example, plant, equipment and employee training).

ACMA activities

Subsection 312(1) of the Telecommunications Act states that in performing its telecommunications functions or exercising its telecommunications powers, the ACMA must do its best to prevent telecommunications networks and facilities being used in, or in relation to, the commission of offences against the laws of the Commonwealth and of the states and territories. Our activities in 2021–22 listed below are consistent with this obligation.

Disrupting online services

Subsection 313(3) enables Commonwealth, state and territory government agencies to request telcos that are internet service providers to provide assistance to disrupt access to illegal online services by blocking access to websites in connection with any of the purposes set out in paragraphs 313(3)(c)–(e)[11] of the Telecommunications Act.

In making requests, Australian Government agencies[12] 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*.[13]

Subsection 313(3) provides agencies with an effective tool to prevent and disrupt online activity that may cause serious harm to the community.

In 2021–22, the ACMA and the Australian Federal Police (AFP) were the only two Australian government agencies that reported using subsection 313(3) of the Telecommunications Act to disrupt online services.

The ACMA made 11 requests to telcos, which resulted in 245 websites for illegal online gambling being blocked. Our work to protect Australians from the harms of illegal online gambling has resulted in 517 illegal gambling websites being blocked since we made our first request in November 2019.

The AFP made 8 requests to telcos, which resulted in 5,481 websites being blocked for the purpose of enforcing the criminal law and laws imposing pecuniary penalties.

Combating phone scams

The ACMA has undertaken a range of scam reduction actions under its *Combating scams action plan*[14] released in November 2019 and ongoing scam reduction work program.

On 2 December 2020, the ACMA registered the Reducing Scam Calls Code. The code was developed by the telco industry in direct response to the ACMA's *Combating scams action plan*. It places obligations on telcos to identify, trace and block scam calls.

[11] This includes enforcing the criminal law, protecting the public revenue and safeguarding national security.

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

[13] Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA), Guidelines for the use of section 313(3) of the Telecommunications Act 1997 by government agencies for the lawful disruption of access to online services, DITRDCA website, 2017, accessed 29 October 2021.

[14] ACMA, *Combating scams action plan*, ACMA website, 2019, accessed 27 September 2022.

In the period from 2 December 2020 to 30 June 2022, over 660 million scam calls were blocked. In the second half of the 2021–22 reporting period, consumer reports/complaints about scam calls to Scamwatch and the ACMA dropped by over 50% and 70%, respectively.

On 30 June 2022, the ACMA made the Telecommunications (Customer Identity Authentication) Service Provider Determination 2022. It aims to protect customers from identify theft and fraud by requiring telcos to use multi-factor authentication before undertaking high-risk customer transactions, such as SIM swaps.

These obligations complement rules in the Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020 to combat mobile number fraud and identity theft. Since the ACMA's introduction of the standard, unauthorised porting has dramatically reduced.

Work was also well underway at the end of the reporting period to register a new Reducing Scam Calls and Scams SMS Code (C611:2022)[15], requiring telcos to identify, trace and block scam SMS in addition to scam calls.

On 27 June 2022, we announced that combating SMS and identity theft phone scams is an ACMA compliance priority for 2022–23.[16] We are working with key partners across government, the financial sector and internationally to identify non-compliance and will take strong enforcement action where warranted.

To obtain data and information relevant to the ACMA's enforcement of the anti-scam rules, we entered into new memoranda of understanding during the reporting period with the Australian Cyber Security Centre, the Canadian Radio-Television and Telecommunications Commission and New Zealand's Department of Internal Affairs.

[15] This new code was registered by the ACMA on 12 July 2022.

[16] ACMA, Compliance priorities 2022–23, ACMA website, 2022, accessed 31 October 2022.