

# Telcos and law enforcement: Monitoring industry performance 2022–23

DECEMBER 2023

**Canberra**

Level 3  
40 Cameron Avenue  
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

**Copyright notice**

<https://creativecommons.org/licenses/by/4.0/>

Except for Commonwealth coats of arms, logos, emblems, images, other third-party material or devices protected by a trademark, this content is made available under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) licence.

We request attribution as © Commonwealth of Australia (Australian Communications and Media Authority) 2023.

All other rights are reserved.

The Australian Communications and Media Authority has undertaken reasonable enquiries to identify material owned by third parties and secure permission for its reproduction. Permission may need to be obtained from third parties to re-use their material.

Written enquiries may be sent to:

Manager, Editorial Services  
PO Box 13112  
Law Courts  
Melbourne VIC 8010  
Email: [info@acma.gov.au](mailto:info@acma.gov.au)

# Contents

<b>Overview</b>	<b>1</b>
<b>Support for agencies</b>	<b>2</b>
Assisting agencies	2
Disclosing telecommunications data	2
Cost of providing assistance	3
Emergency suspension of carriage services	4
Interception capability costs	4
<b>Data retention regime</b>	<b>5</b>
Cost of complying with data retention regime obligations	5
<b>ACMA activities</b>	<b>7</b>
Disrupting illegal online services	7
Combating phone scams	7



# Overview

Each year, the Australian Communications and Media Authority (ACMA) must prepare a report under subsection 105(5A) of the *Telecommunications Act 1997*. The report 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. It must include information about the:

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

This 2022–23 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.

Consistent with our obligation to do our best to prevent telecommunications networks and facilities being used in the commission of offences<sup>2</sup>, this 2022–23 report also includes information about the following ACMA activities:

- > disruption of certain illegal online services with the assistance of telcos
- > combating phone scams.

---

<sup>1</sup> 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.

<sup>2</sup> 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
- > help agencies where reasonably necessary for specific purposes
- > suspend the supply of a service in an emergency if requested to do so by a senior police officer.

The Department of Home Affairs reports annually on the telecommunications sector security reforms under Part 14 of the Telecommunications Act<sup>3</sup> and the Attorney-General's Department on the operation of the TIA Act.

## 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. We commenced one investigation during the reporting period into a telco's compliance with a range of telecommunications-related obligations, including Part 14 of the Telecommunications Act.

## 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.<sup>4</sup>

---

<sup>3</sup> These requirements are set out in section 315J of the Telecommunications Act. The Department of Home Affairs is responsible for reporting on all these matters.

<sup>4</sup> 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.<sup>5</sup> It can help agencies to eliminate potential suspects and support applications for more intrusive investigative tools, including interception warrants. In 2022–23, telcos reported 710,918 disclosures of telecommunications data under section 280 of the Telecommunications Act and the TIA Act (see Table 1).

**Table 1: Disclosures of telecommunications data, 2022–23**

Reason for disclosure	Section	Number of disclosures, 2022–23
<b>Under the Telecommunications Act</b>		
Authorised by or under law	280	4,449*
<b>Under the TIA Act</b>		
Voluntary disclosure	177	60
Authorisations for access to existing information or documents – enforcement of the criminal law	178	523,327
Authorisations for access to existing information or documents – locating missing persons	178A	5,751
Authorisations for access to existing information or documents – enforcement of a law imposing pecuniary penalty or protection of the public revenue	179	65
Authorisations for access to prospective information or documents	180	177,080
Enforcement of the criminal law of a foreign country (existing information)	180A	185
Enforcement of the criminal law of a foreign country (prospective information)	180B	1
<b>Total</b>		<b>710,918**</b>

\* 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 by telcos in 2022–23 is also published in the ACMA's annual report.

Source: Telco industry reports.

## 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.<sup>6</sup> Telcos provide such assistance on the terms and conditions agreed with the relevant Commonwealth, state or territory authority.

<sup>5</sup> 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.

<sup>6</sup> Section 314 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<sup>7</sup> 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 71 carriage services in 2022–23. There were 31 suspensions reported in 2021–22.

## Interception capability costs

The content of telecommunications is protected in Australia.

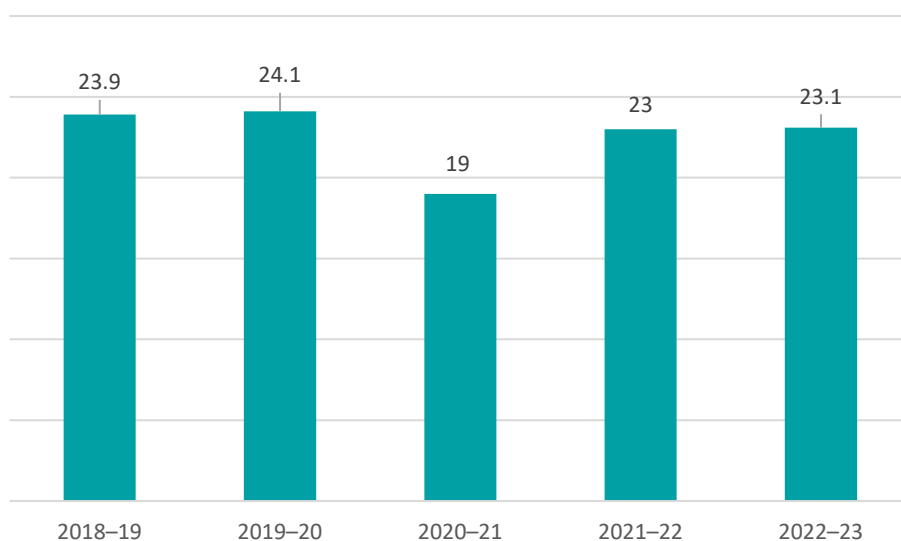
It is a criminal offence under the TIA Act to intercept or access communications passing over a telecommunications system without the knowledge of those involved in that communication. Communications can only be intercepted by agencies that have been issued a warrant under the TIA Act.

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 2022–23, surveyed telcos reported the cost of providing interception capability (excluding capital and ongoing costs) as approximately \$23.1 million (see Figure 1).

**Figure 1: Cost of providing interception capabilities (\$ million), 2018–19 to 2022–23**



Source: Telco industry data request.

<sup>7</sup> 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. This is known as the data retention regime.

Access to data is central to almost all serious criminal and national security investigations.<sup>8</sup> 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.

Telcos can apply to the Communications Access Co-ordinator (through the Attorney-General's Department) 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 Communications Access Co-ordinator in relation to a data retention regime exemption or variation.

We commenced 2 investigations into compliance with the data retention regime in 2022–23.

We did not receive any requests to review an exemption or variation decision in 2022–23.

## Cost of complying with data retention regime obligations

Table 2 sets out telcos' costs (administrative and substantive<sup>9</sup>) of complying with the data retention regime obligations. It also sets out the costs that telcos recovered from criminal law enforcement agencies for responding to requests for data. The recovered costs partially offset the administrative costs reported.

---

<sup>8</sup> Department of Home Affairs, [Data retention obligations](#), Department of Home Affairs website, Australian Government, 2023, accessed 3 October 2023.

<sup>9</sup> 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).

**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
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
2022–23	\$26,019,314.37	\$15,171,490.00

*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 for 2022–23 decreased by 7.5% from the previous year, while costs recovered from criminal law enforcement agencies increased by 7%. The median compliance costs reported were \$37,000. Less than 13% of telcos recovered any costs from criminal law enforcement agencies.

# 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. The ACMA activities in 2022–23 listed below are consistent with this obligation.

## Disrupting illegal 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)<sup>10</sup> of the Telecommunications Act.

In making requests, Australian Government agencies<sup>11</sup> 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*.<sup>12</sup>

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

In 2022–23, 3 Australian government agencies reported making a total of 29 requests under subsection 313(3) of the Telecommunications Act to disrupt 6,549 online services. Of those, the ACMA made 11 requests to telcos, which resulted in 269 websites for illegal online gambling being blocked.

Our work to protect Australians from the harms of illegal online gambling has resulted in 786 illegal gambling websites being blocked (as at 30 June 2023) since we made our first request in November 2019.

## Combating phone scams

The ACMA has undertaken a range of actions to disrupt scams before they reach Australians, including supporting disruption initiatives and making and enforcing new anti-scam rules.

On 12 July 2022, the ACMA registered the C661:2022 *Reducing Scam Calls and Scam SMS Industry Code* (the code). The code requires telecommunications providers to identify, trace and disrupt scam calls and SMS. It replaced the C661:2020 *Reducing Scam Calls Code* (deregistered on 12 July 2022), which only dealt with scam calls.

Under the code, telcos reported blocking over 1.4 billion scam calls and 257 million scam SMS to 30 June 2023. The ACMA has been conducting compliance activities to make sure telcos accurately report scam calls and SMS, after the ACMA uncovered some telcos had not been reporting as required.

---

<sup>10</sup> This includes enforcing the criminal law, protecting the public revenue and safeguarding national security.

<sup>11</sup> State and territory government agencies are encouraged to follow the guidelines.

<sup>12</sup> Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDC), [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](#), DITRDC, Australian Government, 2017, accessed 3 October 2023.

Combating SMS scams was an ACMA compliance priority in 2022–23<sup>13</sup> due to evidence about the prevalence and impact of text scams (ACCC Scamwatch consumer report data indicates reports about SMS scams rose 19% from 2021 to 2022, from around 67,200 to around 79,800 and reported losses rose 183%, from \$10.1 million to \$28.6 million).

The ACMA commenced auditing telcos that send bulk SMS in November 2022 as a potential conduit of SMS scams onto Australian networks. The audit results have led the ACMA to commence investigations into multiple telcos for suspected non-compliance. As at 30 June 2023, the ACMA has published the outcomes of 4 enforcement actions where non-compliance was found.

In February 2023, the ACMA gave Modica Group Limited a direction to comply with the code after we found the telco had allowed SMS to be sent using text-based sender IDs without sufficient checks to ensure they were being used legitimately.

In May 2023, the ACMA gave directions to comply with the code to Sinch Australia Pty Ltd and Infobip Information Technology Pty Ltd, as well as a formal warning to Phone Card Selector Pty Ltd. The ACMA found each entity allowed SMS to be sent using text-based sender IDs without sufficient checks to ensure they were being used legitimately. The [investigation reports and related media releases](#) are available on the ACMA's website.

These obligations complement a suite of ACMA-made anti-scam rules that include the [Telecommunications \(Mobile Number Pre-Porting Additional Identity Verification\) Industry Standard 2020](#) and the [Telecommunications Service Provider \(Customer Identity Authentication\) Determination 2022](#), which were introduced to combat mobile number fraud and identity theft. Since the ACMA introduced these rules, unauthorised porting and high-risk customer transactions (including SIM swaps) have dramatically reduced.

We will keep working to prevent these scams reaching Australians by enforcing existing rules, collaborating with Australian and global partners, and exploring new ways to stop scam messages that impersonate legitimate brands or organisations.

Additionally, we have also engaged with telcos on a range of scam disruption initiatives, including:

- > providing de-identified complaint data to facilitate identification and blocking of scams
- > monitoring and supporting telco efforts to trace the origins of scam traffic and telco capability improvements, including the introduction by key telcos of AI or machine learning to automate and enhance the identification and disruption of scams
- > sharing information and intelligence about current and emerging scam threats, including via regular intelligence reports and the ACMA's Scam Telco Action Taskforce
- > assisting well-known brands and government agencies to engage with telcos to protect their numbers and SMS sender IDs from impersonation.

---

<sup>13</sup> This compliance priority remains ongoing in 2023-24, [Compliance priorities 2023–24](#), ACMA website, Australian Government, 2023, accessed 3 October 2023.