Australian Government | acma Australian Communications and Media Authority

Telcos and law enforcement

Monitoring industry performance 2024–25

DECEMBER 2025

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

Contents

Executive summary

Each year, the 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 associated compliance costs[1]
- costs of complying with Part 5-1A (data retention) of the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

This 2024–25 report includes information about how telcos (carriers, carriage service providers and carriage service intermediaries) 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,[2] this 2024–25 report also includes information about the following ACMA activities:

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

[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 we are not required to report on the matters set out in section 315J of the Telecommunications Act that relate to the telecommunications sector security reforms. In April 2025, this section of the Telecommunications Act moved to the *Security of Critical Infrastructure Act 2018* (the SOCI Act).

[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
- 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.

Under section 312, the ACMA has complementary obligations. It must take all reasonable steps to prevent networks and facilities from being used in connection with criminal activity and provide assistance to enforcement and security agencies. The ACMA fulfils these duties through regulatory oversight, including monitoring compliance and facilitating cooperation between agencies and telcos. These measures ensure that the objectives of Part 14 are implemented effectively and that industry maintains the capability to meet lawful access requirements.

The Department of Home Affairs reports annually on the telecommunications sector security reforms under Part 14 of the Telecommunications Act[3] and the operation of the TIA Act.[4]

Assisting agencies

Telcos must assist agencies under subsections 313(3) to (4B) 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
- support emergency response.

[3] These requirements were set out in section 315J of the Telecommunications Act until April 2025. The requirements have now moved to the SOCI Act.

[4] Following an Administrative Arrangements Order issued in May 2025 and machinery of government changes, this function transitioned from the Attorney-General's Department to the Department of Home Affairs.

We 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), (4), (4A), or (4B) of the Telecommunications Act from agencies, nor did we initiate our own enquiries or investigations.

Interception capability costs

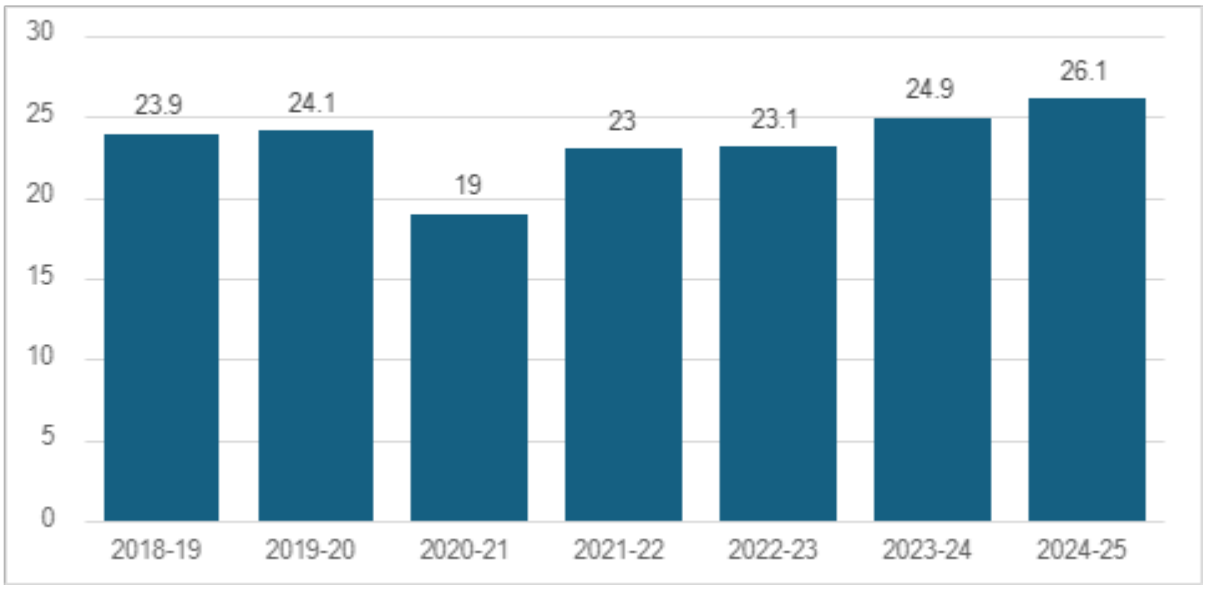
It is a criminal offence under the TIA Act to intercept or access communications passing over a telecommunications system without the knowledge of those involved in that communication. Communications can only be intercepted by agencies that have been issued a warrant under the TIA Act.

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

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 of the Telecommunications Act.

In 2024–25 surveyed telcos reported their interception capability costs as $26,142,868.84 (see Figure 1).

Figure 1: Cost of providing interception capabilities ($ million), 2018–19 to 2024–25



Note: Since the 2022–23 reporting year, a reduced number of telcos were surveyed in relation to their interception capability costs.

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.[5]

Telecommunications data is often the first source of information for agency investigations.[6] It can help agencies to eliminate potential suspects and support applications for more intrusive investigative tools, including interception warrants. Table 1 sets out the disclosure of telecommunications data.

In 2024–25, telecommunications providers reported a 16.6% increase in disclosures under section 280 of the Telecommunications Act. For disclosures under the TIA Act, most categories decreased compared to 2023, with one notable exception: authorisations to locate missing persons recorded the largest increase. Key changes include:

- Authorisations for access to existing information for criminal law enforcement: **–6.1%**
- Authorisations for prospective information: **–16.1%**
- Voluntary disclosures: **–69.5%**
- Existing information for enforcement of foreign criminal law: **–43.4%**
- Prospective information for enforcement of foreign criminal law: **–100%**
- Authorisations to locate missing persons: **+46.6%**
- Requests related to pecuniary penalties or public revenue: **+20%**

[5] Section 280 of the Telecommunications Act deals with authorisations by or under law.

[6] 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.

Table 1: Disclosures of telecommunications data, 2024–25

Reason for disclosure	Section	Number of disclosures, 2024–25
Under the Telecommunications Act		
Authorised by or under law	280	5,964*
Under the TIA Act		
Voluntary disclosure	177	203
Authorisations for access to existing information[7] or documents – enforcement of the criminal law	178	510,013
Authorisations for access to existing information or documents – locating missing persons	178A	14,717
Authorisations for access to existing information or documents – enforcement of a law imposing pecuniary penalty or protection of the public revenue	179	180
Authorisations for access to prospective information[8] or documents	180	166,375
Enforcement of the criminal law of a foreign country (existing information)	180A	77
Enforcement of the criminal law of a foreign country (prospective information)	180B	0
Total		**697,529****

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

*** This represents a subset of the total number of disclosures of personal information made under Part 13 of the Telecommunications Act by telcos in 2024–25, the total number of disclosures is 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, under section 314 of the Telecommunications Act, it must do so on the basis that it does not profit from, or bear the cost of, that help. Telcos provide such assistance on the terms and conditions agreed with the relevant Commonwealth, state or territory authority.

[7] For example, call charge records.
[8] This refers to information that will be generated in the future (e.g., ongoing call or location data)

During the reporting period, one complaint was received regarding a telco's cost recovery under section 314 of the Telecommunications Act. This matter is currently under consideration.

Emergency suspension of carriage services

Under section 315 of the Telecommunications Act, a senior officer of a police force or service[9] 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 36 carriage services in 2024–25 compared to 77 suspensions reported in 2023–24.

[9] 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. This must be for at least 2 years. It is known as the data retention regime.

Access to data is central to almost all serious criminal and national security investigations.[10] 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 Department of Home Affairs) 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 did not receive any requests to review an exemption or variation decision in 2024–25.

We are continuing an investigation into compliance with the data retention regime which we commenced in 2023–24.

In our previous report, we noted that proceedings had been filed in the Federal Court against Optus Mobile Pty Ltd in relation to a data breach in September 2022. The matter is still before the court.

[10] Department of Home Affairs, Data retention obligations, Department of Home Affairs website, Australian Government, 2024, accessed 29 October 2024.

Cost of complying with data retention regime obligations

Table 2 sets out telcos' costs (administrative and substantive[11]) 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.

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
2023-24	$29,729,879.35	$17,111,920.00
2024-25	$37,106,182.52	$18,742,142.50

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 2024–25 increased by 24.81% from the previous year, while costs recovered from criminal law enforcement agencies increased by 9.53%.

This increase is partly attributable to a significant rise in the number of telco's reporting to the ACMA this year, an increase of 194% on the 2023-24 period. However, the distribution of costs remains highly concentrated among larger entities, consistent with previous reporting trends.

Only 5.13% of telcos recovered any costs from criminal law enforcement agencies.

[11] 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).

Other ACMA activities

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)[12] of the Telecommunications Act.

In making requests, Australian Government agencies[13] are expected to follow the whole-of-government guidelines released in June 2017.[14]

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

In 2024–25, 4 Australian Government agencies reported making a total of 464 requests under subsection 313(3) of the Telecommunications Act to disrupt 10,733 online services. Of those, we made 12 requests to telcos, which resulted in 256 websites for illegal online gambling being blocked.

Our work to protect Australians from the harms of illegal online gambling has resulted in 1,251 illegal gambling websites being blocked (as at 30 June 2025) since we made our first request in November 2019.

Combating phone scams

The ACMA supports the government's Fighting Scams initiative to address scams and protect Australians from financial harm. We contribute to the work of the National Anti-Scam Centre (NASC), which coordinates government, law enforcement and the private sector to combat scams.

The ACMA is taking active steps to rebuild confidence in the use of telephone numbers and sender IDs and is working closely with other government agencies on a range of anti-scam measures to protect Australians and make Australia a hard target for scammers.

Enforcing anti-scam rules

The ACMA continues to enforce the 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 Reducing Scam Calls Code, which dealt only with scam calls.

Disrupting SMS impersonation scams under the code was an ACMA compliance priority in 2024–25 due to evidence about the prevalence and impact of text scams. In 2023, Scamwatch reported that text message was the most common scam delivery method, with $27 million lost to SMS scams[15]. Impersonation scams are a predominant type of scam via the channel.

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

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

[14] 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*, DITRDC, Australian Government, 2017, accessed 29 October 2024.

[15] Targeting scams | Report of the National Anti-Scam Centre on scams activity 2023 (nasc.gov.au), page 14

In 2024–25, we promoted and enforced the code, and the obligations on telcos to monitor, detect, and block scam messages and calls, including SMS impersonation scams, and to share information with each other and with the ACMA.

In August 2024, we announced we had directed SMSGlobal Pty Ltd to comply with the code after it allowed over one million SMS to be sent using sender IDs (i.e. shortened business or organisation names that appear at the top of SMS messages such as 'ATO' or 'myGov') without sufficient checks to ensure their use was legitimate.[16] The investigation also uncovered evidence that some scammers had used the vulnerabilities to send SMS brand impersonation scams using well-known brands like AusPost, NAB and ANZ.

In May 2025, we announced we had directed VoiceHub Pty Ltd to comply with the code after it failed to share information with the ACMA about the number of scam SMS it blocked for the July to September 2022 quarter to the April to June 2024 quarter.[17]

The code obligations complement other anti-scam rules that the ACMA continues to enforce, including the Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020 and the Telecommunications Service Provider (Customer Identity Authentication) Determination 2022, which are both designed to prevent mobile number fraud and unauthorised access to telco services.

In May 2025, we announced that Circles Australia Pty Ltd contravened the Pre-Porting Additional Identity Verification Standard for failing to comply with identity verification rules that led to consumers being exposed to identity theft and financial losses.[18] Circles paid a $431,160 infringement notice and the ACMA accepted a three-year court-enforceable undertaking after the investigation.

The ACMA announced that mobile number fraud will be a compliance priority across 2025–26 due to the serious impacts that can occur from non-compliance, including identity theft, misuse of personal information and significant financial loss.

Disruption and engagement

Under the code, telcos have reported blocking over 2.6 billion scam calls (from December 2020 to 30 June 2025) and over 936.7 million scam SMS (from July 2022 to 30 June 2025). We actively monitor blocking figures and industry traceback activities for emerging and longer-term trends to inform disruption, and compliance and enforcement activities.

The ACMA is responsible for establishing the SMS Sender ID Register for Australia in 2025–26. The register will further protect consumers who receive, and entities that send, SMS/MMS messages to Australian mobile numbers, by disrupting scam messages that use sender IDs.

In conjunction with key telcos, and businesses and agencies subject to SMS impersonation scams, the ACMA is providing a voluntary pilot register to disrupt specific sender ID scams until the mandatory register goes live. The pilot was operating across 2024–25.

[16] https://www.acma.gov.au/articles/2024-08/smsglobal-breaches-sms-scam-rules
[17] https://www.acma.gov.au/articles/2025-05/voicehub-breaches-phone-scam-rules
[18] https://www.acma.gov.au/articles/2025-05/circleslife-pays-413k-more-anti-scam-breaches

We have also engaged with telcos, businesses and overseas regulators on a range of scam disruption initiatives, including:

- providing de-identified complaint data to facilitate identification and blocking of scams
- sharing information and intelligence about current and emerging scam threats
- monitoring telco capability uplift, including the introduction by key telcos of technology to automate and enhance the identification and disruption of scams
- assisting well-known brands and government agencies to engage with telcos to protect their numbers and SMS sender IDs from impersonation
- releasing consumer awareness phone scams campaigns and consumer alerts about higher-risk and/or emerging scam threats
- entering into strategic anti-scam relationships with international regulators such as the Commission for Communications Regulation in Ireland and the Office of Communications in the UK.