Australian Government | acma Australian Communications and Media Authority

Telcos and law enforcement

Monitoring industry performance 2023–24

NOVEMBER 2024

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 2023–24 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 2023–24 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.

[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.

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

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) or (4) of the Telecommunications Act from agencies. During the reporting period, we commenced one investigation into a telco’s compliance where the scope of that investigation included compliance with aspects of 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.[4]

[3] 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.
[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 2023–24, telcos reported 757,619 disclosures of telecommunications data under section 280 of the Telecommunications Act and the TIA Act (see Table 1).

Table 1: Disclosures of telecommunications data, 2023–24

Reason for disclosure	Section	Number of disclosures, 2023–24
Under the Telecommunications Act		
Authorised by or under law	280	5,113*
Under the TIA Act		
Voluntary disclosure	177	666
Authorisations for access to existing information or documents – enforcement of the criminal law	178	543,208
Authorisations for access to existing information or documents – locating missing persons	178A	10,041
Authorisations for access to existing information or documents – enforcement of a law imposing pecuniary penalty or protection of the public revenue	179	150
Authorisations for access to prospective information or documents	180	198,303
Enforcement of the criminal law of a foreign country (existing information)	180A	136
Enforcement of the criminal law of a foreign country (prospective information)	180B	2
Total		**757,619****

** 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 2023–24, the total number of disclosure 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, 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] 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[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 77 carriage services in 2023–24. There were 71 suspensions reported in 2022–23.

Interception capability costs

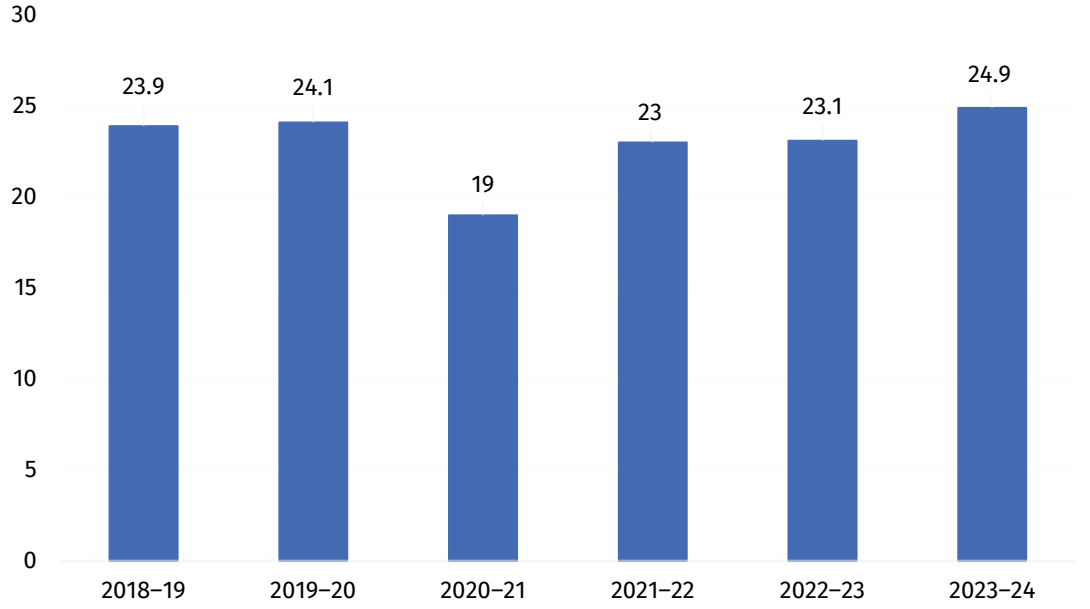
It is a criminal offence under the TIA Act to intercept or access communications passing over a telecommunications system without the knowledge of those involved in that communication. Communications can only be intercepted by agencies that have been issued a warrant under the TIA Act.

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 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 2023–24 surveyed telcos reported their interception capability costs as $24,905,180.80 million (see Figure 1).

Figure 1: Cost of providing interception capabilities ($ million), 2018–19 to 2023–24



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

[7] 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.[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.

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 did not receive any requests to review an exemption or variation decision in 2023–24.

We commenced one investigation into compliance with the data retention regime in 2023–24 which is ongoing. We also filed proceedings in the Federal Court against Optus Mobile Pty Ltd. We allege that during a data breach which occurred between 17 to 20 September 2022, Optus failed to protect the confidentiality of its customers' personal information from unauthorised interference or unauthorised access as required under the TIA Act.

Cost of complying with data retention regime obligations

Table 2 sets out telcos' costs (administrative and substantive[9]) 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.

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

[9] 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
2023-24	$29,729,879.35	$17,111,920.00

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 2023–24 increased by 14.3% from the previous year, while costs recovered from criminal law enforcement agencies increased by 12.78%.

Only 13% of telcos recovered any costs from criminal law enforcement agencies.

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)[10] of the Telecommunications Act.

In making requests, Australian Government agencies[11] are expected to follow the whole-of-government guidelines released in June 2017.[12]

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

In 2023–24, 3 Australian government agencies reported making a total of 144 requests under subsection 313(3) of the Telecommunications Act to disrupt 7,783 online services. Of those, we made 10 requests to telcos, which resulted in 209 websites for illegal online gambling being blocked.

Our work to protect Australians from the harms of illegal online gambling has resulted in 986 illegal gambling websites being blocked (as at 30 June 2024) since we made our first request in November 2019.

Combating phone scams

We have 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 requires telecommunications providers to identify, trace and disrupt scam calls and SMS. It replaced the C661:2020 Reducing Scam Calls Code, which dealt with scam calls.

Under the code, telcos reported blocking over 2.1 billion scam calls (from December 2020) and over 668.3 million scam SMS (from July 2022 to 30 June 2024). We actively monitor blocking figures, and industry traceback activities, for emerging and longer-term trends to inform disruption and compliance and enforcement activities.

Combating SMS scams was an ACMA compliance priority in 2023–24 due to evidence about the prevalence and impact of text scams.[13] The National Anti-Scam Centre's *Targeting scams* report for 2023 stated that text message was the most reported scam contact method in 2023, with 109,621 reports (a 37.3% increase from 2022).[14]

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

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

[12] 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.

[13] Disrupting SMS impersonation scams is an ACMA compliance priority for 2024-25, Compliance priorities 2024–25 | ACMA, accessed 23 September 2024.

[14] Targeting scams: report of the ACCC on scams activity 2023 (nasc.gov.au), pg. 14, accessed 23 September 2024

In 2023–24, we audited telcos that send bulk SMS as a potential conduit of text scams onto Australian networks. The audit results led us to commence investigations into multiple telcos for suspected non-compliance. Between 1 July 2023 and 30 June 2024, we published the outcomes of 9 enforcement actions where non-compliance was found. All 9 telcos were directed to comply with the code or face penalties of up to $250,000 for future code breaches. The investigation reports and related media releases are available on our website.

In May 2024 we directed Symbio Group telcos to comply with the code after we found Symbio Wholesale failed to share information about scam calls with other telcos and the ACMA in a timely manner.

The code 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. These were introduced to combat mobile number fraud and identity theft. Since we introduced these rules, unauthorised porting and high-risk customer transactions (including SIM swaps) have significantly reduced[15].

In January 2024, we announced that Medion Australia Pty Ltd contravened the Customer ID Determination by failing to perform required customer ID authentication processes, leading to financial losses for consumers. Medion paid a $259,000 infringement notice as a result of the investigation.

In February 2024, we found that Telstra contravened the Customer ID Determination after it failed to perform required customer ID authentication processes for 168,000 high risk customer interactions. Telstra offered an enforceable undertaking and paid a $1,551,000 infringement notice as a result of the investigation.

We commenced a voluntary SMS sender ID register pilot in December 2023, as an interim measure while a legislated register is developed.[16] The register is part of the government's Fighting Scams initiative to address scams and online fraud and protect Australians from financial harm. It will help protect alphanumeric sender IDs (i.e. message headers) of SMS sent by brands and government agencies from impersonation by scammers, and protect consumers from receiving these scams.

We have engaged with telcos and businesses, and supported the National Anti-Scam Centre, 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 technology to automate and enhance the identification and disruption of scams
> sharing information and intelligence about current and emerging scam threats, including via regular data sharing and intelligence reports and through 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

[15] A comparison of data we have been receiving since January 2021 demonstrates a reduction in instances of mobile fraud allegations since the introduction of the anti-scam rules.
[16] https://minister.infrastructure.gov.au/rowland/media-release/new-legislation-crack-down-sms-scams, accessed 23 September 2024

> releasing consumer awareness phone scams campaigns and consumer alerts about higher-risk and/or emerging scam threats.

We will keep working to prevent 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.