Australian Government
Department of Infrastructure, Transport, Regional Development, Communications and the Arts

Australian Government
Attorney-General's Department

Policy Statement of Intent under Section 287 of the Telecommunications Act 1997

Revised date: April 2024

Summary

The Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) has developed this policy statement of intent to assist law enforcement and other emergency services to make requests for information using section 287 of the *Telecommunications Act 1997* (Cth) (the Act).

Note: The information contained in this document does not constitute legal advice

Statement of Intent

Telecommunications companies are prohibited under the Act from disclosing or using certain information or documents about their customers ('protected information'). There are however a number of statutory exceptions. This includes section 287 which can be used in limited circumstances, without consent, where there is a serious threat to a person's life or health. Section 287 contemplates an emergency situation where disclosure of protected information is necessary to keep a person safe.

One common example of the use of the provision is when law enforcement and emergency service organisations seek assistance from telecommunications companies to find missing people.

In cases of responding to reports of missing people, time is of the essence and delays in obtaining missing person's information can be detrimental.

Helping emergency services save lives, while ensuring there are privacy protections, is of utmost importance. That is why the Act includes a privacy safeguard at section 287 requiring that the telecommunications company needs to be satisfied that it is 'unreasonable' or 'impracticable' to get the consent of the person involved to the proposed use or disclosure of information.

The Act also includes strict 'secondary disclosure' prohibitions, allowing a person who received information (including the location of the person's mobile phone) or documents about a person to disclose that information or document to another person only to prevent or reduce a serious threat to the life or health of a person.

Altogether, section 287 aims to strike a balance between assisting law enforcement and emergency service organisations to protect the community against threats of life or harm while also protecting the privacy of the affected individual.

Interactions with the TIA Act

Section 287 of the Act does not authorise access to telecommunications information for general investigation or enforcement purposes relating to crime, revenue, or national security matters. The powers under Chapter 4 of the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act) support the operations of law enforcement agencies working in a law enforcement capacity, with oversight regimes tailored to law enforcement operations. For example:

- enforcing the criminal law (sections 178 and 180 of the TIA Act);
- imposing a pecuniary penalty or the protection of the public revenue (section 179 of the TIA Act); and
- investigating a serious offence (section 180 of the TIA Act).

These powers only enable law enforcement agencies to access telecommunications data. Access to the contents of a communication would need to be sought through the relevant interception and access powers under Chapters 2 and 3 of the TIA Act.

Assistance from the Department

Law enforcement and emergency services organisations can seek further (non-time sensitive) guidance from DITRDCA at telecommunications.security@infrastructure.gov.au. Questions relating to the TIA Act should be directed to the Office of the Communications Access Coordinator within the Attorney-General's Department on 1800 271 030 or cac@ag.gov.au.