The Assistance and Access Act: what does the industry assistance framework mean for domestic and international companies?

Australia actively supports the growth and use of technologies, like encryption, that secure the use of digital platforms for banking, shopping, education, health, communications and other key services. These innovative products allow everyday users to harness the potential of the digital world, and their expansion should be encouraged.

The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (the Act), passed into law in December 2018, embodies Australia's commitment to innovation and online security. The industry assistance framework introduced by Schedule 1 of the Act modernises the way Australian law enforcement and national security agencies interact with the modern communications sector. This framework facilitates collaboration between agencies and industry on technical matters related to the investigation or prosecution of serious offences like terrorism and drug trafficking. The framework's robust safeguards and strong emphasis on cooperation with business embodies Australia's commitment to innovation, private enterprise and online security.

More information on the Act can be found on the Department of Home Affairs website - www.homeaffairs.gov.au.

What does the industry assistance framework do?

The Act allows Australia's key law enforcement and national security agencies to request or compel designated communications providers to provide assistance where there is a technological obstacle to investigations and operations. The framework is consultative and requests for assistance are made in close collaboration with the provider.

The framework is not about encryption or information collection – It is about industry assisting law enforcement and national security agencies to lawfully carry out their functions to protect the community.

Why is the industry assistance framework needed?

Australia's previous assistance framework only applies to telecommunications and internet service providers that are Carriers or Carriage Service Providers under the *Telecommunications Act 1997*. While these companies play a central role in the Australian communications network, they are now one subset of many players critical to the supply of communications services and devices, in an increasingly large and diffuse market. Agencies can now ask for assistance from the full range of companies operating in the digital environment, with more transparency and stronger safeguards than before.

Is my company captured?

The industry assistance framework applies to ***designated communications providers***.[1] Your company is likely to be captured if it supplies relevant communications services or products for use, or likely use, in Australia.

The types of companies whose activities are captured include telecommunications operators, providers of electronic services, and developers of software and manufacturers of devices (such as phones).

Assistance cannot be sought from individual employees within your company. Requests for assistance are directed towards the corporate entity itself.

[1] See the definition in section 317C of the Act.

My company is a *designated communications provider*. Do I need to change how we operate?

No. The framework does not place any immediate or ongoing obligations on designated communications providers.

A designated communications provider will only be affected by the Act when issued with a formal request. To meet the legal threshold with any notice or request, the designated communications provider must be in a position to give material assistance to law enforcement and national security agencies, but only to the extent that they are capable of doing so.

A designated communications provider cannot be forced to comply with the impossible. Requests must be *reasonable*, *proportionate, practicable* and *technically feasible.*

Assistance must account for your company's business interests

Requests or notices are subject to detailed decision-making criteria and consultation requirements to protect business interests, data security and to ensure minimal impact on industry.

When issuing a request or notice, agencies must consider the impact on business, privacy and cyber security. These assessments include research and development efforts, personnel allocation or other features likely to impact company operations.

The starting position is that companies should be compensated for the reasonable costs of their assistance. Companies, their employees and their agents will receive civil immunity for good faith conduct in providing this assistance.

Devices and networks remain secure

The Act expressly prohibits any request or requirement that would undermine electronic protection on a systemic-level or make data less secure.

Agencies **cannot** require a designated communications provider to:

- undertake activities that would create a material risk of unauthorised access in a service or product;
- jeopardise a form of electronic protection (e.g. end-to-end encryption);
- refrain from patching a weakness; or
- build decryption capabilities.

These prohibitions rule out, for example, the construction of law enforcement keys or so-called 'exceptional access' systems.

The law contains a detailed **review** process where a provider is being asked to develop a new capability to ensure the provider is not required to do anything that would breach these prohibitions.

Defence for a conflict with foreign laws

If a designated communications provider would have to act offshore in a way that breaks a law of that foreign country in order to comply with a request or notice, the Act creates a defence for non-compliance.

The Act is not intended to force designated communications providers to choose between complying with the Act on one hand and breaching foreign law on the other. It is a defence to enforcement action in Australia if the requested offshore activities would violate relevant foreign laws.

Warrants are still required

The measures in the Act cannot be used for mass surveillance or accessing data where a warrant or authorisation is otherwise required.

The Act does not allow for interception of communications, online surveillance, or access to data without an underlying **warrant** or **authorisation**, where those warrants or authorisations are required under separate laws (for example, the *Telecommunications (Interception and Access) Act 1979*).

Independent oversight

Australia's independent oversight bodies, the Inspector-General of Intelligence and Security and the Commonwealth Ombudsman, have oversight of agency activities under the framework.

Oversight bodies are notified of all key activities under the framework, including the requesting of assistance, and have the authority to inspect (and report on) agency conduct. You will have a direct right of complaint to these independent organisations.

Judicial review of any decision to give a notice or request is also available by default.

Accountability and transparency

The Act prohibits the disclosure of detailed information about requests or notices. There are exceptions to this prohibition to ensure accountability and transparency, without revealing sensitive information. The Act also requires reports to be made to Parliament (and through this, to the public).

Facts and figures on the use of the framework will be available in annual public reports and other reports that go to the Australian Parliament. Designated communications providers themselves can disclose limited statistical information about requests they receive. Information can be disclosed to receive legal advice and, within a designated communications provider, employees and employers can discuss requests or notices from agencies as needed to provide the assistance that has been requested or required.