Australian Government
Department of Home Affairs

Industry assistance under Part 15 of the Telecommunications Act 1997 – Frequently Asked Questions

Contents

Overview of the industry assistance framework under Part 15 of the *Telecommunications Act 1997*

Why do we need the industry assistance framework in Part 15?

Law enforcement and national security agencies have the critical role of keeping the community safe from those who seek to harm us, be they serious criminals, terrorists or others seeking to undermine our national security. However the rapidly evolving technological environment has seriously impeded the ability of these agencies to perform their essential, lawful activities.

Part 15 of the *Telecommunications Act 1997* (the Telecommunications Act) responds to these challenges by providing agencies with a range of new investigatory powers to overcome the increasing barriers to barriers to visibility of criminal activity online. Importantly the legislation does not undermine encryption, and includes powerful safeguards to protect the privacy and data security of those that are not the subject of an investigation.

As a result, Part 15 of the Telecommunications Act assists agencies maintain a safe and secure environment, and ensures that both the public and businesses can continue to rely on digital platforms for essential services such as banking, shopping, education and health.

How and when was this framework introduced?

The framework was established by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (the Assistance and Access Act) on 9 December 2018.

The Assistance and Access Act takes into account Parliamentary committee inquiries and a three-stage consultation process which provided an opportunity for the media, industry, academics, advocacy groups and the public to scrutinise the framework and recommend changes.

What does the Assistance and Access Act do?

The Assistance and Access Act equips Australia's law enforcement and national security agencies with the necessary tools to operate in, and adapt to, the evolving technological environment.

The Australian Government supports the use of technologies, like encryption, which are critical to maintaining cybersecurity and securing devices and networks. However, technology and the communications environment are evolving at a rapid pace and the law, and the agencies it governs, must keep up.

The Assistance and Access Act modernises the powers of Australia's law enforcement and security agencies by:

- **establishing a technologically neutral industry assistance framework**. The framework established a structure through which Australian agencies and the modern communications industry can work together to address the technological obstacles often presented to investigations into serious crimes and national security threats.
    - **The Assistance and Access Act introduced this framework as new Part 15 of the Telecommunications Act.**
    - **This framework is the main focus of the FAQs in this document.**
- **enhancing investigatory and procedural powers** to improve agencies' ability to search for, and collect, data. Today, most information is held in digital format and the Assistance and Access Act modernises the search warrant framework to account for this new reality.

These measures ensure agencies can cope more readily with technological change and combat the loss of evidence and intelligence without undermining the cybersecurity of devices and networks or the privacy of Australians.

What is the industry assistance framework?

The industry assistance framework under Part 15 of the Telecommunications Act establishes a clear structure for cooperative engagement between Australia's law enforcement and national security agencies, and the modern communications industry.

The industry assistance framework introduced three new measures to facilitate this cooperative approach:

- **Technical assistance request** (TARs) – ensures providers are immune to civil liability when voluntarily assisting agencies.
- **Technical assistance notice** (TANs) – establishes a legal obligation for assistance, where the assistance falls within a provider's existing business functions.
- **Technical capability notice** (TCNs) – allows Australia's First Law Officer, the Attorney-General, to require that a provider build a capability to assist law enforcement and national security agencies. The Minister for Communications must also agree before a notice can be issued.

These measures do not replace the need for agencies to obtain a warrant or authorisation to intercept communications, conduct digital surveillance, or access data. Rather, the framework is designed to facilitate the use of these underlying powers, and provide structure to law enforcement requests seeking help from industry.

All requests and notices provide civil immunity and limited criminal immunity. The starting position is that providers are to be compensated for the reasonable costs of complying with request or notice, and will receive civil immunity in relation to acts or things done in good faith to comply with a request or notice.

Is this a revolutionary approach?

No, the industry assistance measures are an evolution of existing arrangements. Traditional Australian telecommunications providers (carriers and carriage service providers) have long had an obligation to provide reasonably necessary assistance to Australian authorities under section 313 of the Telecommunications Act.

However, this regime does not recognise the growing role of new, innovative and global providers in the Australian communications supply chain. Part 15 of the Telecommunications Act addresses this limitation by ensuring agencies can seek the assistance of those companies best placed in the communications supply chain to support critical investigations and prosecutions.

Part 15 of the Telecommunications Act creates a new structure for industry assistance, introducing robust consultation, review, oversight and decision-making thresholds to maintain the security of devices and networks, and provide legal protection and certainty for companies.

Part 15 of the Telecommunications Act also reflects global approaches to the challenges posed by the evolving technological environment to law enforcement and intelligence services. The United Kingdom and New Zealand, for example, have their own regimes which ensures authorities can seek the assistance of companies in the communications supply chain.

How does the legislation interact with existing industry assistance?

Designated communications providers that fall into the category of ***carriers and carriage service providers*** may be subject to both the industry assistance measures in the Assistance and Access Act, and the assistance obligations under section 313 of the Telecommunications Act.

Under section 313, carriers and carriage service providers[1] must give Australian agencies such help as is reasonably necessary for (amongst other things) the enforcement of criminal law, protection of public revenue and safeguarding of national security. Any assistance provided under this regime must be in connection with the operation of telecommunications networks or facilities, or the supply of carriage services. Carriers and carriage service providers may continue to receive requests for help from agencies under section 313 particularly where there is an established procedure in place or a longstanding arrangement that has traditionally ensured the smooth delivery of assistance.

The industry assistance measures extend the existing assistance obligations in section 313 for carriers and carriage service providers to a wider class of communications provider including providers of electronic services, developers of software and manufacturers of devices. However agencies may use the industry assistance measures, instead of section 313, to obtain assistance from carriers and carriage service providers in instances where the provider requires certainty as to the assistance required, or further protections and safeguards.

Providers that are not carriers and carriage service providers[2] **cannot** be issued with a request under section 313.

[1] As well as carriage service intermediaries – entities that arrange for the supply by a carriage service provider of listed carriage services (see section 317C).
[2] Or carriage service intermediaries.

Scope of the laws

Who do the industry assistance measures apply to?

The industry assistance measures only apply to ***designated communications providers***, which are (in general terms) companies, businesses, organisations or individuals who contribute to the communications supply chain in Australia. A *designated communications provider* must supply or operate relevant products for use, or likely use, in Australia. This definition captures telecommunications operators, providers of electronic services, developers of software and manufacturers of devices.

The broad range of entities covered by the definition of *designated communications providers* reflects the global nature of the modern communications environment and the frequency with which communications services cross national boundaries.

It also reflects the rapid evolution of this dynamic industry where a diverse and ever-changing range of players are entering and exiting the Australian communications market.

For more details, refer to section 317C of the Telecommunications Act**.**

I am a *designated communications provider* **– will the framework apply to me?**

There are no standing obligations on designated communications providers under this framework. Providers are only required to take action under the framework when an agency serves a formal request or notice. Before a request or notice can be issued, the relevant authority must be satisfied that the provider is in a position to give necessary assistance to a national security or law enforcement matter (for reference, see sections 317P and 317V of the Telecommunications Act).

Practically speaking, the majority of companies who meet the definition of designated communications provider will not need to engage with the industry assistance framework.

My company operates globally – does assistance have to be connected to Australia?

Yes. Assistance can only be related to the services and products the provider offers, or operates, in the Australian market – Part 15 of the Telecommunications Act **does not** extend to a provider's activities that are unconnected with the supply and use of communications services and devices into Australia.

Can assistance be sought from individual employees of a company?

Requests for assistance are directed towards the designated communications provider entity itself. The industry assistance framework is about seeking help from relevant companies, not employees within that company. A notice would only be served on an individual in their capacity as an employee of designated communications provider. Alternatively, a notice may need to be served on an individual if that individual is a sole trader and is their own corporate entity.

Who can use the industry assistance measures?

The authorities that are able to use the industry assistance measures depend on the type of assistance required.

- **Technical assistance requests** may be issued by the head of the Australian Security Intelligence Organisation (ASIO), the Australian Signals Directorate (ASD), the Australian Secret Intelligence Service (ASIS), the Australian Federal Police (AFP), the Australian Criminal Intelligence Commission (ACIC), or a State and Territory police force.

- **Technical assistance notices** may be issued by the head of ASIO, AFP, ACIC and State and Territory police forces. The Commissioner of a State and Territory police force must also receive approval from the AFP Commissioner before issuing a notice.
- **Technical capability notices** may only be issued by the Commonwealth Attorney-General, with approval from the Commonwealth Minister for Communications, in accordance with a request made by ASIO, AFP, ACIC or a State and Territory police force.

An agency-head may also delegate their powers to senior executives within their organisation. The Commonwealth Attorney-General's power cannot be delegated to anyone else.

Agencies seeking assistance

For what purposes can agencies seek assistance?

Assistance may only be sought in relation to the ***relevant objective*** of the issuing agency. This means that:

- ASIO may only seek assistance in relation to their functions in safeguarding national security;
- ASD may only seek assistance in relation to their cyber security function;
- ASIS may only seek assistance regarding the interests of Australia's foreign relations or the national economic well-being; and
- law enforcement agencies (that are also interception agencies) may only seek assistance in relation to enforcing the criminal law for serious offences in Australia and overseas.

A serious offence means an offence with **a maximum penalty of at least three years imprisonment.** This three-year threshold matches the existing thresholds that law enforcement must satisfy to lawfully use surveillance device warrants or access communications data, like emails or SMS. The industry assistance framework is used in conjunction with underlying warrants. As such it is necessary to align the offence thresholds to ensure agencies can request assistance in relation to lawful investigations and operations that are critical to protecting the community.

What types of assistance may be sought?

The types of assistance that can be sought under the industry assistance measures are listed in the legislation. This includes providing technical information, concealing legitimate law enforcement or national security activities, or removing a form of electronic protection (where a provider is already able to do so for business purposes). Electronic protection is defined in the Telecommunications Act to include authentication and encryption. For more details, refer to section 317E or the examples of the types of assistance that can be sought by law enforcement and intelligence agencies in **Attachment A.**

Part 15 of the Telecommunications Act includes important safeguards to ensure requests for assistance do not require providers to do the impossible. A request for assistance must be ***practicable, reasonable, proportionate and technically feasible.*** Providers will not be asked to fundamentally change their operating procedures and that assistance will be targeted and limited to only what is necessary to achieve the relevant objectives of law enforcement and intelligence agencies.

What types of assistance cannot be sought?

Part 15 of the Telecommunications Act includes strong safeguards and limitations to ensure that providers are not issued with a request for assistance which may undermine the security of digital ecosystems or the privacy of those that are not the subject of an investigation.

The industry assistance measures cannot be used to introduce a ***systemic weakness*** or ***systemic vulnerability*** into a form of electronic protection. This means agencies cannot issue a request for assistance if it would result in so-called 'backdoors' being built or implemented into software or hardware.

Agencies cannot issue a request for assistance if it would inadvertently weaken the information security of other persons. This means that assistance may not be sought if it risks unlawful access to the information of a person unrelated to the investigation. This limitation ensures that the privacy and data security of the general public and business community remains intact.

Further, the measures cannot be used to compel a provider to build a decryption capability or make their encrypted systems less effective. Assistance also **cannot** be asked to prevent a provider from fixing a

security flaw in their products or systems or to compel a provider to build an interception or data retention capability.

The industry assistance framework does not replace or undermine the existing warrant regimes in Australian law – agencies must obtain a warrant or authorisation to allow for communication interception or access to data. This includes seeking Journalist Information warrants as required under the Data Retention Scheme, when agencies seek to access a journalist's data for the purpose of identifying a source.

These limitations are set out in **Division 7** of Part 15 in the Telecommunications Act.

How will companies be notified when issued with a formal request or notice seeking assistance?

In the vast majority of cases, providers will be consulted about the possibility of seeking assistance before any formal request or notice is issued – the default position is there should be no surprises. There are extensive consultation requirements set out in the legislation, and in practice preliminary engagement is encouraged even before formal consultation requirements kick in.

Following preliminary discussions, providers will be given a formal request or notice seeking assistance in writing. These written requests will include information on:

- the assistance required;
- the limitations of the powers, including the prohibition against weakening cybersecurity;
- the rights and obligations for providers; and
- the terms and conditions for giving assistance including cost recovery arrangements.

Assistance requests or notices may also be issued orally in situations where there is an imminent risk of serious harm to a person or damage to property, and it is not practicable to formally issue the assistance request in writing. In such rare circumstances, a written record of the request must be made within 48 hours, and given to the provider as soon as practicable after the record is made.

How will providers know if a request for assistance is genuine?

If providers believe a request or notice to be irregular or unlawful, they should contact the issuing agency to confirm its authenticity. Providers may also contact the relevant oversight body who will be notified of all authentic requests for assistance.

Obligations for providers

How long does a provider have to comply with a request for assistance?

The timeframes for providing assistance will vary depending on the nature of the assistance required and the urgency of the request. Beginning from when the notice was given, the default timeframes are:

- 90 days for technical assistance request.
- 90 days for a technical assistance notice.
- 180 days for a technical capability notice.

However, the duration of the assistance obligation and the period of compliance will be determined in consultation between the agency and provider, and specified in the request or notice itself. In making this determination, the agency is required to take into account the provider's business operations and development cycles.

What if the provider is unable to meet the timeframes in a request or notice for assistance?

The duration of the assistance obligation and the period of compliance will be determined in consultation between the agency and provider. The consultation requirements attached to the use of the industry assistance measures ensures providers have the opportunity to notify agencies of any practical issues that should be considered when determining the compliance timeframes. The timeframes for providing assistance will also be influenced by the nature of assistance required and the urgency of the request.

The Australian Government acknowledges that a provider's circumstances may change which can impact their ability to meet the timeframes agreed upon in the formal notice. To deal with such situations, an issuing agency may extend, vary or revoke the original notice to ensure the provider is able to assist as required. Providers should notify the relevant agency if such action may be required. However, the issuing agency has the ultimate discretion to extend, vary or revoke a notice requesting assistance.

Who will pay the costs of providing assistance?

In the case of voluntary requests, costs are agreed on a contractual basis between the provider and the agency. In the case of compulsory notices, the default position is that assistance will be provided on a no-profit, no-loss basis. During consultation, the agency and provider will work together to establish satisfactory financial arrangements and terms to ensure that providers do not bear the reasonable costs of compliance. In some cases it may be appropriate for providers to be remunerated beyond the costs of compliance. For example, agencies may establish commercial terms with a provider in cases where a large bespoke capability is required or the assistance needs to be actioned as a priority.

Providers will only be required to assist without compensation in very limited circumstances, notably where providing compensation would not be in the public interest. An example could be where a provider's conduct has wilfully created a security risk or specifically designed their services for illicit use.

Will providers be required to respond to the same request for assistance from multiple agencies?

In some cases, providers may be asked or required to comply with multiple requests for assistance concurrently.

In responding to multiple requests, providers should generally prioritise earlier requests first except in cases where the agency has notified the provider of urgent circumstances requiring the immediate actioning of a

request. It is important to remember that providers are required to comply with assistance obligations only to the extent that they are capable of doing so.

When providers are experienced at giving a certain type of assistance they may decide to waive consultation requirements to expedite timeframes for delivery and minimise the impact on their daily functions

Can information in relation to an assistance request be disclosed?

Information in relation to requests and notices cannot be disclosed. The use and disclosure provisions in the legislation are restrictive to protect law enforcement and national security capabilities, as well as to protect sensitive commercial information. There are exceptions – including that providers and their employees may disclose information where this is required to execute the request for assistance, to obtain legal advice or for the purpose of legal proceedings.

Companies can also report statistical information on any requests or notices received in company transparency reports or seek permission for that information to be on-disclosed to other relevant parties.

An employee who receives a request for assistance as a first point of contact between their employer and the law enforcement or intelligence agency, should on-disclose the request or notice to their superiors as required to fulfil its requirements.

Compliance, enforcement and review arrangements

Will providers be protected for actions undertaken to comply with an assistance obligation?

Yes. Providers, their employees and their agents will receive immunity from civil suit and specific computer offences for conduct done in good faith to comply with an assistance request or notice.

What if compliance with Australian law violates foreign laws?

Part 15 of the Telecommunications Act provides a defence against non-compliance if any offshore assistance required would contravene relevant foreign laws. The framework in Part 15 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.

What happens if a provider does not agree with a request or notice?

The industry assistance measures are designed to be collaborative by nature, and agencies and providers are expected to work together to achieve mutually agreeable outcomes. However, Part 15 of the Telecommunications Act contains multiple avenues for providers to challenge a request or notice to ensure that the measures are being used appropriately. These include:

- **Cost arbitration** – if the provider and agency fail to agree on cost arrangements related to a compulsory notice, an arbitrator may be appointed to resolve the dispute.
- **Independent review for TCNs** – providers will be informed of their right to seek independent review, from a former senior judge and a technical expert, on a proposed TCN before the notice is issued. This review mechanism gives the provider an opportunity to seek an independent assessment of a proposed TCN to determine if it would create a systemic weakness or vulnerability.
- **Judicial review** – if a provider does not consider a request or notice meets legislative requirements, they are able to seek judicial review of the decision to issue the request or notice under the *Judiciary Act 1903* (Cth).
- **Independent oversight** – providers will be informed of their right to complain to the relevant oversight body when issued with a request or notice. Agencies are required to notify the relevant oversight body when a request or notice is issued, varied, extended or revoked. These oversight bodies are responsible for overseeing and investigating agency conduct, including whether they have acted in a proper and lawful manner.

If a provider believes the required assistance is not *reasonable, proportionate, practicable* or *technically feasible* – they may make a complaint to the relevant oversight body. The relevant body for requests issued by law enforcement agencies is the Commonwealth Ombudsman, and for national security agencies is the Inspector-General of Intelligence and Security.

What happens if a provider does not comply with a notice?

If a provider refuses to comply with a requirement under a compulsory notice, they may be subject to enforcement proceedings. Enforcement proceedings are not expected to be used widely as agencies will continue to work with providers to ensure the requirements in a notice are met.

Non-compliance with a notice may have serious negative consequences for law enforcement and national security, which is why civil penalties apply to deter providers from contravening their legal obligations. These penalties include:

- **Companies** may face a maximum penalty of approximately AUD $10 million (or 47,619 penalty units)
- **Individuals** (who are sole traders, not employees within an organisation) may face a maximum penalty of approximately AUD $50,000 (or 238 penalty units)

The Commonwealth Communications Access Coordinator is the entity that pursues enforcement - not the requesting agency. Accordingly, providers will have an opportunity to make a case to the Coordinator regarding the reasons for non-compliance before the matter is referred to the Federal Court.

Safeguards and limitations

How will the provider's interests be taken into account?

The industry assistance measures include strong consultation requirements to ensure the provider's interests are considered when developing any request for assistance. Agencies are expressly required to consult with a provider when proposing to request their help. This recognises that providers are best placed to understand how their systems and products work, and reinforces that the scheme is about working in collaboration with industry.

Agencies must consider the potential impact on business operations, amongst other matters, when determining if a proposed request for assistance is *reasonable, proportionate*, *practicable* and *technically feasible*.

How does this legislation impact the security of networks and devices?

The industry assistance framework is designed to maintain and protect the security of networks and devices. The legislation expressly prohibits requesting assistance that would undermine electronic protection on a systemic level, including requests that would have the effect of inadvertently making the communications of the general public or business community less secure.

Agencies **cannot** require a company to:

- jeopardise information security, including by doing things that would increase the risk of hacking;
- weaken electronic protections applied across a range of services or devices (e.g. end-to-end encryption);
- refrain from patching a weakness; or
- build decryption capabilities.

These safeguards rule-out the construction of law enforcement keys or so-called 'exceptional access' systems.

Part 15 of the Telecommunications Act has **review** processes to assess whether a request meets the legislative requirements. Notably, providers are able to seek independent review of the technical and legal parameters of a proposed TCN, including to determine if a proposed request contravenes the prohibition against creating a systemic weakness and vulnerability. Providers are also able to seek judicial review of the decision to issue a notice if they believe the notice does not meet legislative requirements, including if a request contravenes the prohibition against systemic weakness and vulnerability.

How does the industry assistance framework protect personal information and private communications?

Part 15 of the Telecommunications Act contains strong safeguards and limitations to ensure that the industry assistance framework does not interfere with Australians' right to privacy. Access to personal information and private communications is governed by existing, separate warrant and authorisation regimes. In other words, the industry assistance measures do not allow agencies to compel providers to intercept communications, use surveillance devices or access data without an underlying warrant or authorisation permitting such an action.

The laws are about *assistance*, not information collection.

Further, providers cannot be asked to do anything that would require a data retention capability to be introduced, or fundamentally undermine the data security and cybersecurity of devices and networks. This is

designed to ensure that weaknesses or vulnerabilities are not inadvertently introduced into the technologies that we rely on to secure communications and data.

Does the Act impact Australia's ability to safely store data?

No, the security of data centres in Australia are not impacted by the legislation. Part 15 of the Telecommunications Act also includes a number of safeguards and legislative protections to ensure data security and cybersecurity are not compromised, including:

- prohibitions on actions that would introduce systemic weaknesses into technologies which prevents so-called *backdoors* from being introduced into devices and networks.
- decision-making criteria and consultation requirements to protect business interests, data security and cybersecurity, and privacy concerns of the Australian community.

The industry assistance measures are about seeking assistance, not about using this framework by itself to access content or data. Access to data remains subject to existing warrants and authorisations in Australian law.

Does Part 15 of the Telecommunications Act have implications for investment in Australia?

Australia remains a secure and reliable site for investment in, or related to, the telecommunications industry.

The industry assistance measures are designed to ensure Australian law enforcement can operate in the modern technological environment without imposing an undue regulatory or financial burden on communications providers, and without compromising products or services.

Part 15 of the Telecommunications Act includes no standing or ongoing obligations – providers will only be asked or required to assist authorities when served with a formal request or notice for assistance. A provider may give voluntary assistance on the terms they negotiate with the agency. For compulsory notices the default positon is that the reasonable costs of compliance will be compensated on a no profit/no loss basis.

The industry assistance measures do not require companies to fundamentally change the way they conduct their business operations in Australia. In seeking assistance, agencies are explicitly required to take into account the commercial interests of the provider to ensure that compliance with a request or notice does not undermine a provider's business operations. Further, prohibitions against jeopardising information security ensures that providers cannot be required to do things that will make their products less secure.

How can providers reassure their consumers, investors, contractors and stakeholders?

Part 15 of the Telecommunications Act is fundamentally about assistance – and contains provisions to ensure that assistance obligations have a minimal impact to providers' business operations and that the integrity of devices and systems remain intact. Companies' consumers and stakeholders can be assured that the industry assistance measures are subject to strong safeguards and limitations, comprehensive consultation requirements, robust oversight and independent scrutiny arrangements. Additionally, for public transparency, the Assistance and Access Act contains annual reporting requirements, to ensure that consumers and stakeholders can retain their trust in Australian companies and products.

To increase transparency and provide reassurance to providers, companies are able to make statistical disclosures to reveal the number of requests and notices received over the course of a six-month period. Companies may also disclose whether assistance provided over the six-month period was done so on a voluntary or mandatory basis. Publishing this information will allow providers to assure their consumers and stakeholders that they have either not provided assistance.

Subject to agreement and conditions from the relevant agency, companies may on-disclose information about any assistance given to interested parties, like suppliers or investors.

ATTACHMENT A – Types of industry assistance that can be requested under section 317E

Sub section 317E(1)	Listed act or thing	Examples
(a)	Removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider.	- Requesting an ISP provide the password they have enabled on a customer supplied home modem to facilitate a review of its logs during a search warrant to identify connected devices. - Requesting a cloud storage provider changes the password on a remotely hosted account to assist with the execution of an overt account based warrant.
(b)	Providing technical information	- An application provider providing technical information about how data is stored on a device (including the location of the encryption key) to enable forensically extracted data to be reconstructed. - An international cloud hosted storage provider providing details of where a customer's data is hosted to enable a Mutual Legal Assistance Treaty process to be progressed to the host country seeking lawful access. - A mobile device provider providing a copy of their WiFi AP location maps generated through bulk analysis of customers data to correlate with location records extracted during a forensic examination of a device.
(d)	Ensuring that information obtained in connection with the execution of a warrant or authorisation is given in a particular format.	- Requesting a cloud service provider provide a copy of the contents of a hosted account in a particular format pursuant to the execution of an overt account based warrant. - Requesting that data held in a proprietary file format extracted from a device during a forensic examination pursuant to an overt search warrant is converted into a standard file format.
(e)	Facilitating or assisting access to that which is the subject of eligible activities of the provider including, a facility, customer equipment, an electronic service etc.	- Requesting a shared data centre provide access to customers computer rack to enable the execution of a computer access warrant or installation of a data surveillance device under warrant.
(f)	Assisting with the testing, modification, development or maintenance of a technology or capability.	- Requesting that a social media platform assist with testing or development of a tool to automate the creation of online personas and historical content to facilitate online engagement.
(g)	Notifying particular kinds of changes to, or developments affecting, eligible activities of the designated communications provider, if the changes are relevant to the execution of a warrant or authorisation.	- Requesting an ISP advise of any technical changes to their network which could impact on an existing interception.

Sub section 317E(1)	Listed act or thing	Examples
(h)	Modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider.	- Requesting a carrier increase the data allowance on a device that is subject to a surveillance device warrant to enable the surveillance device to be remotely monitored without consuming the target's data. - Temporarily blocking internet messaging to force a device to send the messages as unencrypted SMS's.
(i)	Substituting, or facilitating the substitution of, a service provided by the designated communications provider for: another service provided by the provider; or a service provided by another designated communications provider.	- Requesting a carrier force a roaming device to another carriers network to enable the enhanced metadata collection capabilities of the new carrier to collect information pursuant to a prospective data authorisation.
(j)	An act or thing done to conceal the fact that anything has been done covertly in the performance of a function, or the exercise of a power, conferred by a law of the Commonwealth, a State or a Territory, so far as the function or power relates to: - enforcing the criminal law and laws imposing pecuniary penalties; or - assisting the enforcement of the criminal laws in force in a foreign country; or - the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.	- Requesting that the provider not inform the customer of the assistance provided to enable a computer access warrant. - Requesting that the provider delete an audit log in a customer's device relating to a computer access warrant. - Requesting a provider restore a password that was temporarily changed to enable a computer access warrant. - Requesting a provider allocate a specific dynamic IP address relating to remote access pursuant to a computer access warrant to conceal the access.