Australian Government
Department of Communications and the Arts

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

June 2017

Disclaimer

The material in these guidelines are of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in these guidelines.

Copyright

Introduction

These whole-of-government guidelines have been released in response to the June 2015 report, *Balancing Freedom and Protection: Inquiry into the use of subsection 313(3) of the Telecommunications Act 1997 by government agencies to disrupt the operation of illegal online services* by the former House of Representatives Standing Committee on Infrastructure and Communications.[1]

In July 2014, the then Minister for Communications referred the use of section 313 of the *Telecommunications Act 1997* to disrupt access to online services to the Committee for inquiry and report. The Minister made the referral following the inadvertent disruption of a number of online services in 2013 as a result of a request relying on section 313(3). The incident prompted concerns about the transparency and accountability associated with such requests, as well as in regard to technical implementation.

In its report, the Committee recommended that the Australian Government adopt whole-of-government guidelines for the use of section 313 by government agencies to disrupt access to online services. The Committee also recommended that agencies using the section to disrupt access to online services have the requisite level of technical expertise to carry out such activity or have access to the expertise

In its response to the report, the Australian Government indicated that it supported the Committee's recommendations.

Scope

These guidelines relate to government agencies' use of section 313(3) to request internet service providers disrupt access to certain online services by blocking websites.[2] These guidelines do not cover other requests for assistance made under section 313.

Section 313(3) of the *Telecommunications Act 1997* requires that carriers and carriage service providers, in connection with their operation of telecommunications networks and facilities or the supply of carriage services, give officers and authorities of the Commonwealth, states and territories such help as is reasonably necessary to:

- enforce the criminal law and laws imposing pecuniary penalties;
- assist in the enforcement of the criminal laws in force in a foreign country;
- protect the public revenue; and
- safeguard national security.

[1] The report is available at http://www.aph.gov.au/Parliamentary_Business/Committees/House/Infrastructure_and_Communications/Inquiry_into_the_use_of_section_313_of_the_Telecommunications_Act_to_disrupt_the_operation_of_illegal_online_services/Report.

[2] For example, the Australian Federal Police has used the section to disrupt access to child exploitation material on the INTERPOL 'Worst of' list and for instances of cybercrime.

Applicability

These guidelines apply to Australian Government agencies. State and Territory agencies are encouraged to follow these guidelines should they rely on section 313(3) to disrupt access to online services.

Good practice use of section 313(3) to disrupt online services

A summary of good practice measures for agencies to follow when making section 313(3) requests is provided below. These are consistent with the recommendations of the House of Representatives Standing Committee on Infrastructure and Communications and are further explained on the following pages.

The measures promote the transparent, accountable and responsible use of the section while recognising that agencies have different operational needs. Such an approach helps ensure that agencies online disruption activities are effective and in line with community expectations.

Summary of good practice measures

1. Obtain authority from the agency head as a minimum to be able to make use of section 313(3) to disrupt access to online services
   - Ensure each request to an internet service provider is approved by an Senior Executive Service officer or equivalent
2. Develop, maintain and publish internal policies and procedures for disruption requests
   - Specify how long a disruption is to remain in place
   - Monitor and evaluate disruptions
3. Limit disruptions to serious criminal or civil offences, or threats to national security
   - Make requests as targeted as possible
   - Consult internet service providers prior to making a request
4. Provide information to the public through media releases, online posts, 'stop pages' and annual reporting
5. Have procedures in place to support complaints and reviews
6. Have access to the appropriate technical expertise.

1. Authority and subsequent approvals

Agencies should obtain the authority of their agency head as a minimum to use section 313(3) to disrupt online services. The authority should set out delegations for approving individual requests to disrupt access to online services. The level of officer with the delegated authority should be a Senior Executive Service officer or equivalent, and be specified in the agency's internal policies and procedures.

2. Policies and procedures

To promote transparency and consistency, agencies that utilise or foresee utilising section 313(3) to disrupt online services in the short to medium term should develop and maintain policies and procedures for disruption requests.

Where an agency is not able to apply all of these guidelines due to operational, security or other reasons, it should document such departures in its policies and procedures.

Agencies should publish their policies and procedures online, noting that Australian Government agencies may be required to do so under the Information Publication Scheme contained in the *Freedom of Information Act 1982* (Cth).

Where it would not be appropriate to publish the entire set of policies and procedures, agencies should consult their portfolio Minister on the decision not to publish. At a minimum, agencies should publish a statement on their website noting that they may make requests to disrupt access to online services in reliance on section 313(3), but have determined that it would be inappropriate to publish specific policies and procedures.

Section 313(3) requests to disrupt access to online services should expire after a specified time. Agencies should evaluate their processes and the outcome after each disruption. With the transient nature of the internet, agencies should have 'self-review' procedures to monitor ongoing disruptions and ensure they remain appropriate.

3. Limiting disruption

Agencies should limit use of section 313(3) in disrupting access to online services to cases involving serious criminal or civil offences, or threats to national security. An appropriate threshold would be offences that carry a maximum prison term of at least two years or, if the offence does not carry a prison term, a financial penalty of at least 120 Commonwealth penalty units.[3]

Australia has committed to promoting an open, free and secure Internet.[4] Agencies should consider this commitment alongside a variety of factors when determining whether a request to disrupt access is appropriate. General factors that should always be considered are:

- the availability of other enforcement tools;
- the services on the site;
- the likely effectiveness of the disruption;
- the view of the Internet Service Provider (ISP);
- technical feasibility and costs;
- potential consequences and/or damage to government;
- the nature of the offence; and
- whether there is a public or national interest to do so.

Agencies should specify, in their internal policies and procedures, the types of activities that may be subject to a section 313(3) request.

4. Public information

Providing timely and relevant information to the public about disruption requests improves transparency and will help to increase public awareness about section 313(3).

Agencies should publish each request and include (wherever practicable and reasonable in the particular circumstance) why the request has been made. Public notification can occur through means such as media releases and online posts.

[3] The formula in section 4B of the *Crimes Act 1914* (Cth) has been used as a guide to determine the equivalent financial penalty. At the time of writing, a penalty unit under Commonwealth law was $180, therefore the financial penalty threshold was $21,600.

[4] Australia's Cyber Security Strategy, April 2016.

As part of the notification agencies may also choose to provide information about online criminal activity and support for victims, such as links to the Australian Cybercrime Online Reporting Network (ACORN).

Agencies should provide ISPs with a generic government 'stop page' to be shown to members of the public if they try to access a disrupted site. The 'stop page' should include, where appropriate:

- the name of the agency requesting the disruption;
- the reason (at a high level) that the disruption has been requested;
- an agency contact point via a telephone number and email for more information; and
- information about how a party adversely affected by the disruption could make a complaint or seek a review (see below).

Agencies should also report use of section 313(3) to disrupt access to online services to the Australian Communications and Media Authority (ACMA) for inclusion in the ACMA's Annual Report (the Report). The Report will provide statistical information about the use of section 313(3). Agencies should report within one month after the end of the financial year, or as determined by the ACMA.

For the purposes of these guidelines, the role of the ACMA is to collect and report statistical information about disruption requests under section 313(3), and to be a single repository of this information. This role will improve the overall transparency around the disruption of online services. Information provided by agencies to the ACMA, and which will be published in the Report, should include:

- the authority to use section 313(3) for disruption requests (including when and by whom the authority was provided);
- the existence of internal policies and procedures for disruption requests (including whether they have been published online, the relevant web address or the reason why they have not been published (Agencies may use a web address to provide further information);
- any requests made to ISPs to disrupt online services in reliance on section 313(3) in the previous 12 months (including the number of requests, reasons[5] and number of websites blocked).[6]

Agencies are not required to publish requests where the report may jeopardise ongoing or planned investigations, operational activities or give rise to other law enforcement or national security concerns. Agencies with requests of this nature should provide an annual aggregate number of requests to the ACMA for publication.

5. Complaints and review

In line with established accountability practices, agencies internal policies and procedures should set out complaints and review processes that allow affected parties to contest a decision to disrupt access. The policies and procedures should provide avenues for both internal and external complaints, and should include review mechanisms. Affected parties should be assisted by the agency, rather than being directed to the carrier or carriage service provider.

Agencies should review a disruption upon request by an affected party within timeframes consistent with their established complaints and review procedures. Agencies should contact the relevant carrier

[5] The reason for the request would be the relevant category in paragraphs (c) to (e) of section 313(3).
[6] A form detailing what to report and when is available at http://www.acma.gov.au/theACMA/reporting-template-for-commonwealth-agencies.

or carriage service provider to arrange for the disruption to be lifted if their review reveals that the disruption is no longer appropriate.

6. Technical implementation

Agencies should have the requisite level of technical expertise to disrupt services under section 313(3), or procedures for drawing on the expertise of other agencies or external experts to do so. This will help ensure that requests are effective, responsible, and able to be executed appropriately.

Prior to making a request, agencies should consult ISPs about how assistance may be best provided. This will also assist in managing costs.[7]

Agencies should note that ISPs use different methods to block websites and when making a request, agencies should endeavour to make it as targeted as possible and consider the method used by the ISP. This will usually mean requesting that a Domain Name System (DNS) and/or Uniform Resource Locater (URL)—the specific address of a website—be blocked, rather than Internet Protocol (IP) addresses. Requests to block IP addresses risks disrupting access to non-target websites as IP addresses generally host multiple websites.[8]

[7] Under section 314 of the *Telecommunications Act 1997*, a carrier or carriage service provider can recover its costs of providing help under section 313(3) from the relevant government agency on the basis that it 'neither profits from, nor bears the costs of' giving that help.

[8] The inadvertent disruption of websites in 2013 was the result of a request that IP addresses be blocked.

Diagram: overview of good practice arrangements