Australian Government

Department of Communications

Submission to the House Standing Committee on Infrastructure and Communications

Inquiry into the use of section 313(3) of the *Telecommunications Act 1997* by government agencies to disrupt the operation of illegal online services

September 2014

GPO Box 2154 Canberra ACT 2601 Australia • telephone 02 6271 1000
• website http://www.communications.gov.au

Contents

1. Introduction 3
2. Section 313 3
3. Agency use of section 313 5
4. Rationale 5
5. Issues with current application of section 313 5
6. Proposed reforms 6
   6.1. Development of services disruption procedures 6
   6.2. Services 7
   6.3. Approval to disrupt access to services 7
   6.4. Announcement of disruption 7
   6.5. Technical implementation 7
   6.6. Stop pages 8
   6.7. Review and appeal 8
   6.8. Reporting 9
7. Summary of proposals 9

1. Introduction

Consistent with Article 19 of the International Covenant on Civil and Political Rights, the Australian Government believes that every individual has the right to freedom of expression, including the right to freely seek, receive and impart information and ideas of all kinds through any media, including the internet.

Also consistent with Article 19, the Australian Government recognises that some limitations on freedom of expression are necessary to protect individuals, national security, public order, and public health or morals. These thresholds are already recognised offline: for example, views or content that represent an incitement to violence or child exploitation are acknowledged criminal activities.

In limited circumstances and consistent with these principles, Australian Government agencies have sought the assistance of internet service providers (ISPs) to disrupt access to certain illegal online services through the blocking of access to websites. These requests have been actioned under section 313 of the *Telecommunications Act 1997* (the Act).

The use of section 313 for this purpose, in one particular instance, has been the subject of considerable media criticism. The Department considers that much of this criticism was less about the *type* of service which had been disrupted and more about *how* it had been disrupted. Concerns were raised that the processes around disruption lacked sufficient transparency and accountability – it was unclear to the public why access to services had been disrupted or which agency was responsible.

In light of this, the Committee could consider whether improvements can be made to strengthen transparency and accountability with a view to improving public awareness and perception of the use of section 313 to disrupt access to illegal online services. The Department does not consider it necessary that this be achieved through legislative amendment. Rather, we suggest that it could be achieved through the development of whole-of-government principles to guide Australian Government agency use of the provisions to disrupt access to illegal online services.

2. Section 313

Section 313(3) of the Act requires carriers and carriage service providers in Australia to give officers and authorities of the Commonwealth, and of the states and territories, such help as is reasonably necessary to:

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

Section 313(3) supports carrier and carriage service provider obligations under section 313(1), which requires them to do their best to prevent their networks and facilities from being used in, or in relation to, the commission of offences against the laws of the Commonwealth or of the states and territories. Under section 313(5), carriers and carriage service providers enjoy immunity for complying with these obligations, so long as their actions are in good faith.

Section 313 has antecedents in the Telecommunications Acts of 1989 and 1991. Section 26 of the 1989 Act was a precursor to section 313(1):

TELECOMMUNICATIONS ACT 1989 No. 53, 1989 - SECT 26

AUSTEL and carriers to prevent use of networks and facilities in commission of offences

26. AUSTEL and each of the carriers shall, in exercising their respective powers, use their best endeavours to ensure that telecommunications networks and facilities operated by the carriers are not used in, or in relation to, the commission of offences against the laws of the Commonwealth and of the States and Territories.

Likewise, section 47 of the 1991 Act provided the basis for the current section 313 provisions set out in the *Telecommunications Act 1997*:

TELECOMMUNICATIONS ACT 1991 No. 98 of 1991 - SECT 47

AUSTEL, carriers and service providers to prevent use of networks and facilities in commission of offences

47(1) AUSTEL, the carriers, and the persons who supply eligible services, must, in exercising their respective powers, do their best to prevent telecommunications networks and facilities operated by carriers, or by such persons, from being used in, or in relation to, the commission of offences against the laws of the Commonwealth and of the States and Territories.

(2) AUSTEL, the carriers, and the persons who supply eligible services, must give to officers and authorities of the Commonwealth and of the States and Territories such help as is reasonably necessary for any of the following purposes:

(a) enforcing the criminal law and laws imposing pecuniary penalties;
(b) protecting the public revenue;
(c) safeguarding national security.

(3) AUSTEL is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in performance or purported performance of the duty imposed by subsection (1) or (2).

...

The provisions were drafted with the intent of providing officers and authorities of the Commonwealth, states and territories reasonable flexibility as to the type of assistance that could be sought from the telecommunications industry in support of law enforcement. It is important to note that the type of assistance provided depends on the nature of the request. For example, section 313 is predominantly used by agencies to support information requests and interception warrants that are authorised under the *Telecommunications (Interception and Access) Act 1979* (the TIA Act). Carriers and carriage service providers are required to report to the Australian Communications and Media Authority (ACMA) on any disclosures that are authorised under either Part 13 of the Act or Chapter 4 of the TIA Act.

There have been a number of instances where the assistance sought by government agencies has been in the form of a request to ISPs to disrupt access to certain illegal online services through the blocking of access to websites. It is the use of the provisions for this purpose that the Inquiry, and

this submission, seek to address. The Department understands that the use of section 313 for other purposes is not within the Inquiry's Terms of Reference.

3. Agency use of section 313

The use of section 313 by Australian Government agencies to disrupt access to illegal online services does not appear to be widespread. Following the inadvertent blocking of the Melbourne Free University website in April 2013, the Department contacted government agencies in order to quantify Australian Government use of the provisions for this purpose.

In response, agencies advised that over the 2011-2012 and 2012-13 reporting periods, a total of 32 requests had been made using section 313 to disrupt access to illegal online services. This included 21 requests by the Australian Federal Police (AFP) to disrupt access to domains on the INTERPOL "Worst of" list of child exploitation material, ten requests by the Australian Securities and Investments Commission (ASIC) to disrupt access to websites engaged in financial fraud, and a single request by an agency in the Attorney-General's portfolio to disrupt access to services on counter terrorism grounds. The Department has not been made aware of any further government agency use of the provisions to disrupt access to online services, but notes that agencies are under no obligation to report such use.

The Department is not aware of any state, territory or local government authority seeking assistance from ISPs to disrupt access to online content or services.

4. Rationale

Disrupting access to illegal online services is one of a number of legitimate law enforcement options available in response to criminal online activity. Other options may include having the material removed and, where possible, prosecution of offenders; however, the actual option chosen in any given situation is determined on a case-by-case basis.

As previously noted, government agency use of section 313 to seek assistance to disrupt access to illegal online services appears to have been relatively uncommon. However, there are arguably public benefits to disrupting access to such websites in certain circumstances. For example, ASIC requested that access to certain foreign-based websites be disrupted to help prevent Australians, often retirees, becoming the victims of serious financial fraud. AFP disruption of domains on the INTERPOL list helps prevents access to child exploitation material. And intelligence agencies may also consider it necessary to disrupt access to services that promote or facilitate terrorist activities representing a significant or immediate threat to security and lives.

5. Issues with current application of section 313

There has been criticism that government agency use of section 313 to disrupt access to illegal online services constitutes a policy of broad-based internet filtering. This is not the case. Broad-based filters typically block access to all instances of a specific category of services; for example, all webpages containing online gambling or featuring images or descriptions of pornography.

In contrast, the disruption of access to online services under section 313 to date has been a targeted response to specific instances of illegal services. The types of services that can be targeted are restricted by section 313(3) of the legislation, and disruption of access is typically only requested where an agency considers there is a strong public or national interest to do so. A decision to disrupt

access to a service is specific to that instance. To disrupt access to other, similar services requires a separate request which needs to be considered on its own merits by the relevant agencies.

Another criticism is that the processes around disruption often lack transparency and accountability. The Department considers this to be a valid concern. The problem was demonstrated by the inadvertent disruption of access to the Melbourne Free University website in April last year, during which both users and site owners were unaware that access to the site had been disrupted, which government agency had requested the disruption, and where to go to have the issue resolved.

6. Proposed reforms

To date the number of sites captured by section 313 requests appears to have been very limited, with applications focused on enforcing the criminal law or addressing serious threats to national security. The Department suggests that agencies continue to be responsible for issuing their own notices under section 313 and that the application of section 313 to disrupt access to online services should remain confined to what is specified in the legislation. However, the Department is of the view that the use of section 313 by Australian Government agencies should be subject to a greater degree of transparency and accountability.

To this end, we propose that the Committee consider whether the Government should develop whole-of-government principles to guide Australian Government agency use of the provisions to disrupt access to illegal online services. These principles would range from high-level guidance aimed at meeting the policy objectives set out in legislation, to specific directions and mechanisms which would outline how requests to disrupt access should be applied and reported.

The Department suggests that such principles reflect Australia's positions and obligations which support an open internet. This includes the right to freedom of expression online which increases government transparency and enables innovation, international trade and economic prosperity.

The Department suggests that these whole-of-government principles require agencies to develop internal 'services disruption procedures' consistent with the principles. This will support a coordinated and transparent approach to the application of section 313 across Australian Government agencies.

6.1. Development of services disruption procedures

The Department recommends the Committee consider that, under the whole-of-government principles, individual agencies intending to use section 313 to disrupt access to illegal online services be required to develop and maintain 'services disruption procedures' that clearly outline the internal processes to be followed when disrupting access to illegal online services.

Agencies developing services disruption procedures would be required to consider their existing obligations under the mandatory publication requirements of the Information Publication Scheme (IPS) contained in Part II of the *Freedom of Information Act 1982*. The IPS requires agencies to publish specified categories of information on their website and provides the discretion to publish other information. It is likely that any services disruption policy developed by agencies would fall under the mandatory IPS category of 'operational information', meaning that it must be published online.

Where it would not be appropriate to publish procedures, for operational or security reasons, the Department suggests these should be made available for appropriate scrutiny, despite not being made public. This could involve examination *in camera* by a relevant Parliamentary committee.

6.2. Services

Under existing arrangements, the precise processes involved in issuing a section 313 request vary from agency to agency. Agencies consider a variety of factors in determining whether a request to disrupt access is appropriate, including the availability of other enforcement tools, the services on the site, and the criminal offence that the website is being used to facilitate.

The Department considers that transparency around this process would be improved by better clarifying the types of services that may be the subject of access disruption. Notwithstanding the flexibility inherent in the legislation, and recognising Australia's position and obligations which support an open internet, the Department is of the view that such action should only occur in cases involving serious criminal activity or threats to national security. To assist agencies in making a determination, we suggest the whole-of-government principles articulate a clear threshold. The Department suggests an appropriate threshold might be illegal services or activities that carry a maximum prison term of at least two years (or financial penalty with a degree of equivalence under criminal and civil law).

6.3. Approval to disrupt access to services

As an improved accountability measure, the Department proposes that agencies intending to disrupt access to online services under section 313 be required to seek the approval of their agency head (or portfolio Minister if deemed appropriate) prior to implementing a services disruption policy. This would be a once-off approval establishing an agency as one which may seek to use section 313 to disrupt access to illegal online services in the future. It is suggested that such approval would also set out who in an agency (i.e. what level of officer) would be authorised to make subsequent requests under section 313 to disrupt access to services. This should be reflected in the agency's services disruption procedures.

6.4. Announcement of disruption

On a case-by-case basis, particularly where doing so does not jeopardise ongoing investigations or other law enforcement or national security concerns, the Department suggests that agencies publicly announce, through means such as media releases or agency website announcements, instances where it issues a request to have access to a service disrupted. These announcements would include an explanation of why the request has been sought.

This would serve to both improve the transparency around the decision to disrupt access, while also drawing additional public attention to a particular problem. ASIC, for example, in many cases issued media releases when requesting that access to websites providing fraudulent financial services be disrupted. These media releases included useful information for consumers about how to avoid falling victim to such fraud, and where to report suspicious activity.

6.5. Technical implementation

Given the potential negative consequences, it is important that the technical implementation of any disruption is appropriate. For example, errant disruption may cause financial or reputational damage to legitimate service owners who rely on their online presence. The Department suggests that agencies considering such action should consult across government and relevant stakeholders (such as ISPs) to ensure that the measures outlined in their services disruption procedures are effective, responsible and appropriate.

6.6. Stop pages

The Department proposes that when requesting that ISPs disrupt access to illegal online services, agencies provide ISPs with a generic government stop page (similar to that used by the INTERPOL scheme when preventing access to online child exploitation material). It is suggested that these pages would, where appropriate, include the following information:

- the agency which made the request;
- the reason, at a high level, why the request was made;
- an agency contact point for more information; and
- how to seek a review of the decision to disrupt access.

The Department acknowledges that it may be necessary to have different approaches for different disruption requests. For example, the stop pages for domains blocked under the INTERPOL scheme currently state that the domain has been blocked because it contains child exploitation material. Other stop page notifications, particularly where there is the potential for operational activities to be jeopardised, may not include reasons, or indeed may not be used at all.

6.7. Review and appeal

An agency's 'services disruption procedures' should clearly set out review and appeal processes to allow affected parties an opportunity to question or contest any disruption of access. This should include both internal and external review of decisions.

The 'services disruption procedures' should allow for self-review of any ongoing requests to disrupt access. While requests to ISPs to disrupt access to illegal services would ideally specify how long a disruption is to remain in place, this may not always be possible. Given the transient nature of much of the internet, and that internet addresses are transferable, agencies should have procedures in place to periodically review disrupted services to ensure that the disruption remains valid.

A common sense and pragmatic form of internal review would be for an agency to reassess any access disruption at the request of a complainant. It is expected that, in most instances, this form of review would quickly resolve concerns. Of course, this can only operate effectively if the agency provides contact information through use of a stop page, a public announcement, or both. In cases where services have been disrupted unintentionally, the responsible agency can, once informed, ask the relevant ISPs to cease the disruption. Alternatively, if the responsible agency is of the view that the disruption is necessary and appropriately targeted, it can relay the rationale for this to the complainant.

In the event that informal approaches do not produce an outcome satisfactory to a complainant, it is possible that the complainant could seek a declaration from a court that the disruption is unlawful, and an injunction requiring the service to be reinstated. The *Administrative Decisions (Judicial Review) Act 1977* is one avenue of external appeal. Another option may be to lodge a complaint with the Commonwealth or State Ombudsman.

An agency-led process for disrupting access to online services, with the availability of appropriate review mechanisms, is preferred by the Department to an approach which begins with a judicial process. The latter can often be a lengthy and costly process, and websites and hosting locations can shift and change rapidly during this time. In addition, the continued availability of the services during this period can have serious ramifications. A good example of this is websites involved in the perpetration of illegal investment scams and frauds, which may affect many people and have serious financial consequences if they remain active for even a short period of time. The agency-led process will be contestable under existing and proposed review arrangements.

6.8. Reporting

As an additional transparency measure, the Department proposes that the use of section 313 to disrupt access to illegal online services be reported to the ACMA for inclusion in the ACMA's Annual Report. This measure would improve transparency around the disruption of access to services under section 313 by providing a single repository of this information.

The Department acknowledges that in certain circumstances, reporting of the use of section 313 to disrupt access to online services may jeopardise ongoing investigations, particularly where it relates to matters of national security. In these circumstances, we recommend reporting to an appropriate Parliamentary committee on an *in camera* basis.

7. Summary of proposals

The Department proposes the Committee consider the development of whole-of-government guidelines to guide Australian Government agency use of section 313 to disrupt access to illegal online services, which would specify minimum requirements and recommended procedures to follow when seeking to disrupt such services. These guidelines would require agencies to:

1. develop agency-specific internal policies outlining their own procedures for requesting the disruption of acess to online services (recognising that agencies will have different requirements based on their operational activities);

2. seek clearance from their agency head (or Minister) prior to implementing a service disruption policy for illegal online services as part of their operational activities;

3. ensure that disruption of services is limited to specific material that draws a specified penalty (for example, a maximum prison term of at least two years, or financial equivalent);

4. consult across government and relevant stakeholders (such as ISPs) to ensure that the technical measures outlined in their services disruption policies are effective, responsible and appropriate;

5. use stop pages where operational circumstances allow, and include, where appropriate:

    - the agency requesting the block;
    - the reason, at a high level, that the block has been requested;
    - an agency contact point for more information; and
    - how to seek a review of the decision;

6. publicly announce, through means such as media releases or agency website announcements, each instance of requesting the disruption of access, where doing so does not jeopardise ongoing investigations or other law enforcement or national security concerns;

7. have internal review processes in place to quickly review a block, and potentially lift one, in cases where there is an appeal against the block; and

8. report blocking activity to the ACMA, or where operational circumstances make this impossible or impractical, to the appropriate Parliamentary committee.