
The Parliament of the Commonwealth of Australia

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**

House of Representatives
Standing Committee on Infrastructure and Communications

June 2015
Canberra

© Commonwealth of Australia 2015

ISBN 978-1-74366-332-5 (Printed version)

ISBN 978-1-74366-333-2 (HTML version)

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Australia License.



The details of this licence are available on the Creative Commons website: <http://creativecommons.org/licenses/by-nc-nd/3.0/au/>.



Contents

Foreword	v
Membership of the Committee	vii
Terms of reference	ix
List of abbreviations	xi
List of recommendations	xiii
1 Introduction	1
Referral and conduct of the Inquiry.....	1
Brief overview of section 313.....	2
Structure of the report.....	3
2 Use of section 313 by agencies.....	5
The need for s.313.....	5
Actual use to date	8
The ASIC incident	10
Enforcing compliance.....	12
Defining the use of s.313.....	15
Committee conclusions.....	20
3 Transparency and accountability.....	23
Transparency and accountability	23
Use of warrants and judicial oversight.....	27
Use of block pages	29
Review and appeal	32
Reporting	34

Oversight	36
Committee conclusions.....	39
4 Technical issues.....	41
Technical limits of disrupting online activity.....	41
Costs	47
Avoiding disruption of non-target sites	49
Committee Conclusions	51
5 Legislation, regulation or policy?	53
Guidelines	59
Committee conclusions.....	62
Appendix A – Part 14, <i>Telecommunications Act 1997</i>.....	65
Appendix B – List of Submissions.....	71
Appendix C – Public hearings & witnesses.....	73



Foreword

One of the significant challenges faced by all governments is the need to balance the safety of the community with the rights of the individual – rights that are vital to a healthy democracy and an accountable government – in this case, freedom of speech.

The internet has brought with it unprecedented economic and social opportunities – it has transformed the way we live and work – undoubtedly for the better. But there are some in our community, and abroad, who seek to use it for corrupt purposes.

The examples are varied and many. The internet has created new markets but also the means for producers and peddlers of child abuse material. It has provided a global forum for terrorist organisations and recruiters, and has put these organisations within easy reach of impressionable young people. It has facilitated the trade of illicit goods and services, and allowed scammers to anonymously target vulnerable people for their hard-earned money and personal information.

How we deal with these threats is a question of balance. To do nothing would constitute an abdication of duty – but to go too far would risk trampling those very rights and freedoms we seek to protect. So too, an overzealous censorship programme would muffle the critical voice of the electorate, and erode the accountability of government.

The Infrastructure and Communication Committee has grappled with these questions, and I believe has struck the right balance between competing priorities. The Committee examined the appropriateness and efficacy of using Section 313 of the *Telecommunications Act 1997* to disrupt illegal online services, and has determined that there remains an indisputable need for government agencies to have access to these powers.

The Committee, in its Report, acknowledges past mistakes, and sets out a way forward for the effective use of s.313 by government agencies.

The Committee thoroughly examined the twenty-one submissions offered and the evidence of twenty-three witnesses, and formulated two key recommendations which we believe will ensure that future uses of s.313 by government agencies are appropriate, targeted, and effective. The submissions received were diverse and challenging, and the report is better for that.

My appreciation goes to the witnesses who offered submissions, and whose insights informed the Committee's Final Report. I also wish to thank my colleagues for their constructive contribution, and the Committee Secretariat for the significant way in which they have supported the work of the Committee.

Mrs Jane Prentice MP
Chairman



Membership of the Committee

Chairman Mrs Jane Prentice MP

Deputy Chair The Hon Matt Thistlethwaite MP

Members Mr Andrew Giles MP

Ms Melissa Price MP

Ms Nola Marino MP

Ms Michelle Rowland MP

Mr Clive Palmer MP

Mr Bert van Manen MP

Mr Keith Pitt MP

Mrs Lucy Wicks MP

Committee Secretariat

Secretary	Mr Stuart Woodley
Inquiry Secretary	Dr Bill Pender
Research Officer	Ms Belynda Zolotto
Administrative Officer	Ms Cathy Rouland



Terms of reference

Section 313 of the *Telecommunications Act 1997* provides that carriers or carriage service providers must, in connection with:

- (a) the operation by the carrier or provider of telecommunications networks or facilities; or
- (b) the supply by the carrier or provider of carriage services;

give officers and authorities of the Commonwealth and of the States and Territories such help as is reasonably necessary to:

- (c) enforce the criminal law and laws imposing pecuniary penalties;
- (ca) assist the enforcement of the criminal laws in force in a foreign country;
- (d) protect the public revenue; or
- (e) safeguard national security.

Section 313 provides Australian government agencies (including state government agencies) with the ability to obtain assistance from the telecommunications industry when upholding Australian laws. The Australian Federal Police (AFP) administers the Access Limitation Scheme which uses section 313 to block domains (websites) which contain the most severe child sexual abuse and exploitation material using the INTERPOL 'Worst of' child abuse list. When a user seeks to access one of these sites, they are provided a block page that provides certain information, including reasons for the block, and contact details for any dispute about inclusion of the listing on the INTERPOL list. Other Commonwealth agencies have also in the past used section 313 to prevent the continuing operation of online services in breach or potentially in breach of Australian law (e.g. sites seeking to perpetrate financial fraud).

How law enforcement agencies use section 313 to request the disruption of such services is an important public policy question. Section 313 is also used for other purposes, but the Committee will inquire solely into and report on government agency use of section 313 for the purpose of disrupting illegal online services.

The Committee is to consider:

- (a) which government agencies should be permitted to make requests pursuant to section 313 to disrupt online services potentially in breach of Australian law from providing these services to Australians
- (b) what level of authority should such agencies have in order to make such a request
- (c) the characteristics of illegal or potentially illegal online services which should be subject to such requests, and
- (d) what are the most appropriate transparency and accountability measures that should accompany such requests, taking into account the nature of the online service being dealt with, and what is the best/appropriate method for implementing such measures:
 - a. Legislation
 - b. Regulations, or
 - c. Government policy.

A final report is to be provided by 1 July 2015.



List of abbreviations

ACC	Australian Crime Commission
ACCAN	Australian Communications Consumer Action Network
ACMA	Australian Communications and Media Authority
AFP	Australian Federal Police
A-GD	Attorney-General's Department
ALHR	Australian Lawyers for Human Rights
AMTA	Australian Mobile Telecommunications Association
APF	Australian Privacy Foundation
ASIC	Australian Securities and Investments Commission
CEM	child exploitation material
CLPC	Cyberspace Law and Policy Community
EFA	Electronic Frontiers Australia
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
ISP	Internet Service Provider
NCYLC	National Children's and Youth Law Centre
TIA Act	<i>Telecommunications (Interception and Access) Act 1979</i>

Tor	Originally 'The Onion Router'; software enabling anonymous communication on the internet.
UK	United Kingdom
UNSW	University of New South Wales
URL	Uniform Resource Locator
VPN	Virtual Private Network



List of recommendations

5 Legislation, regulation or policy?

Recommendation 1

The Committee recommends to the Australian Government the adoption of whole-of-government guidelines for the use of section 313 of the *Telecommunications Act 1997* by government agencies to disrupt the operation of illegal online services, as proposed by the Department of Communications, including:

- the development of agency-specific internal policies consistent with the guidelines;
- clearly defined authorisations at a senior level;
- defining activities subject to disruption;
- industry and stakeholder consultation;
- use of stop pages, including:
 - ⇒ agency requesting the block;
 - ⇒ reason for block;
 - ⇒ agency contact; and
 - ⇒ avenue for review.
- public announcements, where appropriate;
- review and appeal processes; and
- reporting arrangements.

Recommendation 2

The Committee recommends to the Australian Government that all agencies using section 313 of the *Telecommunications Act 1997*, to disrupt the operation of illegal online services have the requisite level of technical expertise within the agency to carry out such activity, or established procedures for drawing on the expertise of other agencies.

Introduction

Referral and conduct of the Inquiry

- 1.1 In March 2013, the Australian Securities and Investments Commission (ASIC) used powers available under s.313 of the Telecommunications Act 1997 to disrupt websites perpetrating financial fraud against Australians. This action led to the inadvertent disruption of a number of online services and raised questions regarding the transparency and accountability of the use of s.313 by government agencies to disrupt illegal online services.
- 1.2 In particular, concerns were raised that website owners and users were generally unaware that:
 - an illegal online service had been disrupted;
 - why it had been disrupted;
 - who requested the action taken; and
 - who could be contacted to appeal the decision.
- 1.3 With this in view, on 14 July 2014 the Minister for Communications, the Hon Malcolm Turnbull MP, referred the use of s.313(3) of the Telecommunications Act 1997 by government agencies to disrupt the operation of illegal online services to the Committee for inquiry and report.
- 1.4 The Committee was asked to consider:
 - (a) which government agencies should be permitted to make requests pursuant to section 313 to disrupt online services potentially in breach of Australian law from providing these services to Australians
 - (b) what level of authority should such agencies have in order to make such a request

- (c) the characteristics of illegal or potentially illegal online services which should be subject to such requests, and
 - (d) what are the most appropriate transparency and accountability measures that should accompany such requests, taking into account the nature of the online service being dealt with, and what is the best/appropriate method for implementing such measures:
 - a. Legislation
 - b. Regulations, or
 - c. Government policy.
- 1.5 The Committee was tasked to provide its final report by 1 July 2015.
- 1.6 Over the course of the Inquiry, the Committee received 21 submissions from organisations, government agencies and individuals. A list of submissions is at Appendix B. In addition, between October 2014 and March 2015, the Committee undertook six public hearings in Canberra and Sydney. Details of the public hearings, including a list of witnesses, are at Appendix C.

Brief overview of section 313

- 1.7 Section 313 provides Australian government agencies (including state government agencies) with the ability to obtain assistance from the telecommunications industry when upholding Australian laws. Amongst other things, it enables government agencies to request Internet Service Providers (ISPs) to provide such help as is reasonably necessary to disrupt the operation of illegal online services by blocking access to websites. Requests for assistance are not covered by warrants or court orders but rather the broader obligation of industry to comply with the law. This gives ISPs some flexibility in their response.
- 1.8 The Australian Federal Police (AFP) administers the Access Limitation Scheme which uses s.313 to block domains (websites) which contain the most severe child sexual abuse and exploitation material using the INTERPOL 'Worst of' child abuse list. When a user seeks to access one of these sites, they are provided a block page that displays certain information, including reasons for the block and a link to INTERPOL where any dispute arises over the inclusion of the site on the INTERPOL list. Other Commonwealth agencies have also in the past used s.313 to prevent the continuing operation of online services in breach or potentially in breach of Australian law (e.g. sites seeking to perpetrate financial fraud).

- 1.9 Section 313 deals with the obligations of carriers and carriage service providers. Subsections 1 and 2 deal with preventing the use of telecommunications networks in the commission of offences. Subsections 3 and 4 concern the giving of assistance to government agencies. Subsections 5 and 6 provide protection for carriers and carriage service providers, and their employees, from liability for actions undertaken under s.313. Subsection 7 refers to the giving of help under certain circumstances. For the provisions of s.313 see Appendix A.
- 1.10 With regard to the disruption of illegal online services, subsection 3 is the operative provision. It states:
- (3) A carrier or carriage service provider must, in connection with:
 - (a) the operation by the carrier or provider of telecommunications networks or facilities; or
 - (b) the supply by the carrier or provider of carriage services; give officers and authorities of the Commonwealth and of the States and Territories such help as is reasonably necessary for the following purposes:
 - (c) enforcing the criminal law and laws imposing pecuniary penalties;
 - (ca) assisting the enforcement of the criminal laws in force in a foreign country;
 - (d) protecting the public revenue;
 - (e) safeguarding national security.

Structure of the report

- 1.11 Chapter 2 of the report focusses upon the use of s.313 by government agencies. It examines the need for s.313, its use by government agencies to date, the need for compulsion in enforcing requests for assistance, and various criteria for more strictly defining the use of s.313 – which agencies can use it, what offences it can be used against, and what level of authority should authorise requests. The chapter also briefly examines the ASIC incident and its impact.
- 1.12 Chapter 3 examines a range of issues surrounding transparency and accountability surrounding the use of s.313, including the use or otherwise of warrants and judicial oversight, the use of block pages, review and appeal mechanisms, reporting and oversight.

- 1.13 Chapter 4 considers the technical issues surrounding the use of s.313, including the technical limits of disrupting online activity and means of avoiding the disruption of non-target websites.
- 1.14 Chapter 5 discusses the relative merits of using legislation, regulation or policy to improve/amend the operation of s.313, including questions surrounding the applicability of s.313 for requesting the disruption of websites and the proposal put forward by the Department of Communications for the development of whole-of-government guidelines for the use of s.313.

Use of section 313 by agencies

The need for s.313

- 2.1 The need for the powers conferred by s.313 to disrupt illegal online activity was highlighted in the evidence presented to the Committee. In its submission, the Australian Federal Police (AFP) stated that ‘blocking under section 313 provides law enforcement, national security agencies and regulatory bodies with an effective tool to prevent and disrupt activity which may cause serious harm to the Australian community’. The AFP recommended that ‘section 313 should be available to law enforcement, government agencies and regulatory authorities which have statutory responsibility to address serious and organised crime and matters of national security’.¹
- 2.2 The Australian Securities and Investments Commission (ASIC) also argued strongly in favour of s.313. ASIC’s experience in using s.313 indicated that ‘it is a useful measure for disrupting investment frauds and warning Australian investors that the investment[s] being offered are not legitimate’.² ASIC believed that:
- Given the difficulties in disrupting investment frauds, particularly those based overseas, it is critical that ASIC has at its disposal an effective and flexible enforcement toolkit, including the ability to block illegal websites.³
- 2.3 The Australian Crime Commission (ACC) strongly endorsed agencies having continued access to s.313, stating:

1 Australian Federal Police, *Submission 20*, pp. 1-2.

2 Australian Securities and Investments Commission, *Submission 15*, p. 4.

3 Australian Securities and Investments Commission, *Submission 15*, p. 7.

It is critical that law enforcement and national security agencies maintain access to effective tools to prevent and disrupt criminal activity, particularly at a time when cyber technology is rapidly evolving and being used to facilitate an increasing range of criminal activity.

Section 313 of the Telecommunications Act 1997 has proven to be a useful tool for Australian law enforcement to prevent harm to the Australian community caused by serious and organised crime ... While it is not the only tool available to government agencies to use, it is an important tool nonetheless. To date it has been used successfully to address cases of child sexual abuse and serious financial crime such as transnational fraud – both of which have the potential to cause significant harm to Australia, its economy and its citizens.⁴

- 2.4 The National Children's and Youth Law Centre (NCYLC) considered s.313 'an important mechanism in supporting young victims of internet-related crimes'. Section 313 provided 'a means by which to ensure internet service providers (ISPs) work with government officers and authorities to prevent the ongoing commission of crimes against children and young people in Australia'.⁵
- 2.5 The Synod of Victoria and Tasmania of the Uniting Church in Australia, argued strongly in favour of s.313, stating that:
- ISP level access disruption limits the commercial child sexual abuse industry's ability to build their customer base, thus reducing demand for the production of such material.⁶
- 2.6 The Synod further noted that:
- As of October 2011 five Australian ISPs were already working with the Australian Federal Police to block ready access to a limited list maintained by INTERPOL of child sexual abuse sites. Telstra is one of those ISPs. Between 1 July 2011 and 15 October 2011 Telstra blocked 84,000 attempts by Australians to access the child sexual abuse domains on the list.⁷
- 2.7 The Synod urged that 'the Committee recommend that the Australian Federal Police (AFP) be permitted to continue to use subsection 313(3) to require Australian Internet Service Providers (ISPs) to disrupt ready access to child sexual abuse material for sale online'. It strongly opposed 'a
-

4 Australian Crime Commission, *Submission 16*, p. 1.

5 National Children's and Youth Law Centre, *Submission 9*, p. 1.

6 Uniting Church in Australia, Synod of Victoria and Tasmania, *Submission 12*, p. 25.

7 Uniting Church in Australia, Synod of Victoria and Tasmania, *Submission 12*, p. 4.

return to the situation where Australian ISPs were able to provide ready access to commercial child sexual abuse material online'.⁸

- 2.8 The Communications Alliance, representing the ISPs, considered s.313 a 'useful provision':

It specifically allows providers to engage with law enforcement agencies when the matter does not fall under any of the other provisions in the act or in the Telecommunications (Interception and Access) Act. It is also a quite useful provision when the law has not kept up, understandably, with technological development. That could, for example, be a denial-of-service attack or something like that, where a large institution is affected by that to the detriment of the economy. It would not fall under many other places, but it could fall under section 313, and it allows providers to help as reasonably necessary. We believe that, in that context, the section is useful.⁹

- 2.9 Other evidence, however, took a different view of s.313. In its submission, Australian Lawyers for Human Rights (ALHR) argued that:

No government agency or officer should be permitted to disrupt online services on the basis that they are 'potentially' in breach of Australian law. This is an overbroad interpretation of the current law and shows clearly that the section is not appropriately limited to those means which are strictly and demonstrably necessary to achieve a legitimate legislative aim with the minimum impact upon human rights.¹⁰

- 2.10 Electronic Frontiers Australia (EFA) regarded s.313 as 'a dangerous impediment to Internet freedoms'.¹¹ EFA recommended that s.313 'be struck out completely', stating that 'there is no need for *any* government agencies to require the use of s313 as each respective agency has their own alternative means of achieving their respective outcomes'. EFA recommended that should s.313 be retained, the list of agencies able to employ s.313 'be as limited as possible'.¹²

- 2.11 Likewise, the Australian Privacy Foundation (APF) argued that 'it is not clear that the section fulfils any justifiable need that is not addressed by other much better defined and controlled mechanisms'. APF believed that:

8 Uniting Church in Australia, Synod of Victoria and Tasmania, *Submission 12*, p. 2.

9 Mrs Christiane Gillespie-Jones, Director Program Management, Communications Alliance, *Committee Hansard*, 6 March 2015, p. 8.

10 Australian Lawyers for Human Rights, *Submission 6*, p. 2.

11 Electronic Frontiers Australia, *Submission 17*, p. 2.

12 Electronic Frontiers Australia, *Submission 17*, p. 4.

It is completely unacceptable in a democracy for the parliament to grant the executive powers that are convenient to the executive but that drive a truck through the careful balances that have been achieved over centuries of development of the law.¹³

- 2.12 APF stated that if s.313 was required to fill gaps in the law, ‘it is up to the affected agencies to publicly demonstrate that this is the case and to sustain their argument in the face of counterarguments’. If a need was demonstrated, ‘then the appropriate course of action is for the executive to bring forward appropriate amendments to existing mechanisms’.¹⁴ It urged that ‘no government agencies should be permitted to make requests pursuant to section 313 to disrupt online services potentially in breach of Australian law from providing these services to Australians’. APF believed that ‘this is a task for law-enforcement and the Courts on application from agencies as expert on the facts at issue’.¹⁵ APF’s submission was that s.313 be rescinded or, if not rescinded, ‘the provisions require wholesale reworking in order to overcome a long list of serious problems’.¹⁶

Actual use to date

- 2.13 The evidence presented to the Committee indicates that to date the use of s.313 to disrupt illegal online activity has been limited – a view accepted by the telecommunications industry.¹⁷ The Department of Communications indicated that only three agencies had made use of it,¹⁸ and 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

13 Dr Roger Clarke, Immediate Past Chair, Australian Privacy Foundation, *Committee Hansard*, 4 March 2015, p. 1.

14 Dr Roger Clarke, Immediate Past Chair, Australian Privacy Foundation, *Committee Hansard*, 4 March 2015, pp. 1-2.

15 Australian Privacy Foundation, *Submission 11*, p. 4.

16 Dr Roger Clarke, Immediate Past Chair, Australian Privacy Foundation, *Committee Hansard*, 4 March 2015, p. 2.

17 Ms Lisa Brown, Policy Manager, Australian Mobile Telecommunications Association, *Committee Hansard*, 6 March 2015, p. 9.

18 Mr Rohan Buettel, Department of Communications, *Committee Hansard*, 29 October 2014, p. 2.

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.¹⁹

2.14 The Department noted that 'the disruption of access to online services under s.313 to date has been a targeted response to specific instances of illegal services', and that 'disruption of access is typically only requested where an agency considers there is a strong public or national interest to do so'.²⁰

2.15 The AFP noted that it 'only uses section 313 to disrupt illegal online activity where other mechanisms to prevent the activity have been or are unlikely to be successful'. It 'currently utilises section 313 requests to prevent access to websites which distribute child exploitation material and for cybercrime related matters'.²¹ The AFP indicated that its use of s.313 was not extensive:

Between June 2011 and August 2014 the AFP has issued twenty-three section 313 requests for the purposes of blocking websites used for illegal online activity. The majority of these requests were made to support the blocking of Interpol's 'Worst of List' in relation to online child exploitation material.²²

2.16 570 sites had been blocked, with requests covering multiple domains.²³

2.17 The AFP emphasised that the disruption of websites was 'a last resort',²⁴ and just one tool among many used in fighting crime online. With regard to online fraud, the AFP noted that:

... there are a number of other things that we do, in the background, to remediate the effect of that occurring. It is not as if we just block a site, high-five one another and move on. There is a lot of activity that occurs before and after. But the blocking of the site is one measure that we put in place so that we can do our other business without people being defrauded or being submitted to or viewing images of children being abused.²⁵

19 Department of Communications, *Submission 19*, p. 5.

20 Department of Communications, *Submission 19*, p. 6.

21 Australian Federal Police, *Submission 20*, p. 1.

22 Australian Federal Police, *Submission 20*, p. 2.

23 Assistant Commissioner Kevin Zuccato, Australian Federal Police, *Committee Hansard*, 29 October 2014, p. 6.

24 Assistant Commissioner Kevin Zuccato, Australian Federal Police, *Committee Hansard*, 29 October 2014, p. 6.

25 Assistant Commissioner Kevin Zuccato, Australian Federal Police, *Committee Hansard*, 29 October 2014, p. 6.

2.18 The AFP also emphasised that s.313 was not used for gathering information or data retrieval – they had other measures for that:

If we want other material for investigative purposes ... then there are other processes that we follow – many other processes, from summonses and subpoenas all the way up to telephone interception warrants and search warrants – if we want content. It is very important that we realise that we are not getting any information as a result of undertaking this activity.²⁶

2.19 ASIC has used s.313 to block websites linked to investment scams on ten separate occasions, its use being linked ‘exclusively in response to cold-calling frauds’.²⁷ The focus of ASIC’s use of s.313 has been to request assistance from ISPs ‘with regard to actions where we detected illegal or fraudulent investment sites in Australia’.²⁸ ASIC also emphasised that its use of s.313 was carefully targeted at illegal activity online:

... the appropriate safeguard here is that we are not doing it in a blanket way, and we are not seeking to assert to do it in a blanket way; we are targeting particular websites that are operating illegally within Australia. It is not a question of placing some form of censorship, in our view. So, we think the appropriate response to that sort of concern is, as section 313 currently allows, where there are identified activities that are in breach of the law, that a block could be requested under 313. And, it being specific to particular breaches of the law, I think that balances against the concern that perhaps was being expressed there about broader-scale blocking activities, or censorship or something of that nature. We are a law enforcement agency, and we have a lot of things to do, and our activity is directed to illegal activity.²⁹

The ASIC incident

2.20 Despite the limited use and careful targeting of offenders under s.313, a serious incident occurred in early 2013 when an ASIC request to disrupt fraudulent websites led to the inadvertent blocking of over one thousand legitimate websites, including Melbourne Free University. In 2013, around 26 March, and again around 3 April, ASIC became aware that a serial

26 Assistant Commissioner Kevin Zuccato, Australian Federal Police, *Committee Hansard*, 29 October 2014, p. 8:

27 Australian Securities and Investments Commission, *Submission 15*, p. 4.

28 Mr Greg Tanzer, Australian Securities and Investments Commission, *Committee Hansard*, 3 December 2014, p. 1.

29 Mr Greg Tanzer, Australian Securities and Investments Commission, *Committee Hansard*, 3 December 2014, p. 6.

internet fraud offender was operating fraudulent websites and requested that they be blocked. On 4 April, Melbourne Free University became aware that its website was being blocked, but did not know by whom or why. When questioned, the ISP revealed only that the block had been requested by a government agency. On 11 April, ASIC was informed by an ISP that the Melbourne Free University website had been inadvertently blocked. ASIC requested the lifting of the block on 12 April. It was only some six weeks later, however, after extensive media reporting and investigation, that the source of the block was publicly revealed. The incident was significant because it drew community, political and media attention to the otherwise opaque use of s.313 by government agencies, and the difficulties involved in identifying which agency had requested the disruption of a website and why the disruption was requested. Only as a result of media and parliamentary scrutiny was it revealed that ASIC was the agency which requested the block.³⁰

- 2.21 A subsequent review of s.313 requests alerted ASIC to a blocked IP address hosting in excess of 250 000 websites. Both blocks were removed.³¹ In evidence before the Committee, ASIC explained:

The circumstance of this particular case, as best I understand, is that we requested that a particular internet service provider address be blocked. We understood, or thought, that that address was associated with only the offending website. As it turned out, that address was also associated with a number of other websites. So, the gateway through which a person got to those other websites was the same IP address. Now, we became aware of that; we did not know it at the time that we requested that a particular website address be blocked for a particular purpose with reference to an investigation into a particular matter. But, having become aware of that, obviously what we would do at the very least would be to inquire of the telecommunications provider as to whether there are other websites. And we have our own forensic people who can give us the information as to whether that address

30 Australian Securities and Investment Commission, *Submission 15*, pp. 4–5; Ben Grubb, 'How ASIC's attempt to block one website took down 250,000' <http://www.smh.com.au/technology/technology-news/how-asics-attempt-to-block-one-website-took-down-250000-20130605-2np6v.html> (accessed 13 May 2015); Jasmine-Kim Westendorf & Jem Atahan, 'Proof the internet Filter lives on by other means', <http://www.abc.net.au/news/2013-05-16/westendorf-and-atahan---internet-filter/4694252> (accessed 13 May 2015); Peter Eckersley, Eva Galperin & Danny O'Brien, 'Australian Networks Censor Community Education Website', <https://www.eff.org/deeplinks/2013/04/australian-networks-censor-community-education-site> (accessed 13 May 2015).

31 Australian Securities and Investments Commission, *Submission 15*, pp. 4–5.

is unique to a website or not and whether there might be other avenues that one could take to block that particular website rather than the whole website address.³²

- 2.22 Subsequent to this incident ASIC has made no further use of s.313 requests:

We have not made a s313 blocking request since April 2013. ASIC's current approach is to request voluntary suspension of any fraudulent websites and domain names through correspondence to the hosting ISP and domain name registry. ASIC will also consider issuing a consumer alert or public warning notice. ASIC will consider re-using s313 following appropriate consultation with other relevant agencies such as the Australian Federal Police (AFP) and with the telecommunications carriers.³³

- 2.23 One of the central concerns about this incident was that it was not clear at first what had happened – why these websites had been blocked and at whose direction. According to Electronic Frontiers Australia (EFA):

It was very unclear for some time exactly what was happening. Clearly, there was collateral damage ... and that alerted certain people that something weird was happening – that certain websites were just disappearing as it were.³⁴

- 2.24 EFA noted that 'uncovering the activities of ASIC actually involved a large group of people over many weeks doing some very forensic analysis of what was going on'.³⁵ The block, far from identifying the cause – fraudulent activity – or the actor – ASIC – was 'so buried' that it took weeks to establish what had occurred – weeks in which the online presence of legitimate businesses was compromised for no obvious reason.³⁶

- 2.25 Dr Rob Nicholls, of the University of New South Wales, described the incident as such:

I think that one of the problems that ASIC faced when it took down the many websites that we heard about before, was that the person at ASIC did not understand the issues. The carriers and

32 Mr Greg Tanzer, Australian Securities and Investments Commission, *Committee Hansard*, 3 December 2014, p. 5.

33 Australian Securities and Investments Commission, *Submission 15*, p. 5.

34 Mr Jon Lawrence, Executive Officer, Electronic Frontiers Australia, *Committee Hansard*, 4 March 2015, p. 3.

35 Mr Jon Lawrence, Executive Officer, Electronic Frontiers Australia, *Committee Hansard*, 4 March 2015, p. 3.

36 Dr Roger Clarke, Immediate Past Chair, Australian Privacy Foundation, *Committee Hansard*, 4 March 2015, p. 8.

carriage service providers gave reasonable assistance under section 313, and they dealt with the request on its face, in the same way that they would deal with a request from the AFP on its face, but with an expectation that the work done by the agency would be the same in both cases. It was not. My view is that, if the AFP had been seeking the disruption of access to the same material, their request might well have been in the form of a URL request, ... and they might, for convenience, have said, 'And this is the IP address, but it is a virtual IP hosting address.' And they might have, in any case, gone after either the domain, or the web hosting provider in order to get the material taken down.³⁷

Enforcing compliance

2.26 During the course of the Inquiry, questions were raised about the need for and the extent of the ability of agencies to enforce compliance with s.313. The ACC noted that 'the lawful blocking of websites relies upon private sector compliance with law enforcement requests', and that 'failure to comply with a request to lawfully block a website pursuant to s.313 does not carry any consequences'.³⁸ In its submission, the Synod of Victoria and Tasmania of the Uniting Church in Australia called for compliance to be compulsory and enforceable, stating:

Implementing access disruption to child sexual abuse material online should not be a voluntary decision by ISPs. There will always be ISPs who will not agree to participate.³⁹

2.27 Dr Mark Zirnsak, representing the Synod of Victoria and Tasmania, told the Committee:

Here in Australia the evidence, particularly early on when there was an attempt to get ISPs to work voluntarily with the AFP, Australian ISPs proved to be highly resistive to doing that. There were key players who indicated that they would not assist unless compelled to do so. So I think the evidence is quite strong that in Australia we need a more mandatory approach, because our industry has a very different culture to many of those overseas. I will point out that, from memory, six ISPs actually did voluntarily work with the AFP, and some of those were the biggest – Telstra and Optus were two that did voluntarily work with the AFP, but

37 Dr Rob Nicholls, University of New South Wales, *Committee Hansard*, 6 March 2015, p. 39.

38 Australian Crime Commission, *Submission 16*, p. 1.

39 Uniting Church in Australia, Synod of Victoria and Tasmania, *Submission 12*, p. 33.

there were others who clearly resisted and made it very clear they would not collaborate on access disruption unless compelled to do so.⁴⁰

2.28 In its evidence, the AFP agreed that ‘we rely on the good conscience of companies to assist us in our endeavours’, and that ‘there are, or have been, elements of resistance that have required further discussion’ with ISPs.⁴¹ However, the AFP took the view that taken as a whole the industry was compliant and that there was no need for further enforcing compliance.⁴²

2.29 This view was supported by the evidence given by the Australian Mobile Telecommunications Association, which noted that s.313 ‘enables the provision of assistance by the industry to law enforcement and national security agencies when needed and when guided by the law’, and ‘allows a fairly cooperative approach, with some flexibility’. The Association saw no need for change:

The mobile telecommunications industry and the telecommunications industry generally have a well-established and long-running cooperative relationship with law enforcement agencies and national security agencies. That relationship and the provision of assistance when needed is guided by legislation and regulation as well as the day-to-day operations and protocols in place for provision of assistance when it is necessary and as required under the law. That provision of assistance is sometimes given in times of emergency or natural disasters but also more routinely, and that is guided by regulations, legislation and government policy and guidelines that have been in place for many years.⁴³

2.30 In its evidence, the Department of Communications noted that ISPs were already under a general obligation to comply with the Act.⁴⁴ Furthermore, ISPs had an obligation ‘to prevent the network being used in a particular way for illegal activities ... and the obligation to provide reasonable

40 Dr Mark Zirnsak, Director, Justice and International Mission Unit, Uniting Church in Australia, Synod of Victoria and Tasmania, *Committee Hansard*, 6 March 2015, p. 33.

41 Commander Glen McEwen, Australian Federal Police, *Committee Hansard*, 29 October 2014, p. 8.

42 Assistant Commissioner Kevin Zuccato, Australian Federal Police, *Committee Hansard*, 29 October 2014, p. 9.

43 Ms Lisa Brown, Policy Manager, Australian Mobile Telecommunications Association, *Committee Hansard*, 6 March 2015, p. 8.

44 Mr Ian Robinson, Deputy Secretary, Infrastructure Division, Department of Communications, *Committee Hansard*, 18 March 2015, p. 5.

assistance in their best endeavours'.⁴⁵ How this assistance was provided, however, was in large measure open to the providers:

Essentially, the way carriage service providers assist law enforcement agencies and other government agencies is open to them. The section is drafted in a way that they can provide the assistance that they are capable of providing – their best endeavours. If they have that flexibility then that also allows them to say back to the requester, 'Instead of doing it like that, we could do it like this.'⁴⁶

- 2.31 The Department saw no need for a further element of compulsion or penalties for non-compliance.⁴⁷

Defining the use of s.313

- 2.32 One of the strongest themes in the evidence presented to the Committee was the perceived need to better define and limit the use of s.313. Broadly this came down to limiting the agencies that could use s.313, the type or level of offences against which it could be used, and the level of authority within an organisation authorising the use of s.313. The telecommunications industry was strongly in favour of more clearly defining and limiting access by government agencies to the use of section 313. In their joint submission, the Communications Alliance and the Australian Mobile Telecommunications Association stated:

The Associations note that the concept of 'help as is reasonably necessary' has been extended to include the blocking of websites where it is deemed that illegal activity is connected to that site. Use of s.313(3) for this purpose should be restricted to Government enforcement and national security agencies and requires guidelines, safeguards, reporting and established levels of authority from the requesting Agency to ensure that any blocking and the consequences of such blocking has been considered at a senior level, is properly targeted and that legitimate websites and users are not also inadvertently blocked. Further, it is important

45 Ms Trudi Bean, Deputy General Counsel, Department of Communications, *Committee Hansard*, 18 March 2015, p. 4.

46 Ms Trudi Bean, Deputy General Counsel, Department of Communications, *Committee Hansard*, 18 March 2015, p. 3.

47 Ms Trudi Bean & Mr Ian Robinson, Department of Communications, *Committee Hansard*, 18 March 2015, p. 5.

that there is a quick and efficient review mechanism should someone believe a website has been blocked in error.⁴⁸

2.33 In its submission, ALHR argued that the use of s.313 'should be limited to law enforcement agencies'.⁴⁹ ALHR stated:

The fewer agencies, the less potential there is for the abuse of such powers. It is quite unacceptable to have all State (which includes Local Council) and Federal agencies able to require disruption of online services, even where they are subject to appropriate restrictions and review, which currently they are not.⁵⁰

2.34 iiNet also believed that the use of s.313 'should be restricted to a far narrower range of the critical law enforcement, anti-corruption and national security agencies', and that it was not 'necessary or proportional, for example, for local councils to be able to rely on section 313(1) or (3) to request an ISP to block a site'.⁵¹

2.35 Associate Professor Katina Michael of the University of Wollongong recommended that:

... parliament is very clear with who has the ability to disrupt the operation of illegal online services, why this one or more agencies have been tasked with this effort and whether or not they have adequate knowledge, employee skill set and tried and tested procedures to execute such an endeavour.⁵²

2.36 The Internet Society of Australia proposed that the list of agencies able to use s.313 'be no larger than those agencies that are currently able to request surveillance warrants'.⁵³ The Internet Society also proposed the provisions in the Data Retention Bill as a template for defining which agencies could use s.313, stating:

The terminology in the act currently is 'officers and authorities of the Commonwealth and of the states and territories'. That can be anybody. Again, we go back to what is being debated in the data retention environment. The list that has been drawn up and will be, we understand, put into legislation are things called the criminal law enforcement agency. That is defined now and will be

48 Communications Alliance & Australian Mobile Telecommunications Association, *Submission 7*, p. 2.

49 Australian Lawyers for Human Rights, *Submission 6*, p. 2.

50 Australian Lawyers for Human Rights, *Submission 6*, p. 10.

51 iiNet, *Submission 5*, p. 3.

52 Associate Professor Katina Michael, Associate Dean, International Engineering and Information Sciences, University of Wollongong, *Committee Hansard*, 6 March 2015, p. 25.

53 Internet Society of Australia, *Submission 13*, p. 2.

defined in any legislation for data retention. Why reinvent the wheel? Simply use the term criminal law enforcement agency. You can either spell it out or simply say 'as defined in the data retention bill'. Again, that makes it very clear that if you are asking for assistance in the circumstances where we are talking about a serious offence there is a list of agencies that the parliament has already decided should be entitled to data retention. We think they should also be entitled to seek assistance.⁵⁴

2.37 In its submission, ASIC suggested 'the approach taken in the *Telecommunications (Interception and Access) Act 1979* (TIA Act) in relation to specifying agencies that can apply for stored communications warrants'. ASIC noted that:

Under the TIA Act an 'enforcement agency' may apply for a warrant to access stored communications. The definition of 'enforcement agency' includes any body whose functions include administering a law imposing a pecuniary penalty or a law relating to the protection of the public revenue.⁵⁵

2.38 ASIC noted that it is 'specifically identified as an enforcement agency in the TIA Act'.⁵⁶

2.39 In contrast, the ACC opposed limiting which government agencies should be allowed to use s.313, stating that:

Arbitrarily specifying agencies will artificially restrict the ability of the Australian Government to combat criminal activity conducted online, and will not enable flexible responses to the inevitable evolution of the online landscape.⁵⁷

2.40 The ACC proposed that 'power to disrupt online services potentially in breach of Australian law should be focused on the type, characteristic and proportionality of the activity being conducted, or importantly, facilitated'. This approach would ensure that 'any government agency with responsibility for addressing serious criminal activities, organised crime or national security is automatically afforded the power to lawfully block websites that expose the community to harm'.⁵⁸

2.41 Defining the use of s.313 by the level of offense, or proportionality, was raised by a number of those giving evidence. The Australian

54 Ms Holly Raiche, Chair, Policy Committee, Internet Society of Australia, *Committee Hansard*, 6 March 2015, p. 2.

55 Australian Securities and Investments Commission, *Submission 15*, p. 6.

56 Australian Securities and Investments Commission, *Submission 15*, p. 6.

57 Australian Crime Commission, *Submission 16*, p. 2.

58 Australian Crime Commission, *Submission 16*, p. 2.

Communications Consumer Action Network (ACCAN) observed that ‘one way to confine the number of government agencies would be to limit access to use of power in relation to serious criminal offences and, in turn, limit access to only those agencies empowered to enforce serious criminal offences’. ACCAN suggested the example of the Commonwealth Criminal Code, ‘which defines a serious offence to mean an offence against the law of the Commonwealth, a state or a territory that is punishable by imprisonment for two years or more’. ACCAN believed that would get the balance right.⁵⁹

- 2.42 The Internet Society of Australia also supported confining s.313 ‘to criminal laws where the offence attracts a maximum penalty of at least two years imprisonment for an individual’. It argued that ‘because such assistance involves an individual or organisation’s access to the Internet, it should only be requested when the serious harm is threatened or committed’.⁶⁰ The Internet Society highlighted the example of the *Telecommunications (Interception and Access) Act 1979*:

... which has two pages of definitions and lists what the government believes, obviously, is a serious offence. It includes not only criminal offences but things like fraud. They are the sorts of offences that would attract imprisonment. In our view, the sort of assistance that should be requested should be in relation only to what amounts to a serious offence.⁶¹

- 2.43 The Australian Privacy Foundation recommended that the ‘purpose of any such law be expressly limited to serious criminal laws, defined ... as those that have penalties of five or more years in jail’.⁶²
- 2.44 In its submission, ASIC state that the use of s.313. to disrupt websites ‘should only be used in cases of serious criminal activity or the risk of serious harm to Australians’. Any threshold should be clearly articulated – ‘e.g. criminal activities subject to an offence with a statutory maximum penalty of at least two years imprisonment’. The threshold would ‘include blocking websites that are linked to investment fraud’.⁶³
- 2.45 The Department of Communications also supported a threshold of ‘illegal services or activities that carry a maximum prison term of at least two

59 Mr Xavier O’Halloran, Policy Officer, Australian Communications Consumer Action Network, *Committee Hansard*, 6 March 2015, p. 21.

60 Internet Society of Australia, *Submission 13*, p. 2.

61 Ms Holly Raiche, Chair, Policy Committee, Internet Society of Australia, *Committee Hansard*, 6 March 2015, p. 2.

62 Dr Roger Clarke, Immediate Past Chair, Australian Privacy Foundation, *Committee Hansard*, 4 March 2015, p. 2.

63 Australian Securities and Investments Commission, *Submission 15*, pp. 6–7.

years (or financial penalty with a degree of equivalence under criminal and civil law)'.⁶⁴

- 2.46 The ACC preferred not to define an offence threshold, arguing that:
- Restricting access to Section 313 for the purpose of lawfully blocking websites on a limited list of defined offences will not provide agencies with sufficient flexibility to be able to respond to newly emerging, innovative or novel crime types.⁶⁵
- 2.47 The ACC believed that the current definitions within s.313 remained relevant, 'capturing the type and characteristic of activity to ensure agencies are able to respond to newly emerging, innovative or novel crime types'. However, it also recognised 'merit in considering the proportionality of the activity being conducted or facilitated':
- By incorporating a proportionality threshold, s.313 would provide response agencies with sufficient flexibility to respond to a wide range of criminal or national security threats while at the same time creating a sufficient access threshold to ensure the proportionality of responses. This will ensure that s.313 powers for the purpose of lawfully blocking websites can only be used in response to the most serious threats impacting the Australian community.⁶⁶
- 2.48 The case was also put for defining more strictly the level of authority of officers authorising action under s.313. iiNet argued that a request to block a website 'must at least be authorised by representative of an agency that has a level of seniority and accountability that is clearly prescribed in the Regulations'.⁶⁷ The Internet Society of Australia believed that 'a "senior officer" of a police force, or judicial officer', should have "'reasonable grounds" for a belief in the likelihood [that] a serious crime will be (or has been) committed before any request under the Section is processed'.⁶⁸
- 2.49 ASIC once again suggested the *Telecommunications (Interception and Access) Act 1979* as a model, noting that 'the TIA Act provides that the chief officer of an enforcement agency can make an application for a stored communications warrant and nominate officers or positions involved in the management of the agency to make such applications'.⁶⁹

64 Department of Communications, *Submission 19*, p. 7.

65 Australian Crime Commission, *Submission 16*, p. 2.

66 Australian Crime Commission, *Submission 16*, p. 3.

67 iiNet, *Submission 5*, p. 4.

68 Internet Society of Australia, *Submission 13*, p. 3.

69 Australian Securities and Investments Commission, *Submission 15*, p. 6.

- 2.50 The ACC submitted that ‘staff investigating a relevant offence could submit a written application to an authorised officer – agency head or his/her delegate – [of] their agency setting out the case for implementing a website block’. Applications would ‘detail the facts and circumstances of the case and the offences being investigated, similar to a subpoena or summons application’.⁷⁰
- 2.51 In its submission, the AFP noted that:
- Historically, section 313 blocking requests within the AFP have been authorised by a Commissioned Officer (Superintendent or above). The level of approval has been commensurate with the seriousness of the crime and the level of disruption activity.⁷¹
- 2.52 The AFP believed that ‘this level of internal authorisation provides for an appropriately senior level of accountability and oversight’, and suggested that ‘similar internal authorisation should be the standard for the other Government Agencies using Section 313 for blocking’.⁷²
- 2.53 As a way of improving accountability in the use of s.313, the Department of Communications proposed 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.⁷³

70 Australian Crime Commission, *Submission 16*, p. 2.

71 Australian Federal Police, *Submission 20*, p. 2.

72 Australian Federal Police, *Submission 20*, p. 2.

73 Department of Communications, *Submission 19*, p. 7.

Committee conclusions

- 2.54 The Committee believes there is strong evidence of the need for s.313, whether constituted in its current form or in a modified form. Section 313 allows government agencies to interdict illegal activity online by disrupting websites in circumstances where no other means of intervention may be available. The Committee notes, moreover, that the use of s.313 has been limited to a small number of agencies pursuing a limited range of offences. There is not, on the face of it, any problem with the type of agencies using s.313 or the offences against which it is being used. Furthermore, the Committee notes that s.313 operates within a general exemptions-to-prohibitions framework, where one of the objects of the legislation is to promote and protect access to telecommunications, including the internet, except under specified circumstances – such as the need to disrupt illegal activity. The protection of privacy is one of the principal aims of the legislation – the targeted and proportionate use of s.313 does not negate that.
- 2.55 Nonetheless, the ASIC incident in 2013, where a significant number of websites were inadvertently blocked under a request made under s.313, indicates that there is a problem in the way s.313 is used. The inability of the agency to correctly target the offending websites without causing collateral damage, and the time delay in identifying the problem, suggest that the processes surrounding the use of s.313 need to be tightened and made more transparent.
- 2.56 The Committee notes the widespread calls for limits to be placed on which agencies can use s.313, what it can be used against and who can authorise that use. It takes the view that limiting the agencies which can access s.313 is unnecessary – given the limited number of agencies which utilise it – and unnecessarily restrictive. Nor does the Committee support limiting the offences against which s.313 can be used – this also is unnecessary and overly restrictive. The Committee supports the concept of s.313 being a broad and flexible mechanism for responding to changing circumstances in the online environment. The Committee strongly supports, however, more rigorous internal processes for authorising use of s.313 by agencies, including clear lines of authority. Whether these are best defined by legislation or by guidelines will be discussed in Chapter 5. Additional transparency and accountability measures will be dealt with in Chapter 3.
- 2.57 The Committee supports the view of the government agencies that the level of industry cooperation with s.313 requests is satisfactory and does not, at this stage, need to be underpinned by any further element of compulsion.

Transparency and accountability

Transparency and accountability

- 3.1 The need for greater transparency and accountability in the use of s.313 to disrupt illegal online services was broadly acknowledged in the evidence received by the Committee. A number of submissions were highly critical of the lack of transparency and accountability in the current use of s.313 and highlighted the potential and actual problems this could cause.
- 3.2 In its submission, Australian Lawyers for Human Rights (ALHR) observed that:
- ... the only apparent process, accountability or oversight in agency use of section 313 rests upon the policies of the requesting agencies (which are not available to the public), and the internal policies of ISPs in dealing with such requests (which are not generally available to the public either).¹
- 3.3 ALHR was of the view that ‘this current state of affairs is unsatisfactory and the lack of transparency leaves unchecked potential infringements on the privacy rights and rights to freedom of expression and communication of individuals’.²
- 3.4 The Internet Society of Australia believed that a ‘framework of transparency and effective accountability is critical to ensure that the public interest is protected, and use of the Section is kept to the absolute minimum’.³ The Society argued for an open and accessible internet balanced by transparent regulation:

1 Australian Lawyers for Human Rights, *Submission 6*, p. 7.

2 Australian Lawyers for Human Rights, *Submission 6*, p. 7.

3 Internet Society of Australia, *Submission 13*, p. 3.

Where we would probably take the view of the majority of Australians is that we want the government to protect us but we do not want the internet to be interfered with to the point where we are at a disadvantage compared to other countries. The digital economy relies on having an open and accessible internet. It is about finding a balance, but it is also about transparency and people knowing exactly what is happening, which is why we suggest that when a site is taken down there is a mechanism for people to object and have it reviewed.⁴

3.5 The Australian Privacy Foundation (APF) noted that currently ‘there is no meaningful information published about agencies’ invocation of section 313, what they use it for, how often or what value it delivers’. It argued that in the case of blocking a web page, ‘which is only one of the possible actions’ that could be taken under s.313, ‘an agency must be subject to a legal obligation to communicate the facts and the nature of the dispute process’.⁵

3.6 The Australian Communications Consumer Action Network (ACCAN) highlighted the INTERPOL ‘worst of’ list and how that is managed as an example of how transparency and accountability in the use of s.313 could be improved:

There are transparency and accountability measures built into that. Firstly, multiple agencies must verify whether a website contains material meeting the INTERPOL definition of child sexual abuse material. Secondly, the INTERPOL scheme contains a ‘stop page’ which states the site has been blocked, names the agency that has enforced the block and links to an appeal mechanism.

3.7 ACCAN regarded these measures as the ‘bare minimum in using this power. Without them, website owners are unlikely to know why their website is blocked, let alone what rights to appeal they may have.’⁶ For an example of an INTERPOL block page, see Figure 3.1.

4 Mr Laurie Patton, Chief Executive Officer, Internet Society of Australia, *Committee Hansard*, 6 March 2015, p. 5.

5 Dr Roger Clarke, Immediate Past Chair, Australian Privacy Foundation, *Committee Hansard*, 4 March 2015, p. 3.

6 Mr Xavier O’Halloran, Policy Officer, Australian Communications Consumer Action Network, *Committee Hansard*, 6 March 2015, p. 22.

Figure 3.1 Sample INTERPOL block page



Source Australian Federal Police, Submission 20.3, p. 4. Attempted access to a blocked website through the Telstra network, 16 March 2016.

3.8 The Communications Alliance also argued for a range of measures which it believed would improve transparency and accountability:

Amongst other things, we would want it to contain clear accountabilities, to adequately limit the circuit of agencies that issue those requests and to establish a clear level of authority of the officer that requests such a blocking of a website. It should ensure, as far as possible, that websites are not blocked inadvertently, as has happened in the past. It should contain those so-called 'stop pages' or the landing page so that, when a website is blocked, visitors to that website can immediately recognise what has happened. Importantly, it should also include a review mechanism, where people who believe that the website has been blocked inadvertently, and they are the owner of the website, can appeal against that block.⁷

⁷ Mrs Christiane Gillespie-Jones, Director Program Management, Communications Alliance, Committee Hansard, 6 March 2015, p. 8.

- 3.9 The Department of Communications agreed that ‘the use of section 313 by Australian Government agencies should be subject to a greater degree of transparency and accountability’;⁸ a call echoed by the Australian Securities and Investments Commission (ASIC):

From our perspective, as a serious white-collar-crime law enforcement agency, the transparency is actually quite important. We have typically ... produced a media release or made some public announcement about this when we have taken these actions in these past ... we want to get a public message out. So from our perspective we are quite comfortable with the recommendation that there should be more transparency.⁹

- 3.10 The Australian Crime Commission (ACC) also supported ‘consideration of a formal transparency and accountability regime’ in relation to the use of s.313, ‘to ensure the maintenance of public confidence in government agency use of these powers’.¹⁰ The ACC noted, however, that:

... while accountability and transparency are important, there is also a legitimate need for law enforcement and national security agencies to retain a level of secrecy in order to ensure the integrity of current and future operations.¹¹

- 3.11 The ACC believed that:

... agencies should not be required to publically release information relating to the use of s.313 powers for the purpose of lawfully blocking websites where it could, inter alia, expose sensitive sources and methodologies employed by law enforcement and national security, impact the safety of individuals, or publicly expose active investigations or classified intelligence.¹²

Use of warrants and judicial oversight

- 3.12 The use of warrants and judicial oversight was one of the accountability measures canvassed in the evidence presented to the Committee. ALHR argued strongly for judicial oversight of the use of s.313, stating that:

8 Department of Communications, *Submission 19*, p. 6.

9 Mr Greg Tanzer, Commissioner, Australian Securities and Investments Commission, *Committee Hansard*, 3 December 2014, p. 3.

10 Australian Crime Commission, *Submission 16*, p. 3.

11 Australian Crime Commission, *Submission 16*, p. 3.

12 Australian Crime Commission, *Submission 16*, p. 3.

Judicially reviewed legislation is the key to transparency and accountability. If one accepts our existing Westminster system of democratic Australian government, then effectively one must agree that we should only be regulated by 'law,' and anything not able to be scrutinised by the judiciary is not 'law'.¹³

- 3.13 Furthermore, ALHR believed that 'no government agency or officer should be permitted to disrupt online services on the basis that they are 'potentially' in breach of Australian law'. ALHR stated that 'it should be established before an Australian court or tribunal that a service is in breach of Australian law before any further action can be taken'. ALHR identified the Administrative Appeals Tribunal as the most appropriate tribunal to approve requests to disrupt illegal online activity.¹⁴
- 3.14 Internet service provider (ISP), iiNet argued in favour of all requests pursuant to s.313 being accompanied by a court order and the court order being sent to all ISPs. iiNet stated:
- ISPs should not be placed in a position where they have to make difficult decisions or seek legal advice about what its obligations are under section 313. The decision making on when "help" is required of ISPs should ideally be made by a court.¹⁵
- 3.15 ACCAN took the view that 'it is unreasonable for an ISP or indeed most government authorities to be the arbiters of these legal issues without judicial intervention'.¹⁶ ACCAN's preference was that 'these requests should be accompanied by a court order and that government agencies should only be using these powers without judicial oversight in special circumstances'.¹⁷
- 3.16 Government agencies were generally opposed to the use of warrants and judicial oversight of section 313. In its submission, the Department of Communications preferred an agency-led process for disrupting access to online services, rather than a judicial process. It stated:
- 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

13 Australian Lawyers for Human Rights, *Submission 6*, p. 2.

14 Australian Lawyers for Human Rights, *Submission 6*, p. 10.

15 iiNet, *Submission 5*, pp. 2-3.

16 Australian Communications Consumer Action Network, *Submission 4*, p. 5.

17 Mr Xavier O'Halloran, Policy Officer, Australian Communications Consumer Action Network, *Committee Hansard*, 6 March 2015, p. 22.

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.¹⁸

- 3.17 ASIC concurred, highlighting the difference in speed between judicial proceedings and action under section 313. ASIC noted that whereas court proceedings would take ‘a week to 10 days’, a request to block a website under section 313 could be accomplished within twenty-four hours:

We could get information and undertake the necessary checks that we think are appropriate to see if (a) the entity does not have a licence and (b) either the addresses that are associated with any companies are made up or the entity and the people do not reside at those addresses. Generally, there might be use of false identities in terms of registration. We can check all of that, because that is in our data. We can check that within a matter of hours and have a request up. Within a five-to-10-day window you might see anything up to \$1 million or \$2 million moving through these accounts.¹⁹

- 3.18 Likewise, the AFP urged the retention of section 313 in its current form, stating:

We need to move really fast because the whole judicial process takes times – if we have got to type documents and so forth – to do something that simply makes something stop, right. We are not asking for information – we’re just saying, ‘Look, this needs to stop.’²⁰

- 3.19 The ACC took the view that warrants were not necessary. It believed that the ‘system is working effectively at the moment’ and that the relatively low level of use of s.313 for the disruption of illegal online services indicated ‘that agencies are using it very carefully and judiciously’.²¹

- 3.20 The Synod of Victoria and Tasmania of the Uniting Church in Australia opposed the use of warrants under s.313. The Synod was:

... very concerned about any suggestion that law enforcement, in combatting child sexual abuse material, and availing themselves of

18 Department of Communications, *Submission 19*, p. 8.

19 Mr Tim Mullaly, Australian Securities and Investments Commission, *Committee Hansard*, 3 December 2014, p. 4.

20 Assistant Commissioner Kevin Zuccato, Australian Federal Police, *Committee Hansard*, 29 October 2014, p. 9.

21 Ms Judith Lind, Executive Director Strategy & Specialist Capabilities, Australian Crime Commission, *Committee Hansard*, 25 February 2015, p. 4.

this particular disruption mechanism, should suddenly be subject to having to go through a warrant process or having ACMA or the A-GD oversighting it.²²

- 3.21 Dr Rob Nicholls did not believe that warrants were necessary for the proper operation of s.313 – as long as those authorising action were at a sufficiently senior level to be held accountable for their decisions. Using the example of the *Telecommunications (Interception and Access) Act 1979*, he stated:

The TIA Act essentially says that for prospective data the level of authority is SES 2 – first assistant secretary level or equivalent within the agency. It seems to me that even if that power is delegated within the agency, having somebody at a level where they might expect to be asked questions about the matter, either by a House committee or in Senate estimates, is not an unreasonable thing. Have the person senior enough. Provided you have certainty ... I do not see that you necessarily need a warrant regime provided that, essentially, it is a senior officer's career that is on the line for a decision that the material – access to which is going to be disrupted – is serious enough that they are willing to sign an authorisation.²³

- 3.22 The Australian Privacy Foundation's normal standpoint was that 'judicial warrants [are] the appropriate mechanism', but given the technical nature of requests under s.313, it suggested that 'it may actually be an occasion when a suitably designed process would not include a judicial officer'.²⁴

Use of block pages

- 3.23 Another transparency and accountability measure raised in the evidence presented to the Committee concerned the use of block pages – notices advising that access to a particular site had been stopped. The Internet Society argued that 'if websites are blocked there should at the very least be a message put on the site itself that says, "This has been blocked. It's been blocked by a particular agency. This is the number to call."²⁵

22 Dr Mark Zirnsak, Director, Justice and International Mission Unit, Uniting Church in Australia, Synod of Victoria and Tasmania, *Committee Hansard*, 6 March 2015, p. 33.

23 Dr Rob Nicholls, UNSW, *Committee Hansard*, 6 March 2015, p. 39.

24 Dr Roger Clarke, Immediate Past Chair, Australian Privacy Foundation, *Committee Hansard*, 4 March 2015, p. 4.

25 Ms Holly Raiche, Chair, Policy Committee, Internet Society of Australia, *Committee Hansard*, 6 March 2015, p. 2.

- 3.24 This has several purposes: it would allow people to know that the website was deliberately being blocked, not just unavailable for technical reasons;²⁶ and it would help to identify inadvertent disruption.²⁷ The use of block pages also meant that people would be aware that the authorities had been alerted to the illegal activity, thereby reducing the reporting burden placed on agencies.²⁸
- 3.25 ALHR also advocated the use of block pages detailing ‘which statutory authority requested the block under section 313 with their contact information and detail the process for the website owner to appeal the application of the block’.²⁹
- 3.26 The AFP advised that ‘Interpol provides a generic “stop page” that an ISP can choose to display to their customer’, but that ‘use of the “stop page” is not mandatory and an ISP may prefer to display an error message instead’. The AFP noted that ‘Interpol recommends the use of the “stop page” to increase transparency’. The block page ‘advises the user that their browser has tried to contact a domain that is distributing child sexual abuse material’ and ‘provides avenues for a user to report online content and to make a complaint if they believe that the domain is wrongly blocked’.³⁰
- 3.27 In its submission, iiNet advised that it did its best to promote transparency by ‘insisting that requests for the blocking of sites also provide (at a minimum)’:
- personal contacts of the requestor in the relevant Authority;
 - transparency measures such as:
 - ⇒ a redirection page with details of the reasons for the block and appropriate remediation or appeal processes for the affected parties; and
 - ⇒ evidence that the site contains prohibited content and/or is the subject of a relevant court order or judgment.³¹
- 3.28 The Department of Communications acknowledged that the use of block pages may have mitigated the effects of the ASIC incident:

26 Mr Laurie Patton, Chief Executive Officer, Internet Society of Australia, *Committee Hansard*, 6 March 2015, p. 6.

27 Ms Holly Raiche, Chair, Policy Committee, Internet Society of Australia, *Committee Hansard*, 6 March 2015, p. 6.

28 Dr Mark Zirnsak, Director, Justice and International Mission Unit, Uniting Church in Australia, Synod of Victoria and Tasmania, *Committee Hansard*, 6 March 2015, p. 36.

29 Australian Lawyers for Human Rights, *Submission 6*, p. 11.

30 Australian Federal Police, *Submission 20.3*, p. 4.

31 iiNet, *Submission 5*, p. 4.

As we understand the ASIC example one of the key things was no one really knew what had happened so they did not know who to appeal to or what the explanation was. The first element I think is the proposal for stopped pages. In most cases a stop page would go up and give some background so if there is concern about it people could appeal to the agency concerned.³²

3.29 It also acknowledged that announcing disruptions improves transparency and allows agencies to advertise reasons for their actions.³³ As part of its response to concerns about the use of s.313, the Department proposed the use of block pages, with agencies providing ISPs ‘with a generic government stop page (similar to that used by the INTERPOL scheme when preventing access to online child exploitation material)’, containing 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.³⁴

3.30 This approach was supported by ASIC, which saw the use of block pages as an opportunity to alert people to danger:

... instead of just completely blocking access, the person who is searching that site gets a message that says: ‘This has been blocked for this particular reason – come and contact such and such.’ That also seems to me to offer opportunities to at least get a message to those people to say, ‘It has been blocked because it is an illegal investment site. If you want to know more about protecting yourself against that, please contact us through this sort of number.’³⁵

3.31 Nonetheless, the Department of Communications also acknowledged 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

32 Mr Ian Robinson, Deputy Secretary, Infrastructure Division, Department of Communications, *Committee Hansard*, 18 March 2015, p. 2.

33 Department of Communications, *Submission 19*, p. 7.

34 Department of Communications, *Submission 19*, p. 8.

35 Mr Greg Tanzer, Commissioner, Australian Securities and Investments Commission, *Committee Hansard*, 3 December 2014, p. 3.

operational activities to be jeopardised, may not include reasons, or indeed may not be used at all.³⁶

- 3.32 Similarly, the ACC emphasised the need for operation flexibility in the use of block pages. It advised the Committee:

If you are trying to reinforce a preventative message or an education message or even a deterrence message, there would be circumstances where you would want the person trying to go onto the site to know that this is a blocked site. There may be other circumstances and more in the classified environment where you might want to keep that knowledge classified and covert.³⁷

Review and appeal

- 3.33 According to the Internet Society of Australia, the importance of having a mechanism for reviewing the blocking of websites was highlighted by the ASIC incident:

There was no indication for those people who had lost a website as to why they had lost the website and there was no appeal. That circumstance actually gave rise to one of our recommendations ... First of all, there should be an appeal so that if in fact there has been some assistance given that damages somebody wrongly there ought to be a place for them to go.³⁸

- 3.34 The Internet Society considered various options including appeal to a court or 'some kind of administrative appeal but, nevertheless, legally constituted', but considered court proceedings too 'costly and time-consuming', especially for small businesses or individuals. Nonetheless, the Society believed 'there should be a way for somebody to seek redress'.³⁹
- 3.35 The Communications Alliance and Australian Mobile Telecommunications Association (AMTA) also called for 'a clear and efficient review

36 Department of Communications, *Submission 19*, p. 8.

37 Ms Judith Lind, Executive Director Strategy & Specialist Capabilities, Australian Crime Commission, *Committee Hansard*, 25 February 2015, p. 5.

38 Ms Holly Raiche, Chair, Policy Committee, Internet Society of Australia, *Committee Hansard*, 6 March 2015, p. 2.

39 Ms Holly Raiche, Chair, Policy Committee, Internet Society of Australia, *Committee Hansard*, 6 March 2015, p. 2.

- mechanism where members of the public can report legitimate websites that have been blocked in error'.⁴⁰
- 3.36 ACCAN believed that where an error in the application of s.313 occurred, 'the impact on small businesses and other website operators could be minimised by having a quick, accessible and free path for appeal'. ACCAN noted that 'there are already established review mechanisms for these types of administrative decisions', and suggested that 'reconsideration by the original decision-maker is likely to solve the problem in a timely manner, without the need to seek judicial review'.⁴¹
- 3.37 The Australian Privacy Foundation argued that 'demands by agencies must be able to be objected to, both by the organisation that is subject to the demand and by parties who are or who would be affected by the action'. It recommended that the Government 'propose specific mechanisms whereby the exercise of the power can be contested by any affected party'; and further, that 'wrongful or unjustifiably harmful exercise of the power should be subject to sanctions'.⁴² Electronic Frontiers Australia supported the call for compensation in the event of harm, noting that 'an action to disrupt a service could, in certain circumstances, drive a business into bankruptcy. And that needs, obviously, to be catered for if it is done inappropriately'.⁴³
- 3.38 The Department of Communications confirmed that at present there was no specific review or appeal mechanism under s.313. Rather, 'action could potentially be taken under general administrative law requirements if the carrier were particularly concerned, or a particular issue could be raised with the Commonwealth Ombudsman'.⁴⁴
- 3.39 In its submission, the Department proposed 'guidelines within each agency which outline their own review mechanism, which we hope would be quicker and cleaner' than current arrangements.⁴⁵ One element would be 'internal review mechanisms within agencies; the other existing

40 Communications Alliance and Australian Mobile Telecommunications Association, *Submission 7*, p. 5.

41 Australian Communications Consumer Action Network, *Submission 4*, p. 8.

42 Dr Roger Clarke, Immediate Past Chair, Australian Privacy Foundation, *Committee Hansard*, 4 March 2015, p. 3.

43 Mr Jon Lawrence, Executive Officer, Electronic Frontiers Australia, *Committee Hansard*, 4 March 2015, p. 8.

44 Mr Rohan Buettel, Assistant Secretary, Consumer Protection Branch, Consumer and Content Division, Department of Communications, *Committee Hansard*, 29 October 2014, p. 4.

45 Mr Ian Robinson, Deputy Secretary, Infrastructure Division, Department of Communications, *Committee Hansard*, 18 March 2015, p. 4.

external appeal mechanisms.⁴⁶ Agency service disruption procedures would 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.’ Agencies would also have procedures in place ‘to periodically review disrupted services to ensure that the disruption remains valid’. Furthermore, agencies would ‘reassess any access disruption at the request of a complainant’.⁴⁷ External review could be through the *Administrative Decisions (Judicial Review) Act 1977* or the Ombudsman.⁴⁸

Reporting

3.40 Currently agencies using s.313 to disrupt illegal online services are under no obligation to report such use.⁴⁹ In the interests of greater transparency and accountability, ACCAN urged ‘annual public reporting by government agencies using this power. This will help ensure the power is being applied appropriately.’⁵⁰ The Internet Society agreed, suggesting a reporting regime ‘similar to that currently in place for the Telecommunications Interception and Access Act’:

Such reporting should list the number of requests per agency and should include the basis on which each request is made (e.g. the relevant offence). Such reporting should also include summary data on the number of requests made by ASIO.⁵¹

3.41 iiNet argued that the legislation should:

... provide for specific oversight and transparency measures such as requiring the relevant government agencies to inform the Department of Communications of their use of section 313 to block websites each January and June.⁵²

3.42 In its submission, ALHR proposed oversight of requests under s.313 ‘by a Parliamentary Joint Committee, and an annual report on such requests presented to Parliament’, The report would detail:

46 Mr Ian Robinson, Deputy Secretary, Infrastructure Division, Department of Communications, *Committee Hansard*, 18 March 2015, p. 2.

47 Department of Communications, *Submission 19*, p. 8.

48 Department of Communications, *Submission 19*, p. 8.

49 Department of Communications, *Submission 19*, p. 5.

50 Mr Xavier O’Halloran, Policy Officer, Australian Communications Consumer Action Network, *Committee Hansard*, 6 March 2015, p. 22.

51 Internet Society of Australia, *Submission 13*, p. 5.

52 iiNet, *Submission 5*, p. 4.

- number of requests;
 - basis for requests;
 - costs to the Government and costs to ISPs of implementing and managing the implementation of blocks;
 - policies followed by government agencies in making such requests; and
 - outcome of requests – whether any legitimate sites were incorrectly blocked.⁵³
- 3.43 The Synod of Victoria and Tasmania of the Uniting Church in Australia suggested additional reporting requirements, including:
- the number of times access to known child sexual abuse sites was blocked by each Australian ISP that has been subject to a s.313 requirement to do so; and
 - actively promote where Australians should report inadvertent encounters with child sexual abuse material online.⁵⁴
- 3.44 The AFP welcomed annual reporting of s.313 requests, but suggested that:
- ... releasing specific details publicly as to the nature of each individual request and to which ISP each request was made may have a substantial adverse effect on the proper and efficient operations of the AFP and may be contrary to the public interest.⁵⁵
- 3.45 The ACC also supported reporting of requests under s.313. It stated:
- We can achieve accountability, firstly, by improving reporting, and reporting in terms of the agency, macro-level reporting of the number of requests and for blocking the number of blocked sites, and the broad category or context in which the site was blocked. By that, I mean referring to subsections C to E, whether it is criminal law, public revenue or national security. For that information to be put together in an annual report, it is consistent with the manner in which warrants under the Telecommunications (Interception and Access) Act are reported, as a starting point. All stakeholders would agree that this would be an appropriate mechanism.⁵⁶
- 3.46 The ACC placed caveats around protecting the operational methodology of law enforcement and national security agencies. The ACC did not

53 Australian Lawyers for Human Rights, *Submission 6*, p. 2.

54 Uniting Church in Australia, Synod of Victoria and Tasmania, *Submission 12*, p. 5.

55 Australian Federal Police, *Submission 20*, p. 4.

56 Ms Judith Lind, Executive Director Strategy & Specialist Capabilities, Australian Crime Commission, *Committee Hansard*, 25 February 2015, p. 3.

support 'mandated detailed reporting of every circumstance in which a site is blocked'.⁵⁷

- 3.47 The Department of Communications acknowledged that there was a problem with the lack of reporting of requests,⁵⁸ and proposed, as an additional transparency measure, that the use of s.313 to disrupt access to illegal online services be reported to the Australian Communications and Media Authority (ACMA) for inclusion in its annual report. It was expected that this measure would 'improve transparency around the disruption of access to services under section 313 by providing a single repository of this information'. Nonetheless, the Department recognised 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'. It recommended in these circumstances 'reporting to an appropriate Parliamentary committee on an *in camera* basis'.⁵⁹
- 3.48 Other groups supported using ACMA as the principal reporting agency for requests under s.313, including the ACC and ACCAN.⁶⁰
- 3.49 ACMA itself acknowledged that its 'existing annual reporting to the Minister could be expanded to include information relating to the use of section 313 to disrupt illegal online services'. ACMA believed that 'such reporting would improve transparency around such disruptions', but would be dependent upon ISPs and/or agencies informing ACMA about such activities.⁶¹

Oversight

- 3.50 In addition to reporting the use of s.313, calls were made for s.313 requests to be managed through a central agency or placed under central oversight. The Internet Society of Australia argued that s.313 requests 'should be centrally managed through a single agency, such as the ACMA [or] the Attorney-General's Department'.⁶²

57 Ms Judith Lind, Executive Director Strategy & Specialist Capabilities, Australian Crime Commission, *Committee Hansard*, 25 February 2015, p. 3.

58 Mr Rohan Buettel, Assistant Secretary, Consumer Protection Branch, Consumer and Content Division, Department of Communications, *Committee Hansard*, 29 October 2014, p. 3.

59 Department of Communications, *Submission 19*, p. 9.

60 Ms Judith Lind, Executive Director Strategy & Specialist Capabilities, Australian Crime Commission, *Committee Hansard*, 25 February 2015, p. 4; Mr Xavier O'Halloran, Policy Officer, ACCAN, *Committee Hansard*, 6 March 2015, p. 24.

61 Australian Communications and Media Authority, *Submission 8.1*, p. 2.

62 Internet Society of Australia, *Submission 13*, p. 2.

- 3.51 The APF argued that some form of independent oversight was essential to the use of s.313 to disrupt illegal online services:

In all circumstances it is essential that the exercise of a power be subject to a precondition that a competent, resourced and independent party receive and consider the agency's justification, deny unreasonable proposals and authorise reasonable ones. So, we submit that the committee should recommend that the scheme involve an independent party that has the responsibility and the authority to test whether the basis on which a requesting agency proposes exercise of the power satisfies the defined criteria and reaches the applicable thresholds, failing which the agency cannot use the power.⁶³

- 3.52 The APF regarded ACMA as the logical oversight agency,⁶⁴ a position supported by Electronic Frontiers Australia.⁶⁵

- 3.53 ASIC opposed putting s.313 requests through a central agency, arguing that this would 'have a negative impact on agencies' ability to block offending websites in a timely manner, without necessarily providing significant improvements in either transparency or accountability'.⁶⁶ ASIC preferred an agency-specific regime, bolstered by stronger accountability measures such as appropriate levels of authorisation and delegation in the making of requests. This would allow agencies to respond to illegal online activity with appropriate flexibility and speed.⁶⁷

- 3.54 The Department of Communications also opposed the centralisation of s.313 requests or oversight by a central agency. It told the Committee:

There is a relatively low number of requests and fundamentally we think the issue is about explanation and transparency about those, and provided that is put in place then that is a good first step—just improving arrangements. We suggest as part of our proposal that some of the reporting arrangements would be through the ACMA, which is within our portfolio and does similar reporting on behalf of the telecommunications sector. But I am sure we would not say that there needs to be a central point that

63 Dr Roger Clarke, Immediate Past Chair, Australian Privacy Foundation, *Committee Hansard*, 4 March 2015, p. 3.

64 Dr Roger Clarke, Immediate Past Chair, Australian Privacy Foundation, *Committee Hansard*, 4 March 2015, p. 4.

65 Mr Jon Lawrence, Executive Officer, Electronic Frontiers Australia, *Committee Hansard*, 4 March 2015, p. 1.

66 Australian Securities and Investments Commission, *Submission 15*, pp. 5–6.

67 Mr Greg Tanzer, Australian Securities and Investments Commission, *Committee Hansard*, 3 December 2014, p. 6.

ticks off these requests – especially given there are relatively few and, in fact, most of them are one agency, which is a law enforcement agency who is best placed to make those decisions.⁶⁸

3.55 In particular, the Department opposed using ACMA in an oversight role, because that ‘would mean ACMA would be looking at the law enforcement activities of other bodies and they probably do not have the background to do that’.⁶⁹ Nor did the Department believe that ACMA should be the central agency for handling requests. The Department noted that ACMA did not ‘really have the skill set or background’ to undertake that role;⁷⁰ and suggested that ‘sending those requests through the ACMA may not assist police when they have particularly urgent requirements’.⁷¹

3.56 ACMA itself was not comfortable with the suggestion that it be responsible for the regulatory oversight of the use of s.313 by government agencies. It noted, ‘as a practical matter’, that:

... should additional roles or powers be contemplated in relation to sections 313 and 314, then the interaction between any such new roles or functions would need to be considered, particularly if any kind of ex ante oversight role about actions by either agencies or CSPs were to be contemplated.⁷²

3.57 Becoming the central agency managing requests by other agencies was also problematic from ACMA’s perspective. It raised:

- ‘boundary’ questions including about other section 313 related requests for assistance;
- potential resourcing issues; and
- concerns for the ACMA about acquiring a possible de facto role in terms of being required to make judgements about the merits of active investigations being conducted by other agencies including whether another agency’s intended use of a section 313 request was warranted. These may raise issues about which the ACMA may have limited expertise.⁷³

3.58 ACMA supported the Department of Communications proposal for whole-of-government guidelines, stating that:

68 Mr Ian Robinson, Department of Communications, *Committee Hansard*, 29 October 2014, p. 4.

69 Mr Ian Robinson, Deputy Secretary, Infrastructure Division, Department of Communications, *Committee Hansard*, 18 March 2015, p. 2.

70 Mr Ian Robinson, Deputy Secretary, Infrastructure Division, Department of Communications, *Committee Hansard*, 18 March 2015, p. 2.

71 Ms Trudi Bean, Deputy General Counsel, Department of Communications, *Committee Hansard*, 18 March 2015, p. 2.

72 Australian Communications and Media Authority, *Submission 8.1*, p. 2.

73 Australian Communications and Media Authority, *Submission 8.1*, p. 3.

The ACMA considers that such a proposal would be workable in addressing the issue and the ACMA would be well placed to advise on technical issues relating to the blocking of URLs for inclusion in the proposed guidelines.⁷⁴

- 3.59 ACMA's current roles under s.313 'are to enforce industry compliance with the subsection and to appoint an arbitrator where the parties fail to reach agreement on the terms and conditions on which industry assistance is to be given'. ACMA advised that to date it had 'not had cause to take any enforcement action for non-compliance with subsection 313(3) or to appoint an arbitrator under subsection 314(3) of the Act'. ACMA also 'reports annually to the Minister on matters relating to industry's cooperation with law enforcement agencies in line with its statutory reporting obligations under subsection 105(5A) of the Act'.⁷⁵
- 3.60 ACMA's only direct power to disrupt websites 'stems from its role administering the Online Content scheme under the *Broadcasting Services Act 1992*'.⁷⁶

Committee conclusions

- 3.61 The Committee believes that there is a need to improve transparency and accountability surrounding the use of s.313 by government agencies to disrupt the operation of illegal online services. The ASIC incident stands as an example of that. Greater transparency and accountability may have prevented the incident – it certainly would have made the problem easier to identify and resolve.
- 3.62 A number of measures have been identified in this Chapter that could improve transparency and accountability. The use of warrants and judicial oversight of s.313 has been canvassed. The Committee is of the view that this measure would delay the effective response of agencies to illegal activity online.
- 3.63 The Committee regards the use of block pages – in all but the most sensitive cases involving national security or law enforcement – as essential. Such block pages should identify the agency which made the request, the reason the request was made, an agency contact point, and review procedures.

74 Australian Communications and Media Authority, *Submission 8.1*, p. 3.

75 Australian Communications and Media Authority, *Submission 8*, p. 1.

76 Australian Communications and Media Authority, *Submission 8.1*, p. 1.

- 3.64 Effective review and appeal processes are also essential to the use of s.313 by government agencies. The Committee agrees that all agencies using s.313 to disrupt illegal online services should have in place internal review procedures that allow them to rapidly respond to issues raised by ISPs, web pages owners and the public in relation blocked sites. This would substantially mitigate the sort of problems which arose following the ASIC incident. The Committee is satisfied that suitable judicial and administrative appeals processes exist where agency review processes fail to meet individual expectations.
- 3.65 The Committee endorses proposals for the reporting of agency use of s.313 to disrupt the operation of illegal online activity, such reporting to identify the number of requests, the agencies making requests, reasons for requests and the outcome. The Committee is of the view that ACMA would be the ideal reporting body.
- 3.66 The Committee does not see the need for an oversight agency, or the centralisation of requests. With rigorous processes in place, the Committee believes that individual agencies are best placed to make decisions about the most appropriate way to use s.313 to disrupt websites.
- 3.67 The Committee gives consideration to the best way to implement these reforms – through legislation, regulation or policy – in Chapter 5.

Technical issues

Technical limits of disrupting online activity

- 4.1 During the course of the inquiry, a number of technical issues were raised about the use of s.313 to disrupt illegal online activity, including whether the blocking of websites is practically effective, the cost of disruption to ISPs and their customers, and the ability to avoid inadvertent blocking of non-target websites.
- 4.2 The blocking of websites can involve the targeting of the Internet Protocol (IP) address (the numerical label of an internet resource or computer), the domain name (the unique name of an internet resource) or the Uniform Resource Locator (URL – the specific web address of a website).
- 4.3 When connecting to the Internet, the ISP sends the URL to a domain name server which converts the word-based web address to a numerical IP address. The packets of information sent to and from a website use the IP address of the website and the IP address of a computer, to identify each other when exchanging data.¹
- 4.4 There is not always a one-to-one relationship between the URL and an IP address:
 - ... there is an option that is commonly used called shared IP posting. In this name-based virtual hosting, or shared IP hosting, the virtual host serves multiple host names with one machine and a single IP address. The reason that that works is, when a web browser requests a resource from a web server using hypertext transfer protocol – the HTTP of an address – it includes the host

1 Dr Rob Nicholls, University of New South Wales, *Committee Hansard*, 6 March 2015, p. 38.

name as part of the request. The virtual server uses the information to determine which website to show to the user.²

4.5 In its submission, the Internet Society of Australia acknowledged that while 'blocking known criminal websites may have limited value', it had 'consistently argued against blocking websites more generally because it is neither practical nor effective'. It observed that blocking 'does not prevent access to a vast array of criminal material on the Internet either because it is delivered by means other than the web or because the URL of the material varies with each access'.³

4.6 Dr Roger Clarke of the Australian Privacy Foundation also highlighted the technical limits of blocking. He stated:

One of the mistakes that is often made with the example in focus, which is, of course, the blocking of highly undesirable websites, is that people tend to assume that the web is the internet. The web is one protocol out of 100 that runs over the top of internet. It is only one element of a thin layer at the top. It happens to be responsible for a significant volume of what goes on, but no more than, at a rough guess, 30 or 40 per cent at the moment ... So, if you are trying to attack child pornography being hidden, the web is probably the least likely place to go looking at the moment. That is not understood by enough people, unfortunately, and it is sometimes hard to convey the argument.⁴

4.7 Dr Clarke emphasised that anyone really determined to access illegal material online could do so. The 'critical point is that anybody who has a real reason to dig in and find out can do so'.⁵

4.8 Mr David Vaile, Co-convenor of the Cyberspace Law and Policy Community at the University of New South Wales, also addressed the difficulties facing government agencies in blocking online activities. He noted that:

... depending on what you are targeting against and what methods you are using, you have to consider what is happening on the other side. Internet security is at a point where really no-one in the world can promise that they can protect any bit of information stored behind a perimeter, and the capacity of organised criminal organisations and foreign nation-state actors —

2 Dr Rob Nicholls, University of New South Wales, *Committee Hansard*, 6 March 2015, p. 39.

3 Internet Society of Australia, *Submission 13*, p. 3.

4 Dr Roger Clarke, Immediate Past Chair, Australian Privacy Foundation, *Committee Hansard*, 4 March 2015, p. 6.

5 Dr Roger Clarke, Immediate Past Chair, Australian Privacy Foundation, *Committee Hansard*, 4 March 2015, p. 6.

and subcontractors to them—is extremely broad. For instance, anyone can invent a new form of internet protocol or a new way of using the web protocol on port 80 to do something that is invisible and will not be noted for a couple of weeks or years. You could say that we must make even more effort to try and catch all of that stuff before it goes anywhere, but the evidence of the last five years is that everything is on the side of the attacker and the inventive intruder rather than on the side of the defender. You have to accept that there will be ways around most perimeter security and there will be ways around most filters.⁶

- 4.9 Other technical limitations included the existence of Virtual Private Networks (VPN) and Tor. A VPN ‘creates essentially a dedicated pipe through which you can send secure communications’. It is ‘used in the corporate and government contexts for absolutely legitimate purposes in terms of securing external access to networks’. A VPN ‘allows you to appear to be coming from a location where you are not actually at, so it does obfuscate your location in that sense. It obfuscates potentially your source internet protocol address as well – your IP address’.⁷ Tor is a tool designed to make internet activity anonymous. It is designed to ‘bounce your requests and your traffic around a number of random sites across the internet to essentially anonymise who you are and not just where you are coming from’. Such tools ‘provide the ability for people that wish to get around the sorts of actions that might be taken under section 313 ... to essentially circumvent those actions pretty easily’.⁸
- 4.10 The Australian Federal Police (AFP) acknowledged the difficulties caused by ‘VPNs and the camouflaging activities that people do utilise within the internet’, but highlighted what could be achieved – emphasising that s.313 was just one of a suite of measures undertaken by the AFP:

What we are achieving with the current capacity provided under section 313 is a prevention strategy, and disruption, more in relation to the opportunistic people [who] are dealing in this material; the inquisitive, perhaps ... In relation to the use of VPNs, that is always going to be a challenge; that is the whole concept behind the camouflaging of your activities. The extent of this particular piece of legislation would be somewhat limited in

6 Mr David Vaile, Co-convenor, Cyberspace Law and Policy Community, Faculty of Law, UNSW, *Committee Hansard*, 6 March 2015, p. 17.

7 Mr Jon Lawrence, Executive Officer, Electronic Frontiers Australia, *Committee Hansard*, 4 March 2015, p. 5.

8 Mr Jon Lawrence, Executive Officer, Electronic Frontiers Australia, *Committee Hansard*, 4 March 2015, p. 5.

relation to that. But that is not to say that the AFP and other agencies around the world do not have the ability to monitor and disrupt and prosecute people who are utilising such capabilities.⁹

- 4.11 Addressing the question of whether such efforts were worthwhile, the AFP argued that while a person with a genuine desire to access child exploitation material (CEM) 'may utilise other methods to circumvent the blocking of illegal online services', the 'access limitation scheme is not capable of, nor intended to, capture all persons attempting to access CEM'. It observed that 'blocking of illegal online services is one of many disruption strategies undertaken by law enforcement', and argued that 'the disruption of illegal online services is an effective tool in preventing access through Australian ISP's to CEM'. The AFP noted that, alongside its 'domestic and foreign law enforcement partners', it 'utilises other methods and investigative strategies to identify those attempting to access CEM through Virtual Private Networks or networks such as TOR'. It also noted that disruption was, 'with respect to preventing or restricting systems infected with malicious software access to command and control networks ... an extremely valuable and worthwhile activity':

The end result of effectively removing command and control can lead to the inability of viruses aimed at stealing banking credentials from supplying those credentials to the persons controlling the software.¹⁰

- 4.12 Addressing the success of s.313 in disrupting access to CEM, the AFP stated that while it was 'difficult to quantify the level of disruption this will achieve', the access limitation scheme currently 'covers approximately 82% of private consumers in Australia utilising an Australian Internet Service Provider'.¹¹ It noted:

In the past decade, there has been exponential growth in the use of the internet and the availability of CEM online. In this environment, the AFP must prioritise its limited investigative resources towards investigations that will have the greatest impact in identifying offenders and removing children at risk from harm. This includes investigations in relation to offenders that sexually abuse children, profit from the trading of CEM, or facilitate the sexual and physical abuse of children through online video streaming.

9 Commander Glen McEwen, Australian Federal Police, *Committee Hansard*, 29 October 2014, p. 7.

10 Australian Federal Police, *Submission 20.3*, p. 2.

11 Australian Federal Police, *Submission 20.3*, p. 1.

The AFP utilises the access limitation scheme as one technique to prevent access to CEM online.¹²

- 4.13 Addressing the success of s.313 in disrupting cybercrime, the AFP highlighted the success of law enforcement agencies internationally in blocking access to scams such as the Game over Zeus malware:

The use of s313 in this case is extremely effective as, unlike in the case of CEM where an individual can take subsequent steps to avoid website blocking, malware is limited in its ability to dynamically respond to a loss of command and control infrastructure. This can therefore render networks of malicious software ineffective, dependant on their objectives. Whilst this will not prevent cybercriminals from conducting further damage, it does mean that they need to start again and rebuild their network.¹³

- 4.14 In its evidence, the Synod of Victoria and Tasmania of the Uniting Church in Australia, strongly endorsed the effectiveness of the disruption of websites as a tool in the fight against CEM. It stated:

The Internet Watch Foundation, which is based in the UK, and Cybertip in Canada have done evaluations of access disruption. The finding is that it has led to two main potential outcomes that show its effectiveness. One is that commercial child-sex providers have had to change their [URLs] every few days in order to try to stay ahead of disruption. The second thing is that the cost of accessing the material has gone up. Subscription costs for people buying this material have massively increased ... That is a sign that this is a business model under stress.¹⁴

- 4.15 The Synod also highlighted the manageability of the commercial CEM problem – the limited size of the sector and the success of agencies in disrupting networks:

The Internet Watch Foundation ... talks about the scope of this industry. They estimate that there are probably about 1,000 businesses globally, so it is a manageable target to go after. In that, the peak of the business is probably about 30 key brands. So there are about 30 criminal enterprises that will run multiple sites and outlets that are the key target of this kind of disruption on commercial child sexual abuse material. The fact that you are only

12 Australian Federal Police, *Submission 20.3*, pp. 1–2.

13 Australian Federal Police, *Submission 20.3*, p. 2.

14 Dr Mark Zirnsak, Director, Justice and International Mission Unit, Uniting Church in Australia, Synod of Victoria and Tasmania, *Committee Hansard*, 6 March 2015, pp. 32–33.

dealing with a manageable number of sites allows for this disruption to be well-targeted. You are not dealing with trillions of sites ... The UK Internet Watch Foundation shows that it is possible to keep a running battle against them. From memory, they would disrupt about 600 URLs a day, and they update those twice daily, in the UK Internet Watch Foundation.¹⁵

4.16 The Synod also emphasised the moral effects of disruption – discouraging non-contact involvement with CEM:

Offender typology says that a lot of people who buy stuff are non-contact offenders. So they are actually not engaged in the sexual abuse of children physically themselves. They are purchasing material, and many of them engage in fantasy, thinking, 'I'm not doing anything wrong; this stuff's readily available on the internet.' Again, this is why access disruption helps, because it breaks that notion, 'I'm not doing anything wrong and this is all okay because it's readily accessible on the internet. Nothing's stopping me from getting there.' Suddenly you have a law enforcement message popping up. That may help cut through some of that fantasy that, 'I'm not doing anything wrong and this is all okay.'¹⁶

4.17 Dr Rob Nicholls, of the University of New South Wales, noted the relative ease of avoiding blocks if a person was determined to do so,¹⁷ but also highlighted a range of mechanisms by which agencies could frustrate illegal online activity. One was approaching the website host:

Most hosting businesses are commercial businesses that do not want to offend law enforcement agencies and do not want to be the deep pockets in civil lawsuits, so a stern letter by email to a web host saying that it is hosting material which is offensive, defamatory or inappropriate in some way in Australia can often get a response which is the publisher's defence, 'We didn't know it was there' – perfectly valid – and then potentially a takedown of that offending material.

This works particularly well if the material would breach the criminal law in either the country where the material is actually hosted or where the web hosting company is domiciled. For child

15 Dr Mark Zirnsak, Director, Justice and International Mission Unit, Uniting Church in Australia, Synod of Victoria and Tasmania, *Committee Hansard*, 6 March 2015, pp. 32–33.

16 Dr Mark Zirnsak, Director, Justice and International Mission Unit, Uniting Church in Australia, Synod of Victoria and Tasmania, *Committee Hansard*, 6 March 2015, p. 34.

17 Dr Rob Nicholls, UNSW, *Committee Hansard*, 6 March 2015, p. 12.

pornography and certain other material, that would work quite well.¹⁸

- 4.18 Another was 'to actually look to which domain name server deals with that website and potentially look to see if you can stop that domain name server pointing to the website'. Dr Nicholls noted that:

You certainly have the potential for doing that in Australia, and in particular doing that, because we have only a limited number of fibre-optic trunks which bring traffic into Australia. There are only a limited number of what are called border gateway routers – the bits that interconnect the network of networks – and you could potentially block at that point, but only if the IP address of the website is unique to that URL.¹⁹

- 4.19 Dr Nicholls noted that in his experience law enforcement agencies would 'typically choose to use all possible approaches'.²⁰

- 4.20 The Department of Communications also noted that the disruption of websites was only one of a suite of measures that might be employed by agencies to combat illegal activity online. Disruption was 'not entirely foolproof but it is a quick lever to take action and it can be backed up again if required'.²¹ The Department regarded the disruption of VPNs as essentially a separate issue to be dealt with in other ways.²²

Costs

- 4.21 The potential cost to ISPs of assisting government agencies in the disruption of illegal online activity under s.313 was raised in the evidence presented to the Committee. Associate Professor Katina Michael, of the University of Wollongong, told the Committee:

When it comes to identifying unacceptable use of their service offerings and reporting illegal online services to law enforcement authorities, I think they [ISPs] are very good at doing that. However, carriers, large or small, cannot be expected to dedicate resources wholly to the task of uncovering past, present or future crimes. There are considerable what I would call operational

18 Dr Rob Nicholls, UNSW, *Committee Hansard*, 6 March 2015, p. 12.

19 Dr Rob Nicholls, UNSW, *Committee Hansard*, 6 March 2015, p. 12.

20 Dr Rob Nicholls, UNSW, *Committee Hansard*, 6 March 2015, p. 12.

21 Mr Ian Robinson, Deputy Secretary, Infrastructure Division, Department of Communications, *Committee Hansard*, 18 March 2015, p. 3.

22 Mr Ian Robinson, Deputy Secretary, Infrastructure Division, Department of Communications, *Committee Hansard*, 18 March 2015, p. 3.

costs – specifically, labour, infrastructure and service maintenance costs – associated with supporting authorities in their investigations.²³

4.22 Professor Michael noted that:

From a technical standpoint, the time it takes to investigate a single case can be anywhere from an hour to a long period of time. It depends on the severity and how fast the data needs to get back. Resources are not infinite in organisations, nor are they infinite in policing organisations, for that matter.

4.23 Professor Michael recommended that the Commonwealth ‘budget for this and remunerate or at least pay back the cost to private organisations that have to go above and beyond the particular time frame’. She stated that the Commonwealth agencies also needed to ‘support the installation of equipment to cater for their demands’.²⁴

4.24 Dr Nicholls took a different view of costs, noting that the use of s.313 had operational costs to carriers:

... but the operational costs of configuring the routing table of a border gateway router are mainly the cost of making sure that the 313 notice on its face was something that the carrier or carriage-service provider could rely on to get the immunity that is provided under 313.²⁵

4.25 Dr Nicholls did ‘not believe we are talking about large amounts of money’.²⁶

4.26 The Department of Communications noted that there were already provisions for ISPs to recover costs – ‘although in most cases the costs of this would be immaterial and they probably do not do it’.²⁷

23 Associate Professor Katina Michael, Associate Dean, International Engineering and Information Sciences, University of Wollongong, *Committee Hansard*, 6 March 2015, p. 27.

24 Associate Professor Katina Michael, Associate Dean, International Engineering and Information Sciences, University of Wollongong, *Committee Hansard*, 6 March 2015, p. 28.

25 Dr Rob Nicholls, UNSW, *Committee Hansard*, 6 March 2015, p. 41.

26 Dr Rob Nicholls, UNSW, *Committee Hansard*, 6 March 2015, p. 41.

27 Mr Ian Robinson, Deputy Secretary, Infrastructure Division, Department of Communications, *Committee Hansard*, 18 March 2015, p. 5.

Avoiding disruption of non-target sites

- 4.27 The inadvertent blocking of non-target websites by ASIC in 2013 was the result of a fundamental error in its targeting of websites. ASIC requested that ‘telecommunications carriers block the IP addresses’ of offending websites.²⁸ This opened the way for the inadvertent blocking of the hundreds of thousands of websites that shared the same IP address.²⁹
- 4.28 Attempting to disrupt illegal online activity by blocking IP addresses is also relatively easy to avoid. The Synod of Victoria and Tasmania of the Uniting Church in Australia noted that:
- ... most child sexual abuse providers now use fast fluxing, which means they are changing their IP address every few minutes; it might be every 20 minutes. The AFP actually had some data; I think they watched a site over a prolonged period of time and found it was changing its IP address every 20 minutes. It is senseless then to try to disrupt an IP address.³⁰
- 4.29 Disrupting the domain name – the method used by INTERPOL to disrupt CEM – also carries risks of over-blocking, ‘as the whole domain is deemed illegal if any part of it is found to contain sexual abuse material with children’.³¹ This has led to a cautious approach to the disruption of domains:
- ... with the domain, there is an attempt to contact the domain provider prior to them being put on the list and giving them every opportunity to remove the material prior to them getting on the list, so, where a domain provider is either negligent or wilfully continuing to host that material, there is an argument they deserve to be on the list and have that disrupted as a mechanism to try to force them to take the material down.³²
- 4.30 The criticism of this approach is that ‘the tight criteria of this form of access blocking reduces its effectiveness as a dynamic disruption strategy against the commercial child sexual abuse industry’.³³
- 4.31 The most precise method of disrupting illegal activity online is to target the URL – the web address – ‘because you are then going after just the site

28 Australian Securities and Investments Commission, *Submission 15*, p. 4.

29 Dr Rob Nicholls, UNSW, *Committee Hansard*, 6 March 2015, p. 12.

30 Dr Mark Zirnsak, Director, Justice and International Mission Unit, Uniting Church in Australia, Synod of Victoria and Tasmania, *Committee Hansard*, 6 March 2015, p. 36.

31 Uniting Church in Australia, Synod of Victoria and Tasmania, *Submission 12*, p. 27.

32 Dr Mark Zirnsak, Director, Justice and International Mission Unit, Uniting Church in Australia, Synod of Victoria and Tasmania, *Committee Hansard*, 6 March 2015, p. 36.

33 Uniting Church in Australia, Synod of Victoria and Tasmania, *Submission 12*, p. 27.

itself'. This is the method employed by the UK Internet Watch Foundation.³⁴

4.32 In its submission, the Internet Society of Australia stated that in the 'limited cases' where the use of s.313 may be warranted, 'there should be a process that ensures that only the identified site(s) and service(s) are blocked'. It suggested that 'where the intent is to prevent access to a website, the request should specify that only http/s traffic to a particular domain name should be affected'.³⁵

4.33 The AFP emphasised in its evidence, that the problem with inadvertent disruption was not the legislation but robust processes and due diligence within agencies utilising s.313. It stated:

In relation to undertaking the activity, it is a question of ensuring due diligence. It is a question of if you have got a domain name, then before you ask someone to do something for you make sure you are asking the right question and that you have gone through and satisfied yourself that what they are asking you to do is not going to cause an issue or a problem. It is not a question of the legislation or how the legislation is used. When we, for example, block the 'worst of the worst' list there are procedures in place with Interpol that ensure that we do not make a mistake. If we have, for example, an issue such as Gameover Zeus, where we made a decision to block that particular domain – it was sending out emails and asking people to log on to a site where they were going to get defrauded – then there is a lot of work that goes on behind the scenes to make sure that what we are asking them to do is not going to cause issues for people who have got legitimate business on the internet.³⁶

4.34 The AFP advised the Committee that it had 'not been involved in any inadvertent blocking of websites'.³⁷

34 Dr Mark Zirnsak, Director, Justice and International Mission Unit, Uniting Church in Australia, Synod of Victoria and Tasmania, *Committee Hansard*, 6 March 2015, p. 36.

35 Internet Society of Australia, *Submission 13*, p. 1.

36 Assistant Commissioner Kevin Zuccato, Australian Federal Police, *Committee Hansard*, 29 October 2014, p. 8.

37 Australian Federal Police, *Submission 20.3*, p. 5.

Committee Conclusions

- 4.35 The Committee is cognisant of the fact that by itself the disruption of illegal online services will not prevent criminal activity. People determined to do so will always find a way to get around blocks on the internet, and the capacity to target sites will always be constrained by the need to avoid collateral damage. Nonetheless, the Committee is of the view that there is sufficient evidence that the disruption of websites is technically feasible and provides an effective avenue to frustrate criminal activity where other means are not available and as part of a suite of other investigative and enforcement measures. The fact that particular activities or content may have to be found and blocked repeatedly does not negate the necessity of trying. Rather, it emphasises the fact that – as in any other area of law enforcement – constant vigilance is required. The ability of government agencies to disrupt illegal online services through s.313 is a necessary one.
- 4.36 Avoiding the inadvertent disruption of non-target websites is chiefly the outcome of technological competence and robust administration. Mistakes will be avoided through the use of robust or transparent processes. A better understanding of technology, combined with better processes, will prevent problems from occurring; or, allow a more rapid identification and response to a problem. It is the view of the Committee, therefore, that all government agencies utilising s.313 to disrupt illegal online services should have transparent and robust processes surrounding its use (see Chapter 3), and the requisite level of technical expertise within, or accessible to, the agency to carry out such requests (see Chapter 5, Recommendation 2).
- 4.37 The Committee is also conscious of the potential costs for ISPs in complying with requests for assistance from government agencies under s.313. The Committee believes that it is important that agencies consult with industry about the best means of complying with requests for assistance, including managing costs.

Legislation, regulation or policy?

- 5.1 The question of how to regulate the use of s.313 in the disruption of illegal online services is a contentious one. The Committee has received evidence favouring changes to the legislation, while other submissions have endorsed s.313 as it is and while calling for closer regulation of its use through guidelines.
- 5.2 Evidence presented to the Committee raised questions about the suitability of s.313 for the purpose of disrupting the operation of illegal online services. Mr John Denham observed that s.313 ‘has been around for a long time, and the wording of the section does not appear to have contemplated its use to block internet access to websites’. He noted that ‘the wording would seem to have been lifted from much earlier legislation and aimed purely at telephone/fax/telex communications’.¹ The Internet Society of Australia reminded the Committee that s.313 ‘was drafted many years ago’ and ‘was going to be used by [the police] to cut down the service of some illegal SP bookies’. The Internet Society suggested that ‘the technology has moved on considerably and we think the Act should move on as well’.² The Communications Alliance noted, however, that s.313 ‘was not envisaged to deal with [the] kind of use that it currently receives with the blocking of websites’.³ The Australian Mobile Telecommunications Association (AMTA) noted that:

When the Act was written in 1997, the blocking of websites probably was not foremost in everyone’s minds of how the section

1 Mr John I Denham, *Submission 2*, p. 1.

2 Ms Holly Raiche, Chair, Policy Committee, Internet Society of Australia, *Committee Hansard*, 6 March 2015, pp. 1-2.

3 Mrs Christiane Gillespie-Jones, Director Program Management, Communications Alliance, *Committee Hansard*, 6 March 2015, p. 8.

would be used; whereas in the times we live in now it might be something that happens maybe more frequently.⁴

- 5.3 In its evidence, the Cyberspace Law and Policy Community (CLPC) at the University of New South Wales questioned whether the provisions of s.313 allowed it to be used for the disruption of websites at all. Relying on ‘the plain words of the statute and principles of statutory interpretation’, the CLPC took the view that s.313(3) ‘does not authorise disruption, impairment or blocking’.⁵ The CLPC characterised disruption as a crime prevention activity – the province of s.313(1) – and noted that s.313(7), which sets out particular examples of ‘giving help’ under s.313(3), does not provide for the disruption of websites. Observing the provision of s.313(7), the CLPC stated:

The ordinary provisions of statutory interpretation could extend its scope to include very similar types of help, perhaps preserving the contents and wrapper of a new form of messaging for the law enforcement evidence collection purposes of 313(3).

But in our view they do *not* extend to authorising quite different activities (like blocking or impairing an online service) done for a different purpose (crime prevention and disruption, which is covered in 313(1) but is not tied to 313(7)).⁶

- 5.4 The CLPC believed that s.313 as presently framed:

... cannot be used for mandatory blocking either under (1), the crime prevention section, because there is no obligation for anybody to do anything other than to come to a view about what their best is and to do that, or under (3), because the law enforcement purpose is different from crime prevention and the types of help are different from (7).⁷

- 5.5 It took the view that ‘there is no existing power enabling mandatory requests for disruptive impairment for crime prevention purposes in s.313’, and argued that ‘if any change were to be made, legislation would be necessary’.⁸ The CLPC also believed that ‘legislation should not be developed until a comprehensive investigation is conducted as there is no
-

4 Ms Lisa Brown, Policy Manager, Australian Mobile Telecommunications Association, *Committee Hansard*, 6 March 2015, p. 9.

5 Cyberspace Law and Policy Community, University of New South Wales, *Submission 21*, p. 4.

6 Cyberspace Law and Policy Community, University of New South Wales, *Submission 21*, p. 7. See also, Mr David Vaile, Co-convenor, Cyberspace Law and Policy Community, Faculty of Law, University of New South Wales, *Committee Hansard*, 6 March 2015, p. 14.

7 Mr David Vaile, Co-convenor, Cyberspace Law and Policy Community, Faculty of Law, University of New South Wales, *Committee Hansard*, 6 March 2015, p. 16.

8 Cyberspace Law and Policy Community, University of New South Wales, *Submission 21*, p. 14.

current comprehensive evidence base about the benefits, costs and risks of such an undertaking'.⁹ Referring to the Australian Securities and Investment Commission incident and the broader questions about the operation of s.313 raised by the incident, Mr David Vaile, co-convenor of the CLPC, stated:

Our suggestion would be that we do not keep repeating this series of missteps and also run the risk that I notice a lot of submitters have raised of having a non-transparent, non-accountable and non-reviewable system that does not have any testing of the evidence – no judicial oversight in the form of warrants or orders and effectively no parliamentary oversight because, as far as we can see, there has been no thorough investigation of the issues before this. You need to consider that fundamental question. Some of the questions had started to be asked with the previous filter but were, in a sense, stopped before they went much further. Some of them really have not been asked at all. The proper answer is important. The power is not there as it is. A convenient non-investigation of that question has occurred so far. The proper response is to say that the motivation to do something and to analyse the harms that could reasonably be responded to is a real one that should be responded to, but it needs a much more thorough review rather than starting at the last question. We need to start pretty close to the first questions.¹⁰

5.6 Australian Lawyers for Human Rights (ALHR) believed that any action taken under s.313 should be explicitly defined by legislation. ALHR stated:

Government policy is not a method that could implement appropriate transparency and accountability measures that should accompany government agencies' requests under section 313 as it does not *oblige* a government decision-maker to explain and justify their conduct to a significant other.¹¹

5.7 ALHR argued that 'judicially reviewable legislation is the best and most appropriate method for implementing Transparency and Accountability Measures in respect of section 313',¹² and that:

9 Cyberspace Law and Policy Community, University of New South Wales, *Submission 21*, p. 15.

10 Mr David Vaile, Co-convenor, Cyberspace Law and Policy Community, Faculty of Law, University of New South Wales, *Committee Hansard*, 6 March 2015, p. 17.

11 Australian Lawyers for Human Rights, *Submission 6*, p. 12.

12 Australian Lawyers for Human Rights, *Submission 6*, p. 12.

Accordingly, legislation would implement transparency and accountability measures that should accompany requests under section 313, and rebalance Australia's review and public transparency standards by allowing greater parliamentary scrutiny of section 313; and open, judicial, impartial, and independent supervision of section 313.¹³

5.8 The Communications Alliance argued for 'a more robust framework' around the use of s.313,¹⁴ stating:

... we are of the opinion that the addition of a new section to the act that specifically addresses the legitimate requests by agencies to block websites would provide a useful means to create greater certainty for industry – and, for that matter, agencies – in that context. To create that additional degree of certainty, we also believe that it is necessary that some of the items that I mentioned previously – like the level of authority, stop pages and other things – should be contained in the primary legislation as opposed to the guidelines. We think that it is better public policy to create the certainty through the primary law and that that would contribute greatly to a more effective and more transparent use of the law in that specific context of disrupting illegal online behaviour.¹⁵

5.9 The Communication Alliance suggested s.315 of the Telecommunications Act, dealing with the suspension of supply of carriage service in an emergency, as a template:

We would see a new section in the act – similar to the current section 315 – that specifically addresses the blocking of websites, and in that section, similar again to 315, we would want to see certain elements already in the primary legislation and then maybe an additional guideline.¹⁶

5.10 AMTA were 'quite supportive of the idea of guidelines as proposed by the Department of Communications', but, nonetheless thought 'that going a step further and having a section structured similarly to section 315 would

13 Australian Lawyers for Human Rights, *Submission 6*, p. 13. See also, Ms Roslyn Cook, Vice President, Australian Lawyers for Human Rights, *Committee Hansard*, 6 March 2015, p. 43.

14 Mrs Christiane Gillespie-Jones, Director Program Management, Communications Alliance, *Committee Hansard*, 6 March 2015, p. 8.

15 Mrs Christiane Gillespie-Jones, Director Program Management, Communications Alliance, *Committee Hansard*, 6 March 2015, p. 9.

16 Mrs Christiane Gillespie-Jones, Director Program Management, Communications Alliance, *Committee Hansard*, 6 March 2015, p. 9.

just provide a little more certainty for agencies and industry on how these types of requests might work'.¹⁷

5.11 iiNet believed that 'a standard approach for section 313 requests to block sites should not be left up to agencies and ISPs' own policies but should be set out in Regulations'. iiNet stated that 'legislation should also provide for specific oversight and transparency measures'.¹⁸

5.12 The Internet Society of Australia emphasised the ambiguity in the language of s.313. Ms Holly Raiche, Chair of the Internet Society's policy committee, explained:

... we would say that the language of section 313 generally is a little bit problematic. I realise this inquiry is not about subsections 313(1) and (2), which say that the carrier should do its best, but I think that language is a little bit problematic because there will be some carriers who have particular views about assisting law enforcement agencies and will say, 'Our best is, basically: "The door is closed unless you give me a warrant,"' but there will be smaller providers who will, if they see a couple of police officers at the door, do perhaps far more than they should. Similarly, in subsections (3) and (4), the language is that carriers and carriage providers should give 'such help as is reasonably necessary'. Again, I find that just a little bit hard. What does that mean?¹⁹

5.13 The Internet Society believed that 'while the intent of the section *could* be preserved, a framework for its use is urgently required recognising the public interest and ensuring legitimacy, openness, transparency and accountability'. Without such a framework, the Society argued, 'the section should be removed'.²⁰

5.14 The idea that s.313 was out-of-date or not fit-for-purpose for the disruption of illegal online services was contested by the agencies using or overseeing the legislation. The Department of Communications challenged the proposition that s.313 was not being used as intended, or that its use for the purpose of blocking websites was potentially open to legal challenge given its original drafting. It also disagreed with the view that s.313 was not intended for the prevention of crime or that the act of

17 Ms Lisa Brown, Policy Manager, Australian Mobile Telecommunications Association, *Committee Hansard*, 6 March 2015, p. 11.

18 iiNet, *Submission 5*, p. 4.

19 Ms Holly Raiche, Chair, Policy Committee, Internet Society of Australia, *Committee Hansard*, 6 March 2015, p. 2.

20 Internet Society of Australia, *Submission 13*, p. 1.

blocking did not constitute law enforcement.²¹ The Department argued that law enforcement included ‘preventing citizens from having access to harmful websites’, stating:

I do not think it has to be preparation of a court case. I think enforcing the law goes back some way further than that, to the commission of the crime. I know that telecommunication services or carriage service providers are working with law enforcement ... those sorts of on-the-spot, very flexible ways of operating with law enforcement agencies are essential to retain.²²

5.15 The Department also did ‘not agree that website blocking was not in ... contemplation’ when s.313 was originally formulated. The Department believed that ‘what was in the contemplation was to make it as broad as possible, so that the very quickly-developing telecommunications and communications industry did not need to keep coming back to say, “This is unworkable.”’²³

5.16 The Department noted that legislation often ‘gives the general power and has flexibility within it as certain circumstances change’, and that ‘the current provision just refers to criminal activity really’. This was seen as ‘flexible’ and ‘a good model’.²⁴

5.17 Similarly, the AFP did ‘not have concerns with the legality of carriage service providers’ disruption of illegal online services in response to requests that invoke s313 of the Telecommunications Act’:

In the AFP’s view there is nothing in the terms of the various obligations contained in s313, the drafting history of that provision and its predecessor provisions, or the explanatory memoranda that accompanied the enactment and amendment of those provisions from which to infer that the obligations s313 imposes do not encompass blocking of illegal online activity.

Rather, those various sources indicate that s313 and its predecessor provisions were expressly drafted in broad terms, and that broad formulation has been maintained through various statutory amendments over the course of the provision’s history.²⁵

21 Ms Trudi Bean, Deputy General Counsel, Department of Communications, *Committee Hansard*, 18 March 2015, p. 4.

22 Ms Trudi Bean, Deputy General Counsel, Department of Communications, *Committee Hansard*, 18 March 2015, p. 4.

23 Ms Trudi Bean, Deputy General Counsel, Department of Communications, *Committee Hansard*, 18 March 2015, p. 4.

24 Mr Ian Robinson, Deputy Secretary, Infrastructure Division, Department of Communications, *Committee Hansard*, 18 March 2015, p. 3.

25 Australian Federal Police, *Submission 20.3*, p. 3.

- 5.18 The AFP thought s.313 effective 'in particular because the legislation does not specifically relate to blocking'. S.313 related to 'the provision of assistance to the AFP, amongst other agencies ... it is the vehicle that we use to have the telcos assist us in blocking certain sites'.²⁶
- 5.19 Dr Nicholls questioned the utility of replicating s.315, noting that 'by the time that is drafted and implemented, it is likely to be technologically obsolete'. He believed that the crucial point was 'to have the principle of what a disruption should be'. He supported the Department of Communications proposal for the creation of whole-of-government guidelines in the use of s.313 or an industry code. He believed that with such arrangements in place the current legislation would work.²⁷

Guidelines

- 5.20 In answer to the concerns raised about the use of s.313 to disrupt illegal online services, the Department of Communications proposed 'the development of whole-of-government principles to guide Australian Government agency use of the provisions to disrupt access to illegal online services'.²⁸ The provisions of these guidelines 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'.²⁹ Agencies would then 'develop internal procedures in accordance with the guidelines and publish those procedures online'.³⁰ The guidelines would 'specify minimum requirements and recommended procedures to follow' when seeking to disrupt illegal online services, including:
1. develop agency-specific internal policies outlining their own procedures for requesting the disruption of access 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;

26 Assistant Commissioner Kevin Zuccato, Australian Federal Police, *Committee Hansard*, 29 October 2014, p. 6.

27 Dr Rob Nicholls, University of New South Wales, *Committee Hansard*, 6 March 2015, pp. 40–41.

28 Department of Communications, *Submission 19*, p. 3.

29 Department of Communications, *Submission 19*, p. 6.

30 Department of Communications, *Submission 19*, p. 6.

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.³¹

5.21 According to the Department, the guidelines would provide a clear, flexible and transparent framework for the use of s.313 to disrupt illegal online services:

We are proposing that there be clear guidelines; that particular agencies essentially produce information about how they are using the section, how they are applying it; and that they have clear internal policies as to who is authorised to make these decisions and therefore make sure accountability is at the right level in particular organisations – that they get the authority from senior people to do so. We are proposing that the blocking of sites et cetera is at a threshold level that is significant enough and, as I mentioned before, that there is transparency about what they are doing and why they are doing it. In a lot of cases and in the case of some law enforcement activities, there would also be provisions

31 Department of Communications, *Submission 19*, p. 9.

for that not to occur if that is going to compromise law enforcement actions.³²

- 5.22 The AFP supported the Department's proposal for the development of whole-of-government guidelines for the use of s.313,³³ as did ASIC.³⁴ The Australian Crime Commission (ACC) gave qualified support, highlighting the importance of maintaining 'maximum flexibility, which is currently achieved in the statute'. The ACC identified a range of mechanisms by which s.313 could be more closely defined, but cautioned:

If you are going down to a very narrowly defined offence model then you need your guidelines to be able to rapidly keep up with changes in the environment and changes in the activity that the regulators are seeing to make sure that that can be updated.³⁵

- 5.23 Australian Communications Consumer Action Network also endorsed the proposed guidelines, describing them as 'a sensible suggestion and will improve government agency awareness of the implications of using this power for online enforcement activities'.³⁶

- 5.24 In their joint submission, the Communications Alliance and AMTA recommended that:

In addition to clarifying who is able to use s.313(3), the Associations recommend that any use of s.313(3) should be subject to guidelines or regulations that set out processes and procedures to be used. These should specify, for example, the required level of seniority and minimum technical competence that individuals within an organisation should possess to enable them to authorise a request under s.313(3).³⁷

32 Mr Ian Robinson, Deputy Secretary, Infrastructure Division, Department of Communications, *Committee Hansard*, 29 October 2014, pp. 1–2.

33 Australian Federal Police, *Submission 20*, p. 4; Assistant Commissioner Kevin Zuccato, Acting Deputy Commissioner Close Operations Support, Australian Federal Police, *Committee Hansard*, 29 October 2014, p. 7.

34 Mr Greg Tanzer, Commissioner, Australian Securities and Investments Commission, *Committee Hansard*, 3 December 2014, p. 1; Australian Securities and Investments Commission, *Submission 15.1*.

35 Ms Judith Lind, Executive Director Strategy & Specialist Capabilities, Australian Crime Commission, *Committee Hansard*, 25 February 2015, p. 3.

36 Mr Xavier O'Halloran, Policy Officer, Australian Communications Consumer Action Network, *Committee Hansard*, 6 March 2015, p. 22.

37 Communications Alliance & Australian Mobile Telecommunications Association, *Submission 7*, p. 4.

Committee conclusions

- 5.25 The Committee is conscious of the concerns that have been raised about the lack of clarity and transparency in the use of s.313 to disrupt illegal online services. This lack of clarity and transparency contributed to the inadvertent blocking of websites by ASIC in 2013 and the difficulties surrounding identifying that mistake and correcting it.
- 5.26 Nonetheless, the Committee is of the view that s.313 provides an effective measure of protection to the Australian community in managing illegal online activity, and that the broad nature of s.313 is its strength – allowing it to be adapted to a range of circumstances as the nature of technology and crime evolve. The Committee therefore supports the proposal of the Department of Communications for the formulation of whole-of-government guidelines covering the use of s.313 by government agencies. The Committee believes that these guidelines will preserve the effectiveness of s.313 while mitigating potential problems flowing from its use.

Recommendation 1

- 5.27 **The Committee recommends to the Australian Government the adoption of whole-of-government guidelines for the use of section 313 of the *Telecommunications Act 1997* by government agencies to disrupt the operation of illegal online services, as proposed by the Department of Communications, including:**
- the development of agency-specific internal policies consistent with the guidelines;
 - clearly defined authorisations at a senior level;
 - defining activities subject to disruption;
 - industry and stakeholder consultation;
 - use of stop pages, including:
 - ⇒ agency requesting the block;
 - ⇒ reason for block;
 - ⇒ agency contact; and
 - ⇒ avenue for review.
 - public announcements, where appropriate;
 - review and appeal processes; and
 - reporting arrangements.

- 5.28 In addition, as discussed in Chapter 4, the Committee believes it is vital to the proper execution of requests to disrupt the operation of illegal online services under s.313 that all agencies making such requests have the requisite level of technical expertise within, or accessible to, the agency.

Recommendation 2

- 5.29 **The Committee recommends to the Australian Government that all agencies using section 313 of the *Telecommunications Act 1997*, to disrupt the operation of illegal online services have the requisite level of technical expertise within the agency to carry out such activity, or established procedures for drawing on the expertise of other agencies.**

Mrs Jane Prentice MP

Chairman

13 May 2015



Appendix A – Part 14, *Telecommunications Act 1997*

Part 14—National interest matters

311 Simplified outline

The following is a simplified outline of this Part:

- The ACMA, carriers and carriage service providers must do their best to prevent telecommunications networks and facilities from being used to commit offences.
- The ACMA, carriers and carriage service providers must give the authorities such help as is reasonably necessary for the purposes of:
 - (a) enforcing the criminal law and laws imposing pecuniary penalties; and
 - (b) protecting the public revenue; and
 - (c) safeguarding national security.
- A carriage service provider may suspend the supply of a carriage service in an emergency if requested to do so by a senior police officer.

312 ACMA's obligations

(1) The ACMA must, in performing its telecommunications functions or exercising its telecommunications powers, do its best to prevent:

- (a) telecommunications networks; and
- (b) facilities;

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) The ACMA must, in performing its telecommunications functions or exercising its telecommunications powers, give officers and authorities of the Commonwealth and of the States and Territories such help as is reasonably necessary for the following purposes:

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

(3) The ACMA 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 of the duty imposed by subsection (1) or (2).

(4) An officer, employee or agent of the ACMA 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 connection with an act done or omitted by the ACMA as mentioned in subsection (3).

313 Obligations of carriers and carriage service providers

(1) A carrier or carriage service provider must, in connection with:

- (a) the operation by the carrier or provider of telecommunications networks or facilities; or
- (b) the supply by the carrier or provider of carriage services;

do the carrier's best or the provider's best to prevent telecommunications 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.

(2) A carriage service intermediary must do the intermediary's best to prevent telecommunications 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.

(3) A carrier or carriage service provider must, in connection with:

- (a) the operation by the carrier or provider of telecommunications networks or facilities; or
- (b) the supply by the carrier or provider of carriage services;

give officers and authorities of the Commonwealth and of the States and Territories such help as is reasonably necessary for the following purposes:

- (c) enforcing the criminal law and laws imposing pecuniary penalties;
- (ca) assisting the enforcement of the criminal laws in force in a foreign country;
- (d) protecting the public revenue;
- (e) safeguarding national security.

Note: Section 314 deals with the terms and conditions on which such help is to be provided.

(4) A carriage service intermediary who arranges for the supply by a carriage service provider of carriage services must, in connection with:

- (a) the operation by the provider of telecommunications networks or facilities; or
- (b) the supply by the provider of carriage services;

give officers and authorities of the Commonwealth and of the States and Territories such help as is reasonably necessary for the following purposes:

- (c) enforcing the criminal law and laws imposing pecuniary penalties;
- (ca) assisting the enforcement of the criminal laws in force in a foreign country;
- (d) protecting the public revenue;
- (e) safeguarding national security.

Note: Section 314 deals with the terms and conditions on which such help is to be provided.

(5) A carrier or carriage service provider is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith:

- (a) in performance of the duty imposed by subsection (1), (2), (3) or (4); or
- (b) in compliance with a direction that the ACMA gives in good faith in performance of its duties under section 312.

(6) An officer, employee or agent of a carrier or of a carriage service provider 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 connection with an act done or omitted by the carrier or provider as mentioned in subsection (5).

(7) A reference in this section to giving help includes a reference to giving help by way of:

- (a) the provision of interception services, including services in executing an interception warrant under the *Telecommunications (Interception and Access) Act 1979*; or
- (b) giving effect to a stored communications warrant under that Act; or
- (c) providing relevant information about:
 - (i) any communication that is lawfully intercepted under such an interception warrant; or
 - (ii) any communication that is lawfully accessed under such a stored communications warrant; or
- (ca) complying with a domestic preservation notice or a foreign preservation notice that is in force under Part 3-1A of that Act; or
- (d) giving effect to authorisations under Division 3 or 4 of Part 4-1 of that Act; or
- (e) disclosing information or a document in accordance with section 280 of this Act.

Note: Additional obligations concerning interception capability and delivery capability are, or may be, imposed on a carrier or carriage service provider under Chapter 5 of the *Telecommunications (Interception and Access) Act 1979*.

314 Terms and conditions on which help is to be given

- (1) This section applies if a person is required to give help to an officer or authority of the Commonwealth, a State or a Territory as mentioned in subsection 313(3) or (4).
- (2) The person must comply with the requirement on the basis that the person neither profits from, nor bears the costs of, giving that help.
- (3) The person must comply with the requirement on such terms and conditions as are:
 - (a) agreed between the following parties:
 - (i) the person;
 - (ii) the Commonwealth, the State or the Territory, as the case may be; or
 - (b) failing agreement, determined by an arbitrator appointed by the parties.

If the parties fail to agree on the appointment of an arbitrator, the ACMA is to appoint the arbitrator.

- (4) An arbitrator appointed by the ACMA under subsection (3) must be a person specified in a written determination made by the Minister.

Note: A person may be specified by name, by inclusion in a specified class or in any other way.

- (5) Before making a determination under subsection (4), the Minister must consult the Attorney-General.
- (6) If an arbitration under this section is conducted by an arbitrator appointed by the ACMA, the cost of the arbitration must be apportioned equally between the parties.
- (7) The regulations may make provision for and in relation to the conduct of an arbitration under this section.
- (8) This section does not apply in relation to the obligation of carriers or carriage service providers under Part 5-3 or 5-5 of the *Telecommunications (Interception and Access) Act 1979* (about interception capability and delivery capability).

Note: Part 5-6 of the *Telecommunications (Interception and Access) Act 1979* contains provisions about the allocation of costs in relation to interception capability and delivery capability.

315 Suspension of supply of carriage service in an emergency

- (1) If a senior officer of a police force or service has reasonable grounds to believe that:
 - (a) an individual has access to a particular carriage service; and
 - (b) the individual has:
 - (i) done an act that has resulted, or is likely to result, in loss of life or in the infliction of serious personal injury; or
 - (ii) made an imminent threat to kill, or seriously injure, another person; or

- (iii) made an imminent threat to cause serious damage to property; or
 - (iv) made an imminent threat to take the individual's own life; or
 - (v) made an imminent threat to do an act that will, or is likely to, endanger the individual's own life or create a serious threat to the individual's health or safety;
- and

(c) the suspension of the supply of the carriage service is reasonably necessary to:

- (i) prevent a recurrence of the act mentioned in subparagraph (b)(i); or
- (ii) prevent or reduce the likelihood of the carrying out of a threat mentioned in subparagraph (b)(ii), (iii), (iv) or (v);

the officer may request a carriage service provider to suspend the supply of the carriage service.

(2) The carriage service provider may comply with the request.

(3) This section does not, by implication, limit any other powers that the provider may have to suspend the supply of the carriage service.

(3A) The provider 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 compliance with the request.

(3B) An officer, employee or agent of the provider 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 connection with an act done or omitted by the provider as mentioned in subsection (3A).

(4) In this section:

senior officer, in relation to a police force or service, means a commissioned officer of the force or service who holds a rank not lower than the rank of Assistant Commissioner.

316 Generality of Part not limited

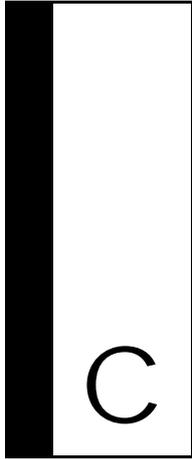
Nothing in this Part limits the generality of anything else in it.



Appendix B – List of Submissions

- 1 Mr Johann Trevaskis
- 2 Mr John Denham
- 3 Civil Liberties Australia
- 4 Australian Communications Consumer Action Network
- 5 iiNet
- 6 Australian Lawyers for Human Rights
- 7 Communications Alliance Ltd & Australian Mobile Telecommunications Association
 - 7.1 Supplementary submission
- 8 Australian Communications and Media Authority
 - 8.1 Supplementary submission
- 9 National Children’s and Youth Law Centre
- 10 Associate Professor Bruce Arnold
- 11 Australian Privacy Foundation
 - 11.1 Supplementary submission
- 12 Uniting Church in Australia, Synod of Victoria and Tasmania
- 13 Internet Society of Australia
- 14 Office of the Inspector of the Independent Commission Against Corruption
- 15 Australian Securities & Investments Commission
 - 15.1 Supplementary submission
 - 15.2 Supplementary submission
- 16 Australian Crime Commission
- 17 Electronic Frontiers Australia
- 18 AIMIA Digital Policy Group

- 19 Australian Government Department of Communications
 - 19.1 Supplementary submission
 - 19.2 Supplementary submission
- 20 Australian Federal Police
 - 20.1 Supplementary submission
 - 20.2 Supplementary submission
 - 20.3 Supplementary submission
- 21 Cyberspace Law and Policy Community, University of New South Wales



Appendix C – Public hearings & witnesses

Wednesday, 29 October 2014 - Canberra

Australian Federal Police

Commander Glen McEwen, Acting National Manager, High Tech Crime Operations

Assistant Commissioner Kevin Zuccato, Acting Deputy Commissioner Close Operations Support

Australian Government Department of Communications

Mr Rohan Buettel, Assistant Secretary, Consumer Protection Branch, Consumer and Content Division

Mr Ian Robinson, Deputy Secretary, Infrastructure Group

Wednesday, 3 December 2014 – Canberra

Australian Securities and Investments Commission

Mr Tim Mullaly, Senior Executive Leader

Mr Greg Tanzer, Commissioner

Wednesday, 25 February 2015 – Canberra

Australian Crime Commission

Ms Judith Lind, Executive Director Strategy & Specialist Capabilities

Dr Nathan Newman, Manager Strategy and Policy Coordination

Wednesday, 4 March 2015 – Canberra

Australian Privacy Foundation

Dr Roger Clarke, Immediate Past Chair

Electronic Frontiers Australia Inc

Mr Jon Lawrence, Executive Officer

Friday, 6 March 2015 – Sydney**Australian Communications Consumer Action Network**

Ms Una Lawrence, Director of Policy

Mr Xavier O'Halloran, Policy Officer

Australian Lawyers for Human Rights

Ms Roslyn Cook, Vice President

Australian Mobile Telecommunications Association

Ms Lisa Brown, Policy Manger

Communications Alliance Ltd

Mrs Christiane Gillespie-Jones, Director Program Management

International Engineering and Information Sciences, University of Wollongong

Associate Professor Katina Michael, Associate Dean

Cyberspace Law and Policy Centre, University of New South Wales

Mr David Anthony Vaile, Co-convenor, Cyberspace Law and Policy Community,
Faculty of Law

Mr Paolo Remati, Juris Doctor Student-Intern

Internet Society of Australia

Mr Laurie Patton, Chief Executive Officer

Ms Holly Raiche, Chair, Policy Committee

Private Capacity

Dr Robert Nicholls

Uniting Church in Australia, Synod of Victoria and Tasmania

Dr Mark Andrew Zirnsak, Director, Justice and International Mission Unit

Wednesday, 18 March 2015 – Canberra**Australian Government Department of Communications**

Ms Trudi Bean, Deputy General Counsel

Mr Ian Robinson, Deputy Secretary, Infrastructure Division