5

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