3

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.

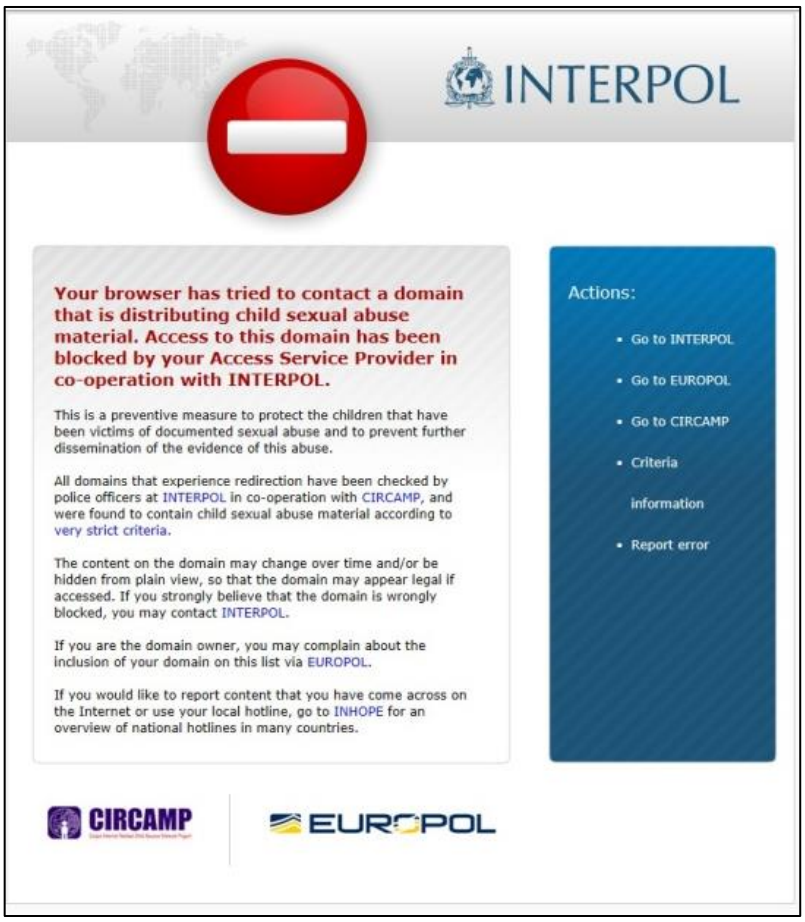
---

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 Telecommunicatons 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.