2

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 he 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.