4

Technical issues

Technical limits of disrupting online activity

4.1 During the course of the inquiry, a number of technical issues were raised about the use of s.313 to disrupt illegal online activity, including whether the blocking of websites is practically effective, the cost of disruption to ISPs and their customers, and the ability to avoid inadvertent blocking of non-target websites.

4.2 The blocking of websites can involve the targeting of the Internet Protocol (IP) address (the numerical label of an internet resource or computer), the domain name (the unique name of an internet resource) or the Uniform Resource Locater (URL—the specific web address of a website).

4.3 When connecting to the Internet, the ISP sends the URL to a domain name server which converts the word-based web address to a numerical IP address. The packets of information sent to and from a website use the IP address of the website and the IP address of a computer, to identify each other when exchanging data.[1]

4.4 There is not always a one-to-one relationship between the URL and an IP address:

> … there is an option that is commonly used called shared IP posting. In this name-based virtual hosting, or shared IP hosting, the virtual host serves multiple host names with one machine and a single IP address. The reason that that works is, when a web browser requests a resource from a web server using hypertext transfer protocol—the HTTP of an address—it includes the host

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

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

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

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

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

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

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

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

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

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

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

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

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

4.9 Other technical limitations included the existence of Virtual Private Networks (VPN) and Tor. A VPN 'creates essentially a dedicated pipe through which you can send secure communications'. It is 'used in the corporate and government contexts for absolutely legitimate purposes in terms of securing external access to networks'. A VPN 'allows you to appear to be coming from a location where you are not actually at, so it does obfuscate your location in that sense. It obfuscates potentially your source internet protocol address as well—your IP address'.[7] Tor is a tool designed to make internet activity anonymous. It is designed to 'bounce your requests and your traffic around a number of random sites across the internet to essentially anonymise who you are and not just where you are coming from'. Such tools 'provide the ability for people that wish to get around the sorts of actions that might be taken under section 313 … to essentially circumvent those actions pretty easily'.[8]

4.10 The Australian Federal Police (AFP) acknowledged the difficulties caused by 'VPNs and the camouflaging activities that people do utilise within the internet', but highlighted what could be achieved—emphasising that s.313 was just one of a suite of measures undertaken by the AFP:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

> Most hosting businesses are commercial businesses that do not want to offend law enforcement agencies and do not want to be the deep pockets in civil lawsuits, so a stern letter by email to a web host saying that it is hosting material which is offensive, defamatory or inappropriate in some way in Australia can often get a response which is the publisher's defence, 'We didn't know it was there'—perfectly valid—and then potentially a takedown of that offending material.
>
> This works particularly well if the material would breach the criminal law in either the country where the material is actually hosted or where the web hosting company is domiciled. For child

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

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

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

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

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

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

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

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

Costs

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

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

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

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

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

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

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

> costs—specifically, labour, infrastructure and service maintenance costs—associated with supporting authorities in their investigations.[23]

4.22 Professor Michael noted that:

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

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

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

> … but the operational costs of configuring the routing table of a border gateway router are mainly the cost of making sure that the 313 notice on its face was something that the carrier or carriage-service provider could rely on to get the immunity that is provided under 313.[25]

4.25 Dr Nicholls did 'not believe we are talking about large amounts of money'.[26]

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

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

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

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

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

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

Avoiding disruption of non-target sites

4.27 The inadvertent blocking of non-target websites by ASIC in 2013 was the result of a fundamental error in its targeting of websites. ASIC requested that 'telecommunications carriers block the IP addresses' of offending websites.[28] This opened the way for the inadvertent blocking of the hundreds of thousands of websites that shared the same IP address.[29]

4.28 Attempting to disrupt illegal online activity by blocking IP addresses is also relatively easy to avoid. The Synod of Victoria and Tasmania of the Uniting Church in Australia noted that:

> … most child sexual abuse providers now use fast fluxing, which means they are changing their IP address every few minutes; it might be every 20 minutes. The AFP actually had some data; I think they watched a site over a prolonged period of time and found it was changing its IP address every 20 minutes. It is senseless then to try to disrupt an IP address.[30]

4.29 Disrupting the domain name—the method used by INTERPOL to disrupt CEM—also carries risks of over-blocking, 'as the whole domain is deemed illegal if any part of it is found to contain sexual abuse material with children'.[31] This has led to a cautious approach to the disruption of domains:

> … with the domain, there is an attempt to contact the domain provider prior to them being put on the list and giving them every opportunity to remove the material prior to them getting on the list, so, where a domain provider is either negligent or wilfully continuing to host that material, there is an argument they deserve to be on the list and have that disrupted as a mechanism to try to force them to take the material down.[32]

4.30 The criticism of this approach is that 'the tight criteria of this form of access blocking reduces its effectiveness as a dynamic disruption strategy against the commercial child sexual abuse industry'.[33]

4.31 The most precise method of disrupting illegal activity online is to target the URL—the web address—'because you are then going after just the site

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Committee Conclusions

4.35 The Committee is cognisant of the fact that by itself the disruption of illegal online services will not prevent criminal activity. People determined to do so will always find a way to get around blocks on the internet, and the capacity to target sites will always be constrained by the need to avoid collateral damage. Nonetheless, the Committee is of the view that there is sufficient evidence that the disruption of websites is technically feasible and provides an effective avenue to frustrate criminal activity where other means are not available and as part of a suite of other investigative and enforcement measures. The fact that particular activities or content may have to be found and blocked repeatedly does not negate the necessity of trying. Rather, it emphasises the fact that—as in any other area of law enforcement—constant vigilance is required. The ability of government agencies to disrupt illegal online services through s.313 is a necessary one.

4.36 Avoiding the inadvertent disruption of non-target websites is chiefly the outcome of technological competence and robust administration. Mistakes will be avoided through the use of robust or transparent processes. A better understanding of technology, combined with better processes, will prevent problems from occurring; or, allow a more rapid identification and response to a problem. It is the view of the Committee, therefore, that all government agencies utilising s.313 to disrupt illegal online services should have transparent and robust processes surrounding its use (see Chapter 3), and the requisite level of technical expertise within, or accessible to, the agency to carry out such requests (see Chapter 5, Recommendation 2).

4.37 The Committee is also conscious of the potential costs for ISPs in complying with requests for assistance from government agencies under s.313. The Committee believes that it is important that agencies consult with industry about the best means of complying with requests for assistance, including managing costs.