Uniting Church in Australia
SYNOD OF VICTORIA AND TASMANIA

Justice and International Mission Unit
130 Little Collins Street
Melbourne Victoria
Australia 3000
Telephone: +61-3-9251 5271
Facsimile: +61-3-9251 5241
jim@victas.uca.org.au

27 May 2016

Submission from the Synod of Victoria and Tasmania, Uniting Church in Australia to the draft guidelines for the use of section 313(3) of the *Telecommunications Act 1997* by government agencies for the lawful disruption of access to online services

The Synod of Victoria and Tasmania, Uniting Church in Australia, welcomes this opportunity to make a submission to the draft guidelines for the use of section 313(3) of the *Telecommunications Act 1997* by government agencies for the lawful disruption of access to online services. The Synod strongly supports the role of Section 313(3) to require carriers and carriage service providers, in connection with their operations of telecommunication networks and facilities or the supply of carriage services, give officers and authorities of the Commonwealth, states and territories such help as is reasonably necessary to:

- Enforce the criminal law and laws imposing pecuniary penalties;
- Assist in the enforcement of the criminal law in force in a foreign country;
- Protect the public revenue; and
- Safeguard national security.

The Synod broadly supports the guidelines as drafted, with additional comments below.

The Synod believes that Section 313(3) requests to disrupt access to online services should not be required to expire after a specified time, but rather should be subject to periodic review. Where online material relates to serious criminal activity, such as child sexual abuse, tax evasion or fraud, then it is appropriate to disrupt access to the material for as long as the material is hosted at the same online location. This is different to the guidelines, which suggest that Section 313(3) requests to disrupt access to online services should expire after a specified time.

Blocking an IP address rather than a URL or a domain is likely to be ineffective, as criminal enterprises often use fast flux to keep changing their IP address. Cybertip.ca noted that some of the child sexual abuse sites use the counter-strategy of fast flux networks. Fast flux domains use nameservers that supply IP addresses that change quickly and constantly. Typically these are IP addresses of compromised residential computers that are serving the content of the webpage or acting as a proxy to the content hosted at another location. This means that a geographic lookup conducted on a website may provide a different result depending on when it is conducted – even if the lookups occur 10 minutes apart. Cybertip.ca found that over a 48 hour period one child sexual abuse website cycled through 212 unique IP addresses, located in 16 different countries (including Australia) and would change

approximately every three minutes.[1] This renders any system that would attempt to block access to child sexual abuse sites on the basis of IP addresses ineffective.

Australian agencies should not be required to consult with an ISP or other business where the agency has a reasonable belief that the ISP or business in question is knowingly assisting the criminal activity in question or is hostile to assisting in law enforcement efforts. The agency should also not be required to consult with the ISP or other business where there is a reasonable fear that the ISP or business in question may tip off the criminals involved that they have attracted the attention of law enforcement. However, the latter point is mitigated by the fact that once the disruption is in place, the criminals know that they have attracted the attention of law enforcement.

The Financial Coalition Against Child Pornography reports online businesses providing "Bulletproof Hosting". These hosts promise customers their websites will not be taken down, regardless of complaints or content. Bulletproof hosts use a combination of distributed services to maintain uptime for their customers. Specific tactics they use include:[2]

- Registering the domain name with a registrar with relaxed enforcement. Depending on the location and enforcement policies, some registrars are used more heavily than others for illicit activities.
- Sharing and shuffling IP addresses to minimise downtime if particular IPs are shut down. This ensures content remains up while being indifferent to the status of particular domains. Instead of relying on one IP, bulletproof hosting relies on multiple IPs that can keep the content up independent of specific IP shut downs.
- Using a standardised yet specific naming methodology for name servers to minimise service interruption.
- Soliciting business and communicating with customers using unmonitored, private media. Bulletproof hosts frequently advertise their services on message boards frequented by their target customer base. From there, e-mail, instant messaging and other non-public options are used to further business dealings. This allows bulletproof hosting services to remain largely underground and reduces exposure to enforcement entities.
- Collecting payment using unregulated payment services to limit scrutiny and preserve anonymity. The use of small payment processors originating from outside the US is popular due to lax regulatory environments and lessened cooperation with law enforcement agencies.

Dr Mark Zirnsak
Director
Justice and International Mission Unit
Synod of Victoria and Tasmania
Uniting Church in Australia
130 Little Collins Street
Melbourne, Victoria, 3000
Phone: (03) 9251 5265

[1] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, pp. 62-63.
[2] Financial Coalition Against Child Pornography, 'Report on Trends in Online Crime and Their Potential Implications in the Fight Against Commercial Child Pornography', 1 February 2011, pp. 12-13.