

ISPANZ POSITION PAPER

CONTENT FILTERING

The Christchurch massacre on 15th March 2019 has emphasised the desirability of ISPs being able to block streamed and social media content originating from terrorists or which may pose a threat to national security. This Position Paper, which previously focussed on content filtering of objectionable material, has been rewritten to include content filtering of terrorist and security related content. Members should read this Position Paper in conjunction with our Information Papers IP 001 on Lawful Interception and IP 003 on Copyright Material which bear on members' legal obligations to aid government security initiatives and their obligations to deny customers' access to content protected by intellectual property law.

No Filtering and No Monitoring

ISPs do not normally filter content or actively monitor their customers' activities. Filtering services are available to customers on an opt-in basis, but ISPs typically don't enforce content restrictions on their customers. While some customers want to be protected from inappropriate or offensive content, one person's propaganda can be another person's news. Applying blanket rules on content filtering would raise significant issues around freedom of speech and freedom of information.

Child Pornography

The most common exceptions to 'no filtering and no monitoring' are the Digital Child Exploitation Filter System (DCEFS), which some ISPs subscribe to, and family content filtering services either offered by ISPs or through third parties to take the "nasties" out of the internet for families and educational institutions.

The Department of Internal Affairs offers the DCEFS to ISPs. The DCEFS focuses solely on websites offering clearly objectionable images of child sexual abuse, which is a serious offence for anyone in New Zealand to access. It is relatively simple to get DCEFS up and running. Basically the system uses BGP via a GIF tunnel and the DIA advertise specific routes relating to child abuse sites, these routes are /32 routes and are advertised approximately 4 times a day. ISPANZ recommends that members investigate implementing DCEFS. Full details can be found at: <https://www.dia.govt.nz/Censorship-DCEFS>

Illegal Activity

In the case of suspected criminal activity the police could issue a search warrant to request end user contact details for a user who was using a given IP address at a given time and date. In these instances the Police would contact the end user directly rather than involving the ISP. Details are contained in IP 001, which is available to ISPANZ members.

Blocking Terrorist or Security Related Content

On 15th March Vodafone NZ, Spark and 2degrees moved rapidly to take the unprecedented step to jointly identify and suspend access to web sites that were hosting video footage taken by the gunman related to the horrific terrorism incident in Christchurch. We commend their rapid action. We also commend their joint letter to the major social media platforms which can be found here: <https://www.reseller.co.nz/article/659010/an-open-letter-from-spark-vodafone-2degrees-facebook-twitter-google/>

Smaller ISPs do not necessarily have the technical ability to act so quickly in the same way, but in this uncertain world their need to may increase. We agree with Vodafone NZ, Spark and 2degrees when they say:

“internet service providers are the ambulance at the bottom of the cliff, with blunt tools involving the blocking of sites after the fact. The greatest challenge is how to prevent this sort of material being uploaded and shared on social media platforms and forums.

We call on Facebook, Twitter and Google, whose platforms carry so much content, to be a part of an urgent discussion at an industry and New Zealand Government level on an enduring solution to this issue.”

ISPANZ supports such a discussion, wishes to take part and encourages members to contribute directly.

In Summary

- ISPs do not normally filter content or monitor customers’ activities.
- ISPs offer filtering services on an opt-in basis.
- ISPANZ recommends that members investigate implementing DCEFS.
- Whilst ISPANZ does not take any position on matters of taste or opinion, we do not condone criminal activity and expect our members to cooperate fully with any police investigation related to possible criminal activity.
- ISPANZ strongly condemns terrorist activity, deplores internet content glorifying terrorist acts or encouraging hate crime, and encourages members to pro-actively cooperate with the police and security services to block such content.
- We support the industry and government discussion advocated by the larger ISPs and wish to contribute to it.