

## Critics pick holes in child porn filter

By [Chris Barton](#)

4:00 AM Saturday Mar 20, 2010



Photo / Bay of Plenty Times

Over the next few months some New Zealanders are likely to get a nasty shock while browsing the internet - a web page that pops up on their computer saying "STOP!".

Some will genuinely be surprised, having accidentally stumbled into a nefarious zone, perhaps by curiously clicking a web link in a spam email, or perhaps by a "popup" diversion from some other website.

Others, however, will have been driven by some sick, unfathomable urge to seek out the material being blocked. For both, the message on screen is the same - accessing the content being blocked is a crime.

In February the Department of Internal Affairs (DIA) quietly started blocking access from New Zealand to about 7000 websites containing images of child sexual abuse.

If all goes to plan, the centralised system known as the Digital Child Exploitation Filter will be progressively rolled out to almost all internet providers.

It has cost \$150,000 for the software and running costs are budgeted at \$25,000 a year.

Supporters say it's a bold move in the battle against an abhorrent trade.

"This is an important step forward in protecting our children from abusers," says director Alan Bell, of child advocacy group ECPAT New Zealand.

Others aren't so sure, saying the filter won't work and that it represents the thin edge of the wedge of more internet censorship and restrictions on the freedom of speech.

"Blocking child porn - on the face of it, that sounds like a good thing," says Tech Liberty spokesperson Thomas Beagle, whose group has set up a website campaigning to stop the filter.

"Our argument is that it won't work and we fear it will be extended in the future."

InternetNZ has similar worries: "A government filtering system, centrally operated, is not the answer. It risks leaving parents feeling that the Government is providing a safe environment, but it cannot deliver on that promise," says internetNZ Policy Director Jordan Carter.

---

For its part, the DIA says the filter is there simply to prevent people from accessing images of child sexual abuse - images that three DIA inspectors have found to be clearly "objectionable" and an offence to possess under the Films, Videos, and Publications Classification Act.

"Even if it's just one image by one image, it will reduce the distribution of images of actual children and babies being victimised and it will act as a deterrent," says DIA deputy secretary for Regulation and Compliance Keith Manch.

When talking about child sexual abuse images, it's difficult to argue against any efforts to censor - except perhaps when the censorship is ineffectual and causes more problems than it solves. Here we attempt to unravel the complexities of attempts to impose control on an untamed internet frontier.

### **Will the filter do its job?**

Groups such as Tech Liberty and internetNZ say the website filter is at best a crude device and not very effective.

They point out the filter can't intercept encrypted web traffic, or file-sharing, email, chat, and instant messaging - the main ways in which child pornography is traded. Website filtering can also easily be evaded by anyone with a reasonable degree of technical skill.

Beagle points out there are plenty of instructions on the net to bypass filters. Some methods involve free software such as The Onion Router (Tor) which was designed to avoid network surveillance and has been used in places like China and Iran, where internet use is highly regulated.

On the other hand, the DIA says there is plenty of evidence that people do visit the websites in question - as shown by overseas operations where agencies take down illegal sites and compile information about those who have accessed them from credit card records.

There is also evidence from the DIA filter trial of tens of thousands of requests per month being blocked.

Manch says some included repeated requests by individuals and "popups and popunders" where sites, uninvited, provide links to other objectionable material.

When the filter is fully operational, the DIA will report such results regularly. "The real issue behind this is the children that are abused to make these images."

Though he understands the argument that the cost benefit of the filter doesn't stack up, Manch says the reality is that every image is the continued victimisation of the child.

Manch accepts the filter has a limited impact on child porn but says it makes an important contribution by preventing some people from accessing images.

"In some cases they may be people doing that for the first time, or early on in their exposure or desire to use these things," he says. "If they get blocked with a page from us, maybe that's useful as a deterrent."

### **How does the filter work?**

As with most filtering systems, the DIA's is built around a list of known websites - in this case sites which host child sexual abuse images. internet service providers using the system set up a secure link between the DIA's computer system and their computers.

---

Via the secure link, the DIA system "advertises" internet routing information that relates to the list of child sexual abuse websites. What it's actually advertising is a false route.

When someone attempts to access a website that matches this routing information, that request is sent to the DIA's filter for examination. If the request is for a website on the DIA's list, the system will present a "landing page" informing the user the request has been stopped. If the request does not match an item on the list, the user sees the requested page as normal.

### **Is all internet traffic filtered?**

No. Most of the time, when people request access to a website it will go straight to that page and won't go to the filter. But it is common for a web server to host multiple websites on a single internet address - like lots of different offices in a multi-storey building.

All requests to sites on one of the filtered addresses will be diverted to the DIA's server. The DIA's filtering server then looks at the request and blocks only those on the banned list.

The landing page for blocked sites gives users the option of disputing the block by completing an appeal form which is then sent to the department. The form does not ask for any contact details, but Manch says people can, if they wish, supply their contact information with a request to have a response from the DIA.

### **Is Big Brother watching?**

Manch says the filter is deliberately designed not to follow-up on information for enforcement purposes.

"We see it as a prevention tool." He says there is no logging of the computer address of the user requesting access to blocked pages.

There is, however, logging of some information for 30 days for trouble-shooting. "No user-identifiable information is kept or recorded. Following the period of 30 days, all records relating to the filter are destroyed."

### **Is the filter the thin edge of the wedge?**

Some are concerned use of the filter will be extended beyond child porn sites; that it may be used, for example, to block access to websites breaching court suppression orders or sites breaching copyright.

Unlike Australia, where the Government is trying to pass a new law that would require mandatory filtering of the internet, New Zealand's filter is implemented voluntarily by agreement with internet providers. To date just two small providers, Watchdog and Maxnet, have started filtering.

Telstraclear and Vodafone have both said they will use the filter when they get the go-ahead from the DIA. Telecom and Orcon haven't yet decided but both say they are working with the DIA. A few, including WorldxChange and Slingshot, have indicated they won't use the filter.

Manch says the initiative has been undertaken by the censorship compliance unit of DIA, and hasn't been discussed with other parts of Government.

The DIA has a Code of Practice and agreements between internet service providers for implementation. The department's contract for the use of the Netclean Whitebox software used by the filter system also constrains its use to only filtering images on child sexual abuse.

### **Does the filter break the internet?**

---

Because it advertises false routes, some commentators say the filter causes the internet to lie, disrupting its proper functioning. Worse still, it creates a potential single point of failure and an ideal place for hackers to attack.

"Malicious false advertisements can break routing and cause packets to go to the wrong server without any identifiable tell-tales for end users to be able to protect themselves," says Gerard Creamer at TechLiberty.

He says the filter introduces an architectural weakness into the New Zealand internet.

Manch disagrees. "The system utilises the same technology that runs the backbone of the internet - that system is inherently stable and able to be scaled very easily." He says if it did fail, all that would happen is people would be able to see the previously blocked websites.

### **Who watches the watchers?**

The Independent Reference Group will have oversight of the process and be a point of review for complaints against the filter and its operation. Some have questioned the independence of the group because some of its members are from the department and the censor's office.

But technology consultant and commentator Mark Harris clearly is independent. On his blog, he says: "I am part of the Independent Reference Group, mainly because I don't believe the filter will work, and because I am implacably opposed to any extension of it."

Manch says the oversight group will have access to information about the banned sites list, but not the list itself. "They are privy to the reasoning behind the block, but not the site that is subject of the block."

Beagle says he's concerned that the DIA is engaged in secret censorship. "We don't know what's being blocked. They are basically saying, 'Trust us'." Tech Liberty attempted to get access to the list through the Official Information Act, but was turned down on the grounds that making the list public would provide a means for people to commit a crime.

Beagle says there is an argument for more transparency. When a similar list was leaked in Germany, it resulted in 20 per cent of the websites named being shut down in a week.

"To suggest this is a dangerous affront to internet freedom is, I think, a pretty long bow," says Vodafone public policy manager Hayden Glass. He agrees that internet providers are essentially a conduit for the internet and, as such, not liable for customer breaches of the law.

But he sees the DIA's initiative as something that will help limit child pornography. When the DIA says, 'Can you help us enforce the law with this system we have created, carefully considering the concerns around internet freedom?', we say, 'Yes this is a sensible thing to do'."

On the web: [www.dia.govt.nz](http://www.dia.govt.nz); [stopthefilter.org.nz](http://stopthefilter.org.nz); [www.ecpat.org.nz](http://www.ecpat.org.nz)

By [Chris Barton](#)

Copyright ©2010, APN Holdings NZ Limited