

12 March 2012

Matt Taylor  
[matt@matthewtaylor.co.nz](mailto:matt@matthewtaylor.co.nz)

Dear Matt

Thank you for your email of 7 February 2012 requesting, under the Official Information Act 1982 (the Act), information concerning the Digital Child Exploitation Filtering System. I will address each of your questions in turn.

**1) *How many URLs came in for review (review being deciding whether they are added to the filter list, or not added to the filter list) in January 2012?***

The Department received 449 URLs for review from members of the public via our partnership with ChildAlert. A further 21 URLs were supplied through our involvement in the Interpol Worst Sites Project. A number of other sites that came to our attention as a result of investigations were also reviewed.

**2) *How many URLs were reviewed in January 2012 (not including the monthly review of all URLs on the list)?***

The Department reviewed over 500 URLs in January 2012.

**3) *How many URLs came in for review in January 2012 from the public?***

See answer to question 1.

**4) *How many of those public provided URLs were subsequently blocked?***

50 URLs that were submitted by the public in January 2012 were subsequently added to the filter list.

**5) *I understand requests for a full copy of the filter list have been previously declined. Could you please send me a list of just the domains from the list of URLs that are blocked, unless the whole domain is blocked (my assumption is if the whole site is blocked it's a site only for child sexual abuse material. I'm looking for the sites that have URLs blocked, but also have non-child sexual abuse content on them). Eg. If***

***http://filesharingsite.com/aw4ey6897 is blocked, I'm looking for just the http://filesharingsite.com part.***

- 6) *If 5) is not possible, the domains of search engines, file sharing locker services, and social networks that have URLs blocked.***
- 7) *If 5) is not possible, a copy of the list with the first domain name part removed, but TLD and the rest of the URL intact. Eg. http://.com/aw4ey6897***

Possession of child sexual abuse material is an offence that carries a maximum penalty of 5 years imprisonment. As the release of part of the URL of the websites being filtered would facilitate a search for such material, the Department is withholding the information requested in questions 5 to 7 in terms of section 6(c) of the Act (where the release of the information is likely to prejudice the maintenance of the law).

- 8) *If 7) is not possible, a copy of the list with just TLDs (or just a count of the different TLDs). Eg. 50x .com, 100x .ru***

The following is a count of the top level domains (TLDs) of the website on the filter list as at 12 March 2012

.com	283	.ru	93
.net	65	.org	4
.info	23	.biz	6
.us	5	.me	2
.tv	1	.in	6
.ir	1	.su	1
.ws	1		

- 9) *Are abuse reports and takedown requests sent to hosting companies and law enforcement etc. when URLs are added to the filter?***

The Department works with partner agencies in other jurisdictions to get international sites removed.

- 10) *In the Independent Reference Group's December 2011 report it states that "Additionally 18% of the users originated from search engines such as google images". Was Google informed of those images?***

We have a very good relationship with Google and they have been made aware of any objectionable links available via their services. The statement in the December 2011 report used Google Images as an example of a type of service. It was not a statement that 18% of users originated from Google Images.

**11) If they were, how long after the DIA was made aware of them was Google made aware of them?**

Google is advised of objectionable links available via its services as soon as is practicable.

**12) Could you please send me a copy of all investigator reports held?**

Attachment 1 is a sample investigator's report of a filtered website. Information that would identify the site, including a screen capture of the webpage has been removed in terms of section 6(c) of the Act. Information that would identify officers involved in the operation of the filter have been withheld in terms of section 9(2)(g)(ii) of the Act (to protect officers from improper pressure or harassment).

**13) What data is collected with appeals?**

The only data that is collected with an appeal is the data the user chooses to submit and the date and time of the appeal.

**14) What data is collected when someone tries to visit a blacklisted site, including log data collected by the <http://dce.net.nz> web host? For 13) and 14), if you could include an example log etc. that would be helpful.**

The filter only records the service provider name, the resource requested and date and time. No user data is stored. Attachment 2 is an officer's report on an appeal which includes the information supplied by the appellant. Information that would identify the site has been removed in terms of section 6(c) of the Act. Information that would identify officers involved in the operation of the filter have been withheld in terms of section 9(2)(g)(ii) of the Act.

**15) In some reports, statistics on device type is included. Device type is not listed in the Code of Practice, 6.1, as data collected. Is other data collected in the course of the filtering process that isn't listed under 6.1, if so, what?**

No other data is collected.

**16) Code of Practice, 6.1 says that the requester's IP address is logged. 6.2 says that the system will anonymise the IP address. A previous response to a request for information stated: "When a request to access a website on the filtering list is blocked the system retains the IP address of the computer from which the request originated. This information is retained for up to 30 days for system maintenance releases and then deleted". So, when are IP addresses anonymised/how long are IP addresses kept for?**

When a person requests a webpage that is blocked, the IP address of the requester will be presented to the service so that blocking page can be sent to them. IP addresses are anonymised by the system itself, no record is kept.

**17) How does the system anonymise IP addresses? For 17), if you could include an example of an anonymised IP address that would be helpful.**

The filtering system anonymises IP addresses using a tool developed by Netclean. By not logging the data, the system prevents anyone from reviewing source IP. All IP addresses appear as 0.0.0.0.

**18) Code of Practice, 6.5 says that “Data shall not be used in support of any investigation or enforcement activity undertaken by the Department.” Has this been the case?**

Data from the filtering system has never been used in support of any investigation or enforcement activity.

**18b) Has data been used in investigations or enforcement activities not undertaken by the Department?**

See answer to question 18.

**18c) Has data been shared with other departments? If so, what data has been shared?**

No data from the filtering system has been shared with other departments.

**19) Could you please send me anything held discussing the implementation of Google Analytics on the <http://dce.net.nz> website?**

Google Analytics is a free service offered by Google that generates statistics about the visitors to a website, in particular the referrers used. Google Analytics is used to confirm other statistics generated from the filter and to provide better reporting to the IRG and public.

**20) Were any privacy issues raised around using Google Analytics on the <http://dce.net.nz> website?**

No. The Department does not consider that the use of Google Analytics raises any privacy concerns.

**21) Does the DIA have a contract or contracts with Google?**

Google Analytics is free software. The terms and conditions for the use of Google Analytics are available at <http://www.google.com/analytics/tos.html>.

**22) If so, could you please send me a copy?**

See answer to question 21.

**23) If 22) is not possible, could you please tell me the title of the contract(s) and what it/they relate(s) to?**

See answer to question 21.

**24) If 22) is not possible, could you please send me parts of the contract or contracts regarding collection, privacy, and disclosure of user data collected?**

See answer to question 21.

**25) What is the data Google Analytics provides used for? Eg. the device type statistics provided in some reports?**

See answer to question 19.

**26) From the Independent Reference Group's August 2011 minutes:**

***“Andrew Bowater asked whether the Censorship Compliance Unit can identify whether a person who is being prosecuted has been blocked by the filtering system. Using the hash value of the filtering system’s blocking page, Inspectors of Publications now check seized computers to see if it has been blocked by the filtering system. The Department has yet to come across an offender that has been blocked by the filter.”***

***Can you please explain what a hash value is? Eg. how they're implemented, how they're stored on visitor's computers, how they're stored on DIA equipment.***

Every image, photograph, document or movie found on a computer can be run through a hashing process that will generate, using a mathematical algorithm, a unique hash value for that file. A hash value is a set of numbers and letters strung together and once assigned this hash value cannot be altered. If the same image is hashed twice, the hash value will remain consistent; however, if even 1 pixel of an image is altered that new image will be assigned a new hash value.

When the Department seizes a computer or storage device as the result of exercising a search warrant, as part of the forensic examination of that device, the Department is able to look to see whether the offender has been blocked by the filter by looking for the unique hash value generated by objects on the blocking page.

While this information plays no part in the prosecution of an individual, it is useful in understanding the behaviour of persons who access child sexual abuse material and the effectiveness of the filtering system.

**27) Does storing hash values violate the “no information enabling the identification of an individual will be stored” part of the Code of Practice, considering individual computers can be matched with requests intercepted by the filter?**

See answer to question 26.

**28) Is the “ensure the privacy of the requester is maintained by allowing an appeal to be lodged anonymously” part of the Code of Practice is being followed?**

Yes.

**29) The Independent Reference Group's March 2011 meeting minutes talks about a Russian child model website. Could you please send me anything held regarding this website?**

The website in question is divided into a public area and a member-only area. The public area contains images of a young girl dressed in a variety of outfits, which would not be classified as objectionable. The member-only area contains more sexualised images of the same girl that are objectionable. The Independent Reference Group (IRG) agreed that, as the purpose of the site was to sexually exploit a child, it should be added to the filter list.

**30) Was the Russian child model website considered a borderline case?**

No.

**31) Was the Russian child model website considered a case of clearly illegal, objectionable images of child sexual abuse?**

See answer to question 29.

**32) Other than the Russian child model website, have any other URLs been brought to the group for discussion over whether they should be blocked? If so, could you please send me anything held regarding those URLs?**

No.

**33) I understand photographs of real life children being sexually abused, CGI and drawings of children being sexually abused, and the Russian child model website are being blocked. Are any URLs being blocked that don't come under that list?**

Material being blocked by the filtering system complies with the Code of Practice, which states:

2.1 The scope of the DCEFS will be limited to preventing access to known websites that contain publications that promote or support, or tend to

promote or support, the exploitation of children, or young persons, or both, for sexual purposes.

2.2 The DCEFS will focus on preventing access to known websites containing child sexual abuse images.

**34) *If so, could you please provide a general description of the content of those URLs?***

See answer to question 33.

**35) *As I understand them, DIA reports say that 0 URLs were removed from the filter between April 2011 and August 2011. Could you please explain why this was?***

On review, all sites continued to contain abuse material and subsequently had not been taken down by enforcement agencies in other countries or were still under investigation.

**36) *How many URLs has the Independent Reference Group reviewed?***

One.

**37) *What was the result of those reviews?***

See answer to question 29.

**38) *How many opportunities has the Independent Reference Group had to review URLs?***

The IRG is able to review any URL on the filter list at each of its meetings.

**39) *How many of those opportunities have they taken up?***

None.

**40) *I understand the whole filter contract has previously been withheld. Could you please send me the section of the filtering contract that discusses what the filter is to be used for and to be limited to?***

While the Department has previously refused to release the whole contract with Netclean, it has referred to clauses in that contract as one of the reasons why the scope of the filtering system can't expand. The following is a summary of the relevant conditions of the Customer Licence Agreement.

The primary goal of the NetClean Whitebox is to block access to child pornography.

In order to achieve the main objective, NetClean allow that even non-child pornography is filtered, as long as it is material which is illegal to possess under

the country's law and that the main objective for the installation is to block access to child pornography.

The filter must not be used to restrict freedom of expression, nor to prevent the transmission of information which in itself is legal to possess.

Furthermore, the installation of NetClean Whitebox must not violate the articles 18 and 19 of the Universal Declaration of Human Rights.

**41) Could you please send me any correspondence, electronic, written or otherwise, with ISPs regarding them joining or leaving the filter?**

Attachment 3 contains the following:

- An email (14/7/08) from the CEO of TelstraClear to the Minister of Internal Affairs and the Minister's reply (20/08/08);
- Emails between the Department and Callplus (21/10/08 and 30/10/08). Technical information regarding the operation of the filter and information regarding its location has been withheld under section 6(c) of the Act. The telephone numbers of officers have been withheld under section 9(2)(g)(ii) of the Act.
- A letter from the Department to Telecom (29/09/09).
- Emails between the Department and Telecom (1/11/10) regarding a draft press release.
- A letter from the Department to ISPs (list enclosed) explaining the filtering system and inviting them to contact the Department for more information. The telephone numbers of officers have been withheld under section 9(2)(g)(ii) of the Act.

Other correspondence with Telecom is being withheld in terms of sections:

- 9(2)(ba)(i) of the Act (to protect information which is subject to an obligation of confidence where the making available of the information would be likely to prejudice the supply of similar information, or information from the same source, and it is in the public interest that such information continue to be supplied);
- 9(2)(j) of the Act (to enable the Department to carry on, without prejudice or disadvantage, negotiation); and
- 9(2)(h) of the Act (to maintain legal professional privilege).

**42) In the March 2011 Independent Reference Group meeting minutes, the following was included:**

***"3. Reporting to ISPs***

***Officials noted that more detailed reports on traffic through the filtering system is being distributed to each ISP. ISPs use this data to assist in the management of their systems, including the operation of their internal filtering systems that they offer customers."***



***And from the October 2010 meeting:***

***"3. Reporting to ISPs***

***Officials noted that the data obtained from the filter can demonstrate patterns of requests for blocked websites that may be of interest to ISPs. This information includes the 50 most blocked sites and the time of day that the filter is most active but cannot identify particular ISPs. The Group agreed that the DIA should draw any such patterns to the attention of ISPs."***

***Could you please send me a copy of any reports that have been sent to ISPs?***

This information has been withheld under section 9(2)(b)(ii) of the Act (would be likely unreasonably to prejudice the commercial position who is the subject of the information).

***43) If not covered by 42), could you please send me a copy of any correspondence with ISPs, written, electronic, or otherwise that draws attention to patterns described above?***

See answer to question 42.

***44) Minutes from the February 2010 Independent Reference Group meeting mention a presentation: "The Group suggested that the Department publish as much information about the system as possible. This would include regular statistics and a copy of the presentation."***

***Could you please send me a link to the presentation this refers to, or, if it's not available, send me a copy of it?***

A search of the Department's records has been unable to locate the presentation referred to above. Attachment 4 is a presentation made to the Netsafe Conference in April 2010 which reproduces the information presented to the IRG in February 2010.

***45) Could a URL be added to the filter list without the approval of three inspectors and without the knowledge of the Independent Reference Group, including by another member of staff not part of the inspector team?***

No.

***46) Could you please describe limitations, if any, that would prevent the above from happening?***

The addition of a URL to the filter list requires three inspectors of publications to agree that the website comes within the scope of the filter system. Once a change to the filter list is agreed, only one officer has the ability to edit the filter list. As the task of reviewing the filter list is shared between members of the Censorship Compliance

Unit it is unlikely that the same three inspectors will be involved in the review of a website.

**47) From the Common Questions and Answers page:**

***"In the long term, if it is made more difficult for persons with a sexual interest in children to access this material, the market will decline and fewer children will be exploited." Could you please send me any statistics or figures held that back this up?***

The Department firmly believes that if the market for child sexual abuse material is reduced, then fewer children will be abused to support that market. The problem is a global one, to which the Department's website filtering system can only make a small contribution. The Department therefore has no statistics or figures to confirm that the filtering system has lead to fewer children being exploited.

**48) *Has the Chief Censor been consulted over decisions relating to the filter? If so, could you please send me anything held regarding those decisions?***

Many of the publications blocked by the filter have been the subject of classification and are therefore on the online database of classified material that is accessible on the Office of Film and Literature Classification website.

**49) *Could you please send me a copy of any contract the DIA has with companies that provide internet services to power the filter, including the web and domain hosts for the <http://dce.net.nz> website?***

DIA has no contracts with providers of internet services that relate to the filtering system.

**50) *If 49) is not possible, could you please send me parts of the contracts regarding collection, privacy, and disclosure of user data collected?***

See answer to question 49.

Where I have decided to refuse your request for information, I have taken into consideration whether reasons, that might otherwise render it desirable in the public interest to make the information available, are outweighed by the need to withhold it. Under section 28(3) of the Act you have the right to apply to the Ombudsman for a review or investigation of this decision.

Yours sincerely



Steve O'Brien  
Manager, Censorship Compliance Unit

**Procedural Information**

Reviewed By:			
Review Details			
Time	12:31	Date	25 Aug 2009

**Review Process**

URL:	http://.		
Captured:	Yes	No	Reason If No:
<b>Overview:</b> Movie site. Girls (babies – adult) being sexually abused, performing sexual acts and posing.			
Decision			
Further Review			
<b>Outcome:</b>			
<b>Actioned:</b>			
Date:		Signed	

RELEASED UNDER THE  
OFFICIAL INFORMATION ACT

Digital Child Exploitation - Filter Review Report

Url	
Inspector 1	<input checked="" type="checkbox"/>
Inspector 2	<input checked="" type="checkbox"/>
Inspector 3	<input checked="" type="checkbox"/>
Review	
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
•	
•	
Comments	

RELEASED UNDER THE  
OFFICIAL INFORMATION ACT

# CCUFIL2319 – Complaint Review

Attachment 2

Page 1

## Procedural Information

Reviewed By:	*****		
Complaint Details			
Time	13:19	Date	17/04/2010
Complaint Details			
Date: 4/17/2011 1:19:01 PM - Importance: Normal			

## Review Information

### General Information

Checked logs for sites blocked between 13:19 and 13:21. Sites in that timeframe identified as \*\*\*\*\*

## Review Process

URL:	*****
Captured:	Yes
Decision	Continue blocking

## Further Review

### Outcome:

### Actioned:

Date: 17/04/2011

Signed: \*\*\*\*\*

RELEASED UNDER THE  
OFFICIAL INFORMATION ACT





Allan FREETH  
<Allan.Freeth@team.telstra  
clear.co.nz>

14/07/2008 01:31 pm

To rbarker@ministers.govt.nz

cc

Subject [Contains Potentially Offensive Language] Filtering Internet  
sites in the interests of New Zealand children

Attachment 3

Dear Minister

TelstraClear has made a change to its Internet services in the interests of New Zealand children and their families.

We will add a filter to all web browsing by Clearnet and Paradise customers that stops browsers from accessing known child sex abuse sites around the world. There are more than 7,000 such sites and the sad fact is that they are accessed, deliberately or otherwise, by thousands of New Zealanders each month.

Anyone using a TelstraClear Internet connection who reaches the web address of a known child sex abuse site will be greeted by a page advising them access has been blocked. We will not monitor or report on what individual customers do, so their privacy is assured.

I am writing this note because we wanted you to know that, as a company with a high proportion of staff with young families, we felt compelled to make this change. While we believe the Internet is a wonderful source of information and that people have the right to determine what they view based on personal taste, there is nothing positive about content that reflects the suffering of children.

Also, as part of our efforts to help parents keep children safe online, we have flown over, Australian cyberbullying expert Dr Martyn Wild. Dr Wild works closely with Telstra to help parents keep their children safe on line, and he will provide customer seminars on the subject in the main cities this week.

Recent UK research showed that children have increased their Internet usage from seven hours a week to 14 hours a week over the past year, with more than half of British parents unsure where to go to find out how to help keep their kids safe on line. Given the growth we have had in broadband customers over the past year, we believe these statistics are relevant to New Zealand.

Finally, I would like to acknowledge the positive role of the Department of Internal Affairs, which manages the list of child sex abuse sites, liaises with international agencies and helps in the real time battle against people who perpetuate this kind of content. It is a good example of how government and business can work together for consumers.

Regards

Allan L Freeth

CEO

TelstraClear

TelstraClear - Best speed, Best price, Best performance, Best loved, Best join.... phone  
Residential 0508 888 800 Business 0508 249 777

This email contains information which may be confidential and subject to copyright. If you are not the intended recipient you must not use, distribute or copy this email or attachments. If you have received this email in error please notify us immediately by return email and delete this email and any attachments.

TelstraClear Limited accepts no responsibility for changes made to this email or to any attachments after transmission from TelstraClear Limited. It is your responsibility to check this email and any attachments for viruses.

Emails are not secure. They can be intercepted, amended, lost or destroyed and may contain viruses. Anyone who communicates with TelstraClear Limited by email is taken to accept these risks.



**Office of Hon Rick Barker**

Minister of Internal Affairs  
Minister of Civil Defence  
Minister for Courts  
Minister of Veterans' Affairs  
Associate Minister of Justice

Allan L Freeth  
CEO  
TelstraClear  
Allan.Freeth@team.telstraclear.co.nz

COMPLETED

Dear Allan

Thank you for your email of 14 July 2008, advising me that TelstraClear has joined the Department of Internal Affairs' (DIA) trial programme for filtering websites containing images of child sexual abuse. I was also interested to hear some of the other things that TelstraClear is doing to ensure the safety of children online.

I appreciate the support that TelstraClear has shown for my department's role in combating the distribution of images of child sexual abuse. Your company's association with the filtering trial from its inception in 2006 and its excellent working relationship with the Censorship Compliance Unit are testament to TelstraClear's commitment to combating this offensive trade. I am sure that your customers also appreciate this commitment.

The filtering trial is still in its early stages and, if successful, DIA will endeavour to expand the programme to other interested ISPs in a planned manner. While participation by ISPs in the filtering programmes will remain on a voluntary basis, I expect that customer demand will mean that most ISPs will join the programme.

The importance of Internet Protocol (IP) address data to DIA investigations has been recently drawn to my attention. The identification of individual computer addresses and the ability to correlate this information with the location of those computers is vital to catch offenders who distribute images of child sexual abuse. I am advised that ISPs consider that, in terms of the Privacy Act 1993, they are required to dispose of information related to IP addresses once this information is no longer necessary for the operation of their businesses. While it is up to each ISP to determine how long they keep this information, I was concerned to learn that some ISPs retain this information for only a very short time. I hope that we can continue to build on the successful partnership between government and business and that TelstraClear will continue to support my Department's investigations by retaining IP address data for a longer period of time.

Yours sincerely

20 AUG 2008

Hon Rick Barker  
MINISTER OF INTERNAL AFFAIRS



**From:** Peter Pilley  
**Sent:** Thursday, 30 October 2008 10:45 a.m.  
**To:** 'RichardB@callplus.co.nz'  
**Cc:** Steve O'Brien  
**Subject:** Re: DIA Digital Child Exploitation - Filtering System

Richard

Thanks for the email

Firstly no we do not peer with APE

The session is created by the setting up of a IPIP tunnelling between the 2 sites then I create a bgp session and you. Peer with it

During the trial we had 0 false positives as we review the list each month to ensure it is corecy and current

The complaints that came in over the 2 years the trial ran for were from users annoyed there collection had been taken away

We had no other complaints during the period however I ensured the each participating ISP had all contact numbers for me and my colleagues and all email addresses with instructions that if there

RELEASED UNDER THE  
OFFICIAL INFORMATION ACT

customers complain to forward them on to us so we can ensure our system

You are correct in saying that 1 IP can host many sites and yes other systems cannot tell the difference between a legit site and a list site however our system can differentiate between these requests and if it is for a site not of interest the request is allowed through

The connection procedure is very simple and takes a matter of minutes after that we can control the process

I hope that helps

Regards

Peter Pilley

**From:** Richard Baalham

**To:** Peter Pilley

**Cc:** Adrian Dick

**Sent:** Thu Oct 30 10:32:20 2008

**Subject:** RE: DIA Digital Child Exploitation - Filtering System

Hi Peter,

I have been tasked to investigate the DCE filtering system with a view to implementation, as such I have a few questions for you (tried to call but I guess you are in meetings):

I see that this solution is effectively overriding BGP routes for the sites that contain (as far as you are concerned) illegal images/content.

1. How do false positives get dealt with i.e. if only a small number of files on a site (under the same IP address/DNS resolution) are considered illegal what happens?
2. I see that 6 users complained, however what number as a proportion of connected users during the trial called in or otherwise contacted to complain either to yourselves or the serving ISP?
3. Do you peer via APE? if not how do we peer to your tunnel/BGP router?
4. I guess that the BGP session will need more than just a peering relationship, what attributes are you setting or require us to set on your behalf?

I will probably ask more questions but these will get us started.

Thanks,

Richard

**From:** Peter.Pilley@dia.govt.nz [mailto:Peter.Pilley@dia.govt.nz]

**Sent:** Tuesday, 21 October 2008 11:32 a.m.

**To:** Graham Walmsley

**Cc:** Steve.O'Brien@dia.govt.nz

**Subject:** DIA Digital Child Exploitation - Filtering System

Graham

This is an email to introduce ourselves and also to tell you about our Digital Child Exploitation - Filtering System initiative.

The Censorship Compliance Unit is a unit dedicated to tracking and identifying users on the internet sharing, promoting, profiting from child sexual abuse material.  
The legislation we enforce is the Films, Videos and Publications classification Act.

We have over the last 2 years built a system for the purposes of restricting access to sites that host child sexual abuse materials such as images, movies, stories etc...  
The system uses a list compiled by the us and translates the list into routes that are advertised to your network via BGP.

If a user attempts to access a site hosted on one of the routes, they are sent to our system where the request is filtered to ascertain if it is known to us.  
if it is known the user is redirected to our landing page <http://www.dce.net.nz>.

If the site is not known to us the request is allowed through.

In the event a user feels the filter was inappropriate they have the ability to make an appeal via the landing page.

This appeal goes directly to my cellphone, blackberry, work email, it is also sent to 2 other Inspectors from the unit. It is also retained on our mail servers for further followup.

The appeal is then processed and a report is compiled detailing the appeal and whether or not the site will continue to remain in the list or be removed.

over the last 2 years we have trialled the system and it was a complete success, this trial came to a close as of 30 September

The ISP's who participated Telstra, IHUG, Maxnet have put their name forward to be included in the enterprise system.

Telecom is coming online very soon.

Over the 3 phases of the trial we were able to identify any potential / probable holes in the system and have come out of the trial with a very robust system.

The system will also be complemented by the Hotline service we are bringing online in the next couple of months to receive and process users reports via the web or an 0800 number.

The complaints system established in Phase 2 has now become an established procedure in terms of response and documentation and to date we have had 6 complaints from users. These complaints related to their annoyance at the site that hosts the abuse material not being able to be accessed.

The scalability tests performed in Phase 3 have enabled us to gauge the size of the system required to service New Zealand's internet users.

Our new system is to be hosted by

To participate in the system is very simple.

1: We setup a tunnel between the 2 sites (IPIP), I let the participating ISP choose the ip's for the tunnel.

EXAMPLE

ip ->

netmask

2: I configure a BGP session and you pair with it our AS is

EXAMPLE

```
router bgp
bgp router-id
neighbor
neighbor
Tunnel
neighbor
neighbor
neighbor ;
```

3: We then confirm the connection and the routes are delivered.

If you have any questions please dont hesitate to contact me.

Peter

Peter Pilley  
Senior Inspector  
Censorship Compliance Unit  
Department of Internal Affairs.  
Peter.Pilley@dia.govt.nz  
PH:  
MOB:  
EX:

**Richard Baalham**

**Networks Design & Build Manager**

Direct: +64 9 929 0200  
Mobile: 021 2838881  
Fax: +64 9 929 0201

This message and any attachments contain privileged and confidential information. If you are not the intended recipient of this message, you are hereby notified that any use, dissemination, distribution or reproduction of this message is prohibited. If you have received this message in error please notify the sender immediately via email and then destroy this message and any attachments.



29 September 2009

Dean Schmidt  
Senior Executive Government Relations  
Telecom New Zealand Ltd  
PO Box 570  
WELLINGTON

46 Waring Taylor St. PO Box 805  
Wellington, New Zealand  
Telephone +64 4 495 7200  
Facsimile +64 4 495 7222  
Website [www.dia.govt.nz](http://www.dia.govt.nz)

Dear Dean

**WEBSITE FILTERING**

I understand that Telecom has now expressed its willingness to participate in the website filtering system to be operated by the Department, as one part of a strategy to help limit New Zealanders' access to images of child sexual abuse. We are delighted that this initiative will have the support of New Zealand's largest telecommunications company.

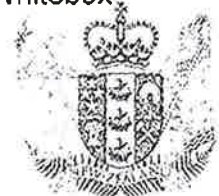
Telecom's cautious approach to date is understandable. However, as you are aware there is a compelling case that any ISP's participation in the website filtering system is lawful.

This case is based on the argument that redirecting a get request to the Whitebox and then to the Department's server is not an *interception*. In addition, even if a get request is a *communication*, and we suggest that it is not, then it is certainly not a *private communication*, because there can be no reasonable expectation of privacy in respect of a request that is analogous to the address on an envelope. Finally, even if a get request is in fact a private communication, there might be an argument that the ISP is a *party* to that communication.

Telecom should feel reassured that making out any one of these four points would be enough to ensure that the prohibition in section 216B of the Crimes Act 1961 is not breached.

If Telecom has any residual concern that redirecting a get request into the website filtering system is an *interception* of a *private communication*, then we suggest that it proactively obtain the express or implied consent of its users, through the use of on-line terms and conditions of use. This would ensure that Telecom is a *party* to the communication, and that the offence provision in section 216B would not apply.

The Department has considered whether to utilise the provision in the Crimes Act to make an Order in Council exempting an interception device from the provisions of Part 9A. The Department does not intend to do so as we consider this unnecessary in light of the points made above. We do not see the Whitebox



software as an *interception device*, and as a result think it would be inappropriate and confusing to seek an Order in Council premised on it being such a device

Finally, I note your concern that regardless of the strength of our view that what is occurring is entirely legal, someone may seek to challenge it. While I accept that the potential for challenge to arise cannot be completely discounted, I suggest that this risk is minor in comparison with the benefits of joining the website filtering system. Should a challenge emerge, to the extent the Department is able to assist to overcome those proceedings, we would do so.

Thank you again for agreeing to participate in the website filtering system. If you do have any further worries, please feel free to discuss them directly with me (ddi: 04 495 9329) or Steve O'Brien (ddi: 04 495 9371).

Yours sincerely

A handwritten signature in black ink, consisting of a stylized 'K' and 'M' with a horizontal line extending to the right.

Keith Manch  
Deputy Secretary, Regulation and Compliance

cc: Grant Fraser, Senior Solicitor, Telecom NZ Ltd

RELEASED UNDER THE  
OFFICIAL INFORMATION ACT

**To:** Craig Armitage; Steve O'Brien; Lloyd Bezett; Peter Pilley  
**Cc:**  
**Date/time Received:** 1/11/2010 12:07:53 p.m.  
**Subject:** FW: DIA / Telecom announcement

Attached is the final version of Telecom's planned announcement on Wednesday of signing up to the DCEF for check. It contains our additions/changes of a week or so ago. Let me know if you have any concerns and I'll respond. Thanks

Trevor Henry  
Senior Communications Adviser  
Regulation and Compliance  
The Department of Internal Affairs  
Direct Dial: +64 4 495 7211  
Mobile: +64 275 843 679  
[www.dia.govt.nz](http://www.dia.govt.nz)

**From:** Emma-Kate Greer [mailto:Emma-Kate.Greer@telecom.co.nz]  
**Sent:** Monday, 1 November 2010 11:41 a.m.  
**To:** Trevor Henry  
**Cc:** Anna Skerten  
**Subject:** DIA / Telecom announcement

Hi Trevor

Sorry about the delay in sending our announcement regarding the filter – is Wednesday ok from your perspective?

Attached is the statement based on your changes. We will need to run a final check past our lawyers here but I will let you know if anything changes – likewise let me know if there are any concerns at your end.

Also, would you like your contact details on the attached?

Thanks,

Emma-Kate

**Emma-Kate Greer**  
Corporate Communications Manager - Retail

**T** 09 358 5804 (extn 93204)  
**M** 027 655 4499  
**E** [emma-kate.greer@telecom.co.nz](mailto:emma-kate.greer@telecom.co.nz)

Level 1, The Plaza, 2 Hereford Street  
Auckland  
[www.telecom.co.nz](http://www.telecom.co.nz)

We're **BackingBlack**, are you?

This communication, including any attachments, is confidential. If you are not the intended recipient, you should not read it - please contact me immediately, destroy it, and do not copy or use any part of this communication or disclose anything about it. Thank you. Please note that this communication does not designate an information system for the purposes of the Electronic Transactions Act 2002.

Converted Attachments

Attachment image001.jpg converted to managed file image001.jpg)

Attachment DIA Media Release 21102010 Updated DRAFT.DOC converted to managed file DIA Media Release 2 DRAFT.DOC)

RELEASED UNDER THE  
OFFICIAL INFORMATION ACT



## **DRAFT media release**

[Date]

### **Telecom supports Internet filtering system**

Telecom has today announced it will join the Department of Internal Affairs' Digital Child Exploitation Filtering System. The system filters the web content of participating Internet Service Providers (ISPs) to block access to known websites that contain child sexual abuse material.

Telecom Retail CEO, Alan Gourdie says Telecom is committed to assisting the Department of Internal Affairs in this step towards addressing this serious issue.

"The abuse and exploitation of children is intolerable and this filter works to block access to the worst-of-the-worst child exploitation websites."

The Acting Deputy Secretary of Internal Affairs, Craig Armitage, welcomed Telecom's decision to sign up to the filtering system.

"We are working in partnership with New Zealand ISPs. This filter provides a service provider with the means to protect their customers from inadvertently accessing these illegal websites and to fight and raise awareness of the worldwide problem of child sexual abuse and exploitation. The filter is an important tool to reduce the demand for child abuse material currently available on the Internet. Telecom and other ISPs signing up are to be commended for taking this step."

Mr Gourdie says while participating ISPs are signing up to combat child abuse, people should remain vigilant when taking steps to keep their families safe online.

"This filter does not negate the need for continued supervision and monitoring of Internet use to keep kids safe online. We encourage Kiwis to keep their Internet security up to date – Telecom's McAfee Security Suite includes parental controls and is free for all our customers with compatible operating systems.

"Parents can also find more information about online safety at [netsafe.org.nz](http://netsafe.org.nz) and [hectorsworld.com](http://hectorsworld.com)."

The Digital Child Exploitation Filtering System was made available to ISPs in March 2010 following a two-year trial, and is overseen by an Independent Reference Group, of which Telecom is a member.

For more information on the Digital Child Exploitation Filtering System please visit  
[http://www.dia.govt.nz/diawebsite.nsf/wpg\\_URL/Services-Censorship-Compliance-Digital-Child-Exploitation-Filtering-System?OpenDocument](http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Censorship-Compliance-Digital-Child-Exploitation-Filtering-System?OpenDocument)

Ends

For more information please contact:

Emma-Kate Greer  
Corporate Communications Manager – Retail  
027 655 44 99  
[emma-kate.greer@telecom.co.nz](mailto:emma-kate.greer@telecom.co.nz)

Trevor Henry  
Senior Communications Adviser  
Regulation and Compliance  
The Department of Internal Affairs  
04 495 7211  
0275 843 679

RELEASED UNDER THE  
OFFICIAL INFORMATION ACT

16 March 2010

Dear

### **Digital Child Exploitation Filtering System**

I am writing to advise you of the availability of the Digital Child Exploitation Filtering System (DCEFS).

The DCEFS is a website filtering initiative that has been developed by the Department of Internal Affairs and is being offered to all Internet Service Providers (ISPs). Connection to the system is voluntary and ISPs may disconnect at any time.

A great deal of traffic goes to websites containing images of child sexual abuse. The DCEFS is designed to assist in combating the trade in child sexual abuse material by making it more difficult for persons with a sexual interest in children to access that material. By reducing the market for such images, the DCEFS will help ensure that fewer children are abused in support of that market.

### **Context for the DCEFS**

In New Zealand, the DCEFS will complement other enforcement activity undertaken by the Department. This activity includes the provision of information to assist in preventing and deterring censorship offences, online investigations into the possession and trading of child sexual abuse material on peer-to-peer networks and the prosecution of offenders.

The purpose of the DCEFS, as part of the Department's approach, is to assist in preventing access to child sexual abuse material. It does not have an enforcement focus. . The DCEFS will therefore contribute to the international effort to combat the trade in child sexual abuse images and raise the public's awareness of this type of offending and the harm caused to victims.

## Ensuring Confidence in the DCEFS

The Department recognises that, to ensure public confidence in the DCEFS, the scope of the system must remain on child sexual abuse material and its operation must be open to scrutiny. Accordingly, the Department's contract for the use of the software that supports the DCEFS constrains its use to filtering to child sexual abuse material and a Code of Practice has been put in place to govern the operation of the system. Additionally, an Independent Reference Group (IRG) will ensure the system is operated in compliance with the Code. Information on the Code of Practice and the IRG can be found on the Department's website at [www.dia.govt.nz](http://www.dia.govt.nz).

## Basic details of the DCEFS

The DCEFS was designed by Netclean Technologies Sweden AB and filters users' requests via a secure connection between an ISP and the Department, using a master list of known objectionable sites that will be maintained by the Department. ISPs will not be provided with the list of website URLs on the filtering list.

Once a requester seeks an IP address that is on the filtering list they will be directed to the Department's system where the particular URL requested is checked against the filtering list. If there is not a match, the request allowed on its way to the world-wide web. If there is a match between the requested URL and the filtering list the requester is redirected to a landing page that:

- informs the requester that he/she has been prevented from accessing the requested website,
- informs the requester of the reason for the redirect, and
- provides the requester with a method to appeal the action.

The method of filtering and the location of the filter on the network have been chosen so that there is no degradation to the performance of the Internet. Significant steps have been taken to ensure the technical integrity of the filter. The Department is able to discuss and demonstrate all the technical features of the system with ISPs as part of their consideration of the use of the DCEFS.

If you wish to discuss the possibility of connecting to the DCEFS, please contact me on [redacted], or if you wish to discuss technical matters call Peter Pilley on [redacted]

Yours sincerely



Steve O'Brien  
National Manager  
Censorship Compliance Unit



Actrix  
ASC Data  
Airstream Networks  
Airnet NZ  
BorderNET  
BorgWiFi  
Compass Communications  
Plain Communications  
Cybermedia New Zealand  
Enternet Online  
Evolution Wireless Consultants  
Teldave Communications  
Farmside  
Freenet  
GetRheel  
Go2 Internet  
AGRE Enterprises  
Helix Wireless Ltd  
Internet Hawke's Bay  
ICONZ  
Inspire Net  
KC Internet  
Kinect  
Kiwi Online  
KTSA Internet  
NATCOM  
Netsmart  
Netspeed Data  
NZNET Internet Services  
NZWireless  
Orcon Internet  
Planet Internet  
PrimoWireless  
Slingshot  
Snap Internet  
TelstraClear  
thepacificnet  
The Packing Shed  
thinair Communications  
Uber Networks  
Vodafone New Zealand  
Web World  
WirelessWeb  
WIZwireless  
Woosh  
WorldNet Services  
Xnet  
Xtreme Networks

RELEASED UNDER THE  
OFFICIAL INFORMATION ACT