Digital Child Exploitation Filtering System

Code of Practice

A code for the operation of the Department of Internal Affairs' website filtering system to prevent access to websites containing images of child sexual abuse

JANUARY 2010

EXPLANATORY STATEMENT

The expansion of the Internet has led to many positive developments. However, the fact remains that criminals, individuals as well as organised groups, are also using this technology as a means of producing, collecting and distributing images of child sexual abuse.

Child sexual abuse images are not "just images" but evidence of actual criminal activity. The possession and distribution of this material creates an international market that supports and encourages further abuse. The children who are victims of this activity sometimes suffer the psychological effects of their abuse for many years after the physical offending has ended. Images that are distributed on the Internet never go away. With each download the person involved is re-victimised.

The Digital Child Exploitation Filtering System is designed to assist in combating the trade in child sexual abuse images by making it more difficult for persons with a sexual interest in children to access that material. The Filtering System will complement the enforcement activity undertaken by the Censorship Compliance Unit of the Department of Internal Affairs. This activity includes online investigations into the trading of objectionable images on peer to peer networks and the prosecution of offenders.

Website filtering is only partially effective in combating the trade in child sexual abuse images. In particular website filtering is effective only after the fact and does not prevent the creation of illegal material nor, in the case of images of child sexual abuse, the exploitation of children. The system also will not remove illegal content from its location on the Internet, nor prosecute the creators or intentional consumers of this material.

The focus of international enforcement will continue to be the identification and rescue of victims, and ensuring that these websites are quickly shutdown and their owners prosecuted. However, not every legal system recognises the distribution of child abuse images as a serious crime, and few enforcement agencies around the world have the resources and training to carry out online investigations and the forensic examination of computers.

Current Legislation

The Films, Videos, and Publications Classification Act 1993 (the FVPC Act) deems a publication to be objectionable if it promotes or supports, or tends to promote or support the exploitation of children, or young persons, or both, for sexual purposes (section 3(2)(a)).

The FVPC Act provides that possession of an objectionable publication with knowledge or reason to believe it is objectionable is a serious offence carrying a term of imprisonment not exceeding 5 years or a fine not exceeding $50,000.

The offence of distributing an objectionable publication, including over the Internet, with knowledge that the publication is objectionable carries a maximum term of imprisonment of up to 10 years. Distributing includes

making a publication available for others to access, such as on a website or through file sharing.

New Zealand law contains no provision that specifically authorises the operation of a website filtering system or to require Internet Service Providers (ISPs) to connect to such a system. Participation in the Digital Child Exploitation Filtering System by ISPs is therefore voluntary.

CONTENTS

Digital Child Exploitation Filtering System

Code of Practice

1. Purpose

1.1 The Digital Child Exploitation Filtering System (DCEFS) will contribute to the international effort to combat the trade in child sexual abuse images. Reducing the market for such images will help ensure that fewer children are abused in support of that market.

1.2 The DCEFS will help reduce the number of New Zealanders who possess, distribute and make child sexual abuse images.

1.3 While the risk of inadvertent exposure to child sexual abuse images is low, the DCEFS will contribute to promoting a safer online environment for the New Zealand public.

2. Scope

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 (FVPC Act, section 3(2)(a)).

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

2.3 The DCEFS will not prevent access to any website or impair any Internet traffic that is not clearly within the scope as defined in paragraph 2.1.

2.4 The DCEFS is a preventative measure and not an enforcement tool.

3. Independent Reference Group

3.1 The Department shall establish an Independent Reference Group (IRG), the membership of which shall be representative of:

- enforcement agencies
- the Office of Film and Literature Classification (OFLC)
- Internet Service Providers (ISPs)
- Internet users
- agencies and community groups with an interest in the welfare of children.

3.2 The general function of the IRG is to maintain oversight of the operation of the Digital Child Exploitation Filtering System to ensure it is operated with integrity and adheres to the principles set down in this Code of Practice.

3.3 Meeting of the IRG will be held quarterly.

3.4 The IRG shall appoint a presiding member and determine its own meeting procedures.

3.5 Members of the IRG shall meet their own costs for attendance at meetings of the Group.

3.6 The following information shall be made available to members of the IRG:

- inspectors' reports referred to in paragraph 4.4,
- details of all appeal applications and the resulting action taken,
- reports of any technical issues with the filter or connections to any ISP,
- such other information that may lawfully be provided to assist the IRG in fulfilling its function.

3.7 The IRG shall produce an annual report on the operation of the DCEFS. Reports of the IRG shall be published on the Department's website.

4. The Filtering List

4.1 The Censorship Compliance Unit in the Department of Internal Affairs has developed a large database of sites (the filtering list) offering child sexual abuse material. The filtering list is compiled from the following sources:

- intelligence obtained through partnerships with national and overseas enforcement agencies that work on combating the trade in child sexual abuse material;
- the Department's forensic examination of computers seized during the investigation and prosecution of offences in this country;
- an online reporting facility for child sexual abuse images called *Child Alert* that has been launched by End Child Prostitution, Child Pornography and Trafficking in Children (ECPAT NZ); and
- reports of illegal content made directly to the Department by members of the public.

4.2 Where clarification is needed as to whether a website contains images of child sexual abuse, the images in question shall be submitted to the Office of Film and Literature Classification for a classification.

4.3 The list will be reviewed monthly, to ensure that it is up to date and that the possibility of false positives is removed. Inspectors of Publications will examine each site to ensure that it continues to meet the criteria for inclusion on the filtering list.

4.4 Inspectors will prepare and maintain a report in respect of each website that is on the filtering list that provides:

- the site address by URL;
- the date that the site was reviewed and the reviewing inspector;
- what an inspector observed on the site each time it is reviewed; and
- a recommendation for whether the site stays on the filtering list or is removed.

4.5 Additions will only be made to the filtering list with the agreement of 3 inspectors that the publication on the website meets the criterion of containing images that promote or support, or tend to promote or support, the exploitation of children, or young persons, or both, for sexual purposes.

4.6 The removal of websites from the filtering list will be reported regularly to the Manager, Censorship Compliance Unit.

4.7 All additions and deletions to the filtering list will be reported to the next meeting of the IRG.

5. Appeal process

5.1 When a person requests a webpage that is on the filtering list, they shall be presented with a landing page.

5.2 The landing page is designed to achieve the following objectives:

- inform the requester that he/she has been prevented from accessing the requested website and why
- provide the requester with a method to appeal the action.
- provide the requester with a link to the Department of Internal Affairs website, where additional information about the operation of the censorship system and help seeking information can be found.

5.3 A person who considers that they have been wrongly blocked from visiting a legitimate website may appeal the inclusion of the blocked webpage on the filtering list.

5.4 The process for the submission of an appeal shall:

- be expressed and presented in clear and conspicuous manner;
- ensure the privacy of the requester is maintained by allowing an appeal to be lodged anonymously.

5.5 Each appeal will be considered by an inspector, who shall re-examine the website concerned to determine whether it still meets the criterion for inclusion on the filtering list.

5.6 Where the information supplied by an appellant is inadequate, a reasonable effort shall be made to correctly identify the website.

5.7 Each appeal and the resulting action shall be entered in an appropriate report.

5.8 The appeals submitted and the actions taken will be reported to the next meeting of the IRG.

6. Data

6.1 During the course of the filtering process the filtering system will log data related to the website requested, the identity of the ISP that the request was directed from, and the requester's IP address.

6.2 The system will anonymise the IP address of each person requesting a website on the filtering list and no information enabling the identification of an individual will be stored.

6.3 The collection of data is necessary so that the system is able to be reviewed to ensure 24-hour, 365-day uptime, and no loss of business due to a technical glitch or fault, for ISPs who join the system.

6.4 The logs will be used to troubleshoot the connections between the Department's system and the ISP.

6.5 Data shall not be used in support of any investigation or enforcement activity undertaken by the Department.

6.6 Data may be used for statistical and reporting purposes; for example to inform the Department of the level of demand in New Zealand for child sexual abuse images.

6.7 The logs will be kept for 30 days, which is the standard period for keeping logs for troubleshooting and is period consistent with Rule 9 of the Telecommunications Information Privacy Code 2003. At the end of this period the logs are then manually deleted and a record is made noting this.

7. Code Development and Review

7.1 The Department, in conjunction with the IRG, shall review the Code after 12 months operation.

7.2 The IRG may institute a review or amendment to the full Code or parts of the Code at any time.