

NEW ZEALAND CENSORSHIP COMPLIANCE UNIT

Mr Paul Duke
Department of Internal Affairs, New Zealand

*Paper presented at the conference: Internet Crime
held in Melbourne, 16-17 February 1998, by the Australian Institute of Criminology*

Three areas will be covered in this paper, they are:

1. The role of the New Zealand Department of Internal Affairs;
2. Types of Internet cases we investigate; and
3. Initiatives we have taken to increase awareness and be effective in the field.

The Role of the Department

The Censorship Compliance Unit of the Department of Internal Affairs was established on 1 July 1996.

The Unit is nation-wide, with six Inspectors operating throughout New Zealand. The majority of staff have an enforcement background, either NZ Police or Customs.

We have the mandate to enforce the Films, Videos and Publications Classification Act 1993. This legislation replaced the Indecent Publications Act 1963, the Films Act 1983, and the Video Recordings Act 1987.

This Act provides the power to obtain and execute search warrants in relation to offences involving objectionable publications. Objectionable publications are deemed to be (broadly speaking) those which deal with matters of sex, horror, crime, cruelty, or violence, in such a manner as to be injurious to the public good. The full definition of 'objectionable' may be found in Section 3 of the Act.

The Act also specifies the penalties involving objectionable publications. The most severe is found in Section 124. A person convicted under this section could face a fine of up to \$20,000 or imprisonment for a term not exceeding one year.

To gain a successful conviction under this Section, the prosecution must prove the defendant knew or had reasonable cause to believe the publication was objectionable.

There would be very few people in New Zealand who could argue that the images we encounter are not objectionable, or that they did not think they were wrong to be in possession of them.

While dealing with all forms of objectionable publications, be it films, videos, magazines or any form of printed material, our focus has been the apprehension of traders of child pornography on the Internet.

We have completed over 110 investigations into child pornography on the Internet.

Of the 41 prosecution cases we have prepared since our inception, 27 relate to child pornography on the Internet. We have now had six Internet cases before the Courts, gaining convictions in all of them.

Types of Cases:

Internet contains The WorldWide Web (www), Newsgroups, and Internet relay chat (IRC). Any of these areas of Internet may contain objectionable material and indeed all of them do. Our focus to date has been on IRC and we spend a fair amount of time monitoring Internet relay chat sessions.

IRC is where you can communicate computer to computer. It is an open forum which operates in real time.

This means the words that are typed will appear on the recipient's computer screen almost immediately, and the reply will appear in the same way. This communication can be made with a group of people, or with an individual, conversing through a channel on a common subject.

The channels are named relative to the subject under discussion. At any one time there are about 15,000 - 20,000 people using the undernet of Internet IRC world wide. There are thousands of different channels, a number of which are devoted to the trading of objectionable material.

Some of the channels we frequent covertly will have names such as:

- * "PRETEEN SEX PICS"
- * "FAMILYSEX PICS"
- * "DOG SEX"
- * "GAYDADS4SONS PICS"
- * "YOUNG GIRL RAPE SEX"

I'm not sure why these particular channels should be deemed to be chat channels because very little conversation goes on. People are usually too busy trading pictures : children engaged in sexual acts with other children, and/or with adults; acts of bestiality; images depicting extreme violence - whatever the subject matter of the 'chat' channel in question.

The three common formats traded are still image files (usually in .jpg or .gif format); text files containing short stories (usually in .txt format); and video clip files (usually in .avi or .mpg format) which are short movies about 20 seconds long.

One notorious .avi is entitled "SLAMING A 6 YR OLD" and shows an adult male engaged in sexual intercourse with a six year old girl. Still images captured from this video have also been noted in IRC channels.

By actively monitoring these chat channels and using basic computer commands, we can establish who particular New Zealanders are in the objectionable areas.

The trick is in being able to talk to them in computer 'chat' lingo and gain their confidence so they feel at ease in trading with you.

Once we have evidence that a person has traded in objectionable material, we identify them through their electronic address, and a search warrant is obtained and executed on their Internet Service Provider to identify the name of the user and physical address of the computer. From those details, a search warrant is executed on the suspect's address.

At this time, we have no "offender profile" for Internet offenders except that so far they have all been male and, to varying degrees, most suffer in relation to their ability to socially communicate. We have offenders from 14 years to 70 years, with wide ranging employment such as truck drivers, computer sales people, company directors, teachers, sickness beneficiaries and students. They have not all been 'computer geeks' and indeed some have had relatively basic computer knowledge.

Our major traders in objectionable material will have literally thousands of pictures on their computers. The biggest collection to date has been about 30,000 pictures.

We have found these people want to talk, to tell how clever they are with their computer, what their collection consists of, and often what they have done physically.

Often this is bravado, but from what some offenders have told us, we have gained valuable supporting evidence that has led to their later conviction, e.g. one computer user bragged to us how and where he met underage girls outside school grounds, where he took them and what he did.

We liaise closely with the NZ Police, and where any danger or suspicion of physical abuse is encountered, they are involved.

Some activities come to our attention due to the offender's actions on the Internet first. We have begun inquiries because of the trading of objectionable pictures but, on execution of search warrants found one offender to have been videoing up the skirts of schoolgirls from a miniature camera concealed in his shoe.

Another such case showed the offender to have convinced his girlfriend to set up covert video cameras in numerous girls changing rooms at swimming pool complexes.

On examining the contents of one known paedophile's computer, we found that he was taking on the identity of a young girl and would attempt to make contact with local children, we believe to arrange face to face meetings at the local bus stop.

One investigation was co-ordinated between two offices in that we were communicating with a Christchurch offender via our Wellington computer at the same time myself and Police executed a search warrant on his address. He was still attempting to trade objectionable material with our staff in Wellington as I went through the front door.

Evidence was gained through examination of his computer to suggest he was involved sexually with two boys, both under 13 years of age.

Our investigations have also shown us that New Zealand paedophile networks are utilising the Internet.

A disturbing aspect of our investigations is the number of children involved in trading hard core pornography. We have picked up about 26 individuals between the ages of 14 and 17 years. Some of these children were just curious, but it is a big step from down-loading or viewing pornographic pictures, to actually trading in hard-core child pornography.

Initiatives we have taken to increase awareness and be effective in the field:

We have taken steps to heighten awareness of the Act and what we do, through the production of Information brochures - these have been delivered to the majority of publication outlets in New Zealand and have been sent to every police station.

We have produced a leaflet as a guide to Internet on-line safety. This leaflet includes guidelines for both parents and children on some of the dangers of the Internet and outlining some common-sense solutions.

We have completed about 10 investigations on overseas offenders, preparing files which are forwarded via Interpol to the country concerned. To date these have included Japan, USA, England, Sweden, Holland, Colombia, Belgium, Australia and Indonesia.

Staff have received relevant computer training in the United States. One of the greatest benefits of this training has been making contact with people from various agencies involved in similar work. Indeed it is our hope to make such contacts with as many of you as we are able during this conference.