Parliamentary Joint Committee on the Australian Crime Commission

Inquiry Into Cybercrime

Submission No:15
Received 13 May 2003
Ms Sharon Trotter
Manger Content Assessment
Australian Broadcasting Authority
PO Box Q500
Queen Victoria Building
SYDNEY NSW 1230
☎02 9334 7865 02 9334 7799
E-mail: Sharon.Trotter@aba.gov.au

Office of
Professor David Flint
Chairman

22 May, 2003

The Secretary
Parliamentary Joint Committee on the Australian Crime Commission
Suite S1 107
Parliament House
Canberra ACT 2600

Dear Secretary

ABA SUBMISSION TO CYBERCRIME INQUIRY

I attach for your consideration the Australian Broadcasting Authority's submission to the Parliamentary Joint Committee on the Australian Crime Commission's cybercrime inquiry. The submission was approved by the ABA on 9 May 2003.

Please contact Ms Sharon Trotter, Manager Content Assessment, if you have any queries regarding the content of the submission.

Yours sincerely

Professor David Flint

Australian
Broadcasting
Authority

Parliamentary Joint Committee on the Australian Crime Commission – Cybercrime Inquiry

Submission by the Australian Broadcasting Authority

Australian Broadcasting Authority
Sydney
May 2003

Published by the Australian Broadcasting Authority
201 Sussex Street
Sydney NSW 2000

Contents

Introduction and overview

On 2 April 2003, the Parliamentary Joint Committee on the Australian Crime Commission announced that it would undertake an inquiry on recent trends in practices and methods of cybercrime with particular reference to:

1. child pornography and associated paedophile activity;
2. banking, including credit card fraud and money laundering; and
3. threats to national critical infrastructure[1].

The Australian Broadcasting Authority (ABA) administers the co-regulatory scheme for Internet content, which is established under Schedule 5 to the *Broadcasting Services Act 1992*. The scheme commenced operation on 1 January 2000 and aims to respond to community concerns about illegal and offensive Internet content, including child pornography and other paedophile related material. It includes a complaint handling mechanism for dealing with problematic content, codes of practice that set out the obligations of Internet service providers (ISPs) and Internet content hosts (ICHs) in relation to Internet safety matters, and measures to promote community awareness of Internet safety issues. The Department of Communications, Information Technology and the Arts is currently undertaking a review of the scheme[2]. The Act requires the Minister for Communications, Information Technology and the Arts to table in Parliament a report of the review within 15 parliamentary sittings days of it being completed.

This submission provides information on the ABA's activities in implementing the scheme and other information to assist the committee's consideration of issues associated with Internet child pornography and paedophile activity. As the other matters to be considered by the committee are outside the scope of the ABA's functions in relation to Internet content, the ABA does not propose to provide a submission on these issues.

The submission provides an overview of the co-regulatory scheme administered by the ABA and the ABA's functions under the scheme, sets out action taken by the ABA's complaint hotline in relation to reports of Internet child pornography and paedophile material, outlines work being undertaken by the ABA in co-operation with counterpart bodies overseas, and flags the potential risks associated with the introduction of portable convergent devices.

Unless otherwise stated, references to clauses are references to clauses of Schedule 5 to the *Broadcasting Services Act 1992*.

[1] See http://www.aph.gov.au/Senate/committee/acc_ctte/cybercrime/tor.pdf

[2] Information about the review, including submissions lodged by interested parties, is available on the DCITA web site at http://www.dcita.gov.au/Article/0,,0_1-2_10-3_481-4_111736,00.html.

Overview of co-regulatory scheme

The Internet and new digital technologies have many benefits and advantages and the overwhelming view of Australians is that the impact of these technologies has been a positive one[1]. However, these technologies have also created new opportunities for persons with sexual interest in children to produce, distribute and collect child pornography and engage in other types of paedophile activity. Such usage of the Internet has been the subject of considerable research and debate[2] and has been a focus of concern for policy makers, the Internet industry and child welfare bodies.

The co-regulatory scheme for Internet content established under Schedule 5 of the *Broadcasting Services Act 1992* aims to address community concerns about illegal and offensive Internet. The scheme commenced operation on 1 January 2000, and establishes a framework within which government, industry and the community share responsibility for Internet content matters. This section of the ABA's submission provides an overview of the scheme and the ABA's role in administering it, with an emphasis on those aspects of the scheme that have particular relevance to Internet child pornography and paedophile activity.

Scope

Internet content

The Act defines Internet content as information that is kept on a data storage device and accessed or available for access using an Internet carriage service (clause 3). Ordinary email, chat, 'real time' services and information transmitted in the form of a broadcasting service are expressly excluded from the definition. In interpreting the definition of Internet content, the ABA has had regard to the Explanatory Memorandum for the Broadcasting Services Amendment (Online Services) Bill 1999, which states that:

> Examples of Internet content include pages on the world wide web, email threads, material available for general access for Usenet newsgroups and information available from databases (page 16).

Prohibited content

Clause 10 of Schedule 5 of the Act defines prohibited content as content that has been classified RC or X by the Classification Board and, in the case of content that is hosted in Australia, content that has been classified R and is not subject to a restricted access system.

[1] Australian Broadcasting Authority (2001), *The Internet at home: a report on Internet use in the home,* ABA, Sydney.
[2] See for example Taylor, M. (2000), *The Nature and Dimensions of Child Pornography on the Internet* at http://www.stop-childpornog.at/pa_taylor.html.

The definition of prohibited content is underpinned by the National Classification Code and the Classification Board's Guidelines for Classification of Films and Computer Games[3]. The guidelines set out the types of material covered by each of the classifications. They state that child pornography and material that promotes or provides instruction in paedophile activity will be classified RC. Such material is therefore prohibited under Schedule 5 of the Act.

Material that has not been classified but which if classified would be prohibited content is regarded as potential prohibited content, and is dealt with in a similar way to prohibited content.

Elements of the scheme

The co-regulatory scheme is comprised of a range of regulatory and non-regulatory measures.

Complaints hotline

The Act establishes a mechanism for dealing with complaints about illegal and offensive Internet content. Members of the public can complain to the ABA about Internet content that they believe is or may be prohibited. The ABA investigates all valid complaints, and takes action in relation to prohibited and potential prohibited content. Action taken by the ABA is determined according to where the content is hosted. If the content is hosted in Australia and is prohibited, or is likely to be prohibited, the ABA will direct the ICH to remove the content from their service[4]. If the content is not hosted in Australia and is prohibited, or is likely to be prohibited, the ABA will notify the content to the suppliers of scheduled filters in accordance with the registered Internet Industry Association (IIA) code of practice (see below).

The Act requires the ABA to refer 'sufficiently serious' Internet content to a member of an Australian police force or, by agreement with an Australian police force, to another competent body. In all cases the ABA has discretion to defer taking action in relation to such content to avoid prejudicing a criminal investigation. The ABA has received one such request to defer action during the period of the scheme's operation.

On the basis that child pornography and other paedophile-related material is illegal in Australian States and Territories, and in many international jurisdictions, content of this nature is regarded as sufficiently serious' for the purposes of the Act. The procedures followed by the ABA in relation to such content are set out in service agreements and memoranda of understanding between the ABA and State and Federal police forces.

Sufficiently serious content hosted outside Australia is notified to the Australian Federal Police. Alternatively, as an associate member of Internet Hotline Providers in Europe Association (INHOPE) the ABA notifies the material to an INHOPE hotline if

[3] The code and guidelines can be found on the web site of the Office of Film and Literature Classification at http://www.oflc.gov.au/resource.html?resource=62&filename=62.pdf.

[4] Where content has not been classified, the ABA issues an interim take-down notice to the ICH and asks the OFLC to classify the content. When the content has been classified, the ABA advises the ICH of the classification and, if necessary, issues a final take-down notice to the ICH.

one operates in the country concerned. Such hotlines have close working relationships with law enforcement agencies in their respective jurisdictions. The ABA has agreed with the AFP that where such a hotline exists, the ABA will refer material to that hotline, and this arrangement is reflected in the ABA-AFP service agreement. The ABA has also agreed with the AFP that it will refer the details of an individual content host only once in any twelve months period.

Sufficiently serious content that is hosted in Australia is notified to the police force in the State or Territory in which the host appears to be located.

Further information about such referrals is provided below

Codes of practice for the Internet industry

The Act encourages the development by industry of codes of practice that set out the obligations of ISPs and ICHs in relation to a range of Internet content and safety matters. The Internet industry, through the IIA, has developed three codes of practice that address the matters set out in clause 60. Content Codes 1 and 2 cover the activities of ISPs while Content Code 3 deals with the responsibilities of ICHs[5]. While the codes were developed by the IIA, whose ISP and ICH members account for the majority of Australian Internet users, the codes apply to all participants in these sections of the Internet industry.

Included in Content Code 2 is a 'designated notification scheme' that provides a mechanism for dealing with prohibited and potential prohibited content hosted outside Australia, that has been the subject of a complaint. Under the procedures set out in the code, ISPs are required to provide end-users with one of the filter products or services that are listed in the Schedule to the code (unless satisfied that a user has made alternative arrangements that are effective in preventing access to such content). The ABA notifies the details of prohibited and potential prohibited content to the maker or distributor of each of the scheduled filters. The makers or distributors of these scheduled filters have undertaken to update the products to give effect to notifications received from the ABA, thereby preventing users of the products from accessing the content.

Community education

Recognising that the nature of the Internet limits the scope for traditional regulatory responses, the scheme includes non-regulatory measures such as community education. As the rate of Internet take-up by Australian families continues to grow, the ABA is concerned to ensure that families are aware of how to manage the potential risks associated with some areas of the Internet.

The ABA's role in promoting community awareness of Internet safety issues commenced prior to the introduction of the co-regulatory scheme. With the commencement of the scheme on 1 January 2000, the ABA assumed a statutory role to advise and assist parents and responsible adults in relation to the supervision and control of children's access to the Internet, and to conduct community education

[5] The current codes are available on the Internet Industry Association's web site at http://www.iia.net.au/contentcode.html or on the ABA's web site at http://www.aba.gov.au/internet/.

programs, in consultation with relevant industry, community and government bodies (clause 94).

Detailed information about the activities undertaken by the ABA in this area can be found in the ABA's submission to the Ministerial review of the operation of the co-regulatory scheme[6].

Chat

Because their content is not stored, chat services are outside the scope of the ABA's complaint handling mechanism and the ABA does not investigate complaints about content or behaviour encountered in chat rooms.

Nonetheless, the ABA's research has shown that chat and messaging applications are particularly popular with young people. Indeed, such applications provide young people with excellent opportunities to make friends and develop important social and communication skills, and they are an enjoyable way for young people to enhance their computer and Internet skills. However, the ABA is aware that chat rooms are often used by adults with a sexual interest in children to make contact with them, usually with a view to establishing an online relationship with them, prior to arranging a face-to-face meeting. In the ABA's view, non-regulatory measures such as education and awareness-raising play an important role in addressing the risks associated with children's use Internet chat services[7].

Chat safety information is included on the ABA's Cybersmartkids web site, www.cybersmartkids.com.au, launched on 18 December 2001 and is also available in brochure form. The ABA actively promotes these resources through schools, libraries and community organisations. The ABA is also working with Childnet International, a United Kingdom-based charity concerned with ensuring children are able to use the Internet safely, in bringing to Australia the innovative activity 'Net Detectives' in which groups of children learn about Internet safety issues while using the Internet to solve a 'who done it' mystery. The ABA is working with State and Territory departments of education and some non-government school bodies to conduct two pilot activities in Australian schools later in 2003. It is hoped that further activities will be run in 2004.

[6] Available on the DCITA web site at http://www.dcita.gov.au/Article/0,,0_1-2_10-3_481-4_111736,00.html.

[7] The ABA notes that regulatory measures to address online 'grooming' of children have been adopted in a number of overseas jurisdictions, and understands that similar initiatives are being considered in Australia and State and Federal levels.

Operation of complaint mechanism

This section of the ABA's submission provides information on the operation of the complaint mechanism established by the scheme and administered by the ABA, including liaison between the ABA and law enforcement agencies in relation to illegal content.

Establishment of complaint hotline

The complaint mechanism established by the Act gives the ABA the power to investigate complaints, and initiate its own investigations, in relation to Internet content that is, or may be, prohibited. As noted above, prohibited content includes child pornography and other paedophile-related material.

The Act requires that complaints about Internet content be made to the ABA in writing, or by way of a specified kind of electronic transmission (clause 24). To facilitate easy lodgement and prompt investigation of complaints, the ABA established an 'online hotline' that enables complaints to be lodged electronically using an online complaint form on the ABA's web site (http://www.aba.gov.au/hotline/). All complainants are advised of the outcome of their complaints.

In establishing and operating the hotline, the ABA has been guided by internationally recognised principles. In particular, the ABA has been concerned to ensure the security and confidentiality of all material investigated, and related information such as URLs, web site names and page titles, consistent with international practice in this area.

Complaints investigated 1 January 2000 to 31 October 2002.

Child pornography and other paedophile material has accounted for a significant proportion of the complaints received and actioned by the ABA. Of the approximately 1900 complaints received in the period 1 January 2000 to 30 April 2003, just under one-third have resulted in location of child pornography, and material of this nature accounts for almost one-half of completed investigations in which prohibited or potential prohibited content was located. Some 805 items, or 55 per cent of all items actioned, have been in these categories.

Of these 805 child pornography and paedophile material items, around 80 per cent have been located on overseas-hosted web sites, mainly in the United States and Russia, and most Australian-hosted items have been located in Usenet newsgroups that are hosted by major Australian ISPs. The ABA is aware that a significant amount of child pornography is distributed through a small number of such groups and the use

of newsgroups to distribute such material has been the subject of several studies[1]. The highly transient nature of newsgroup content generally and the fact that many ISPs host such content, have created some difficulties in administering the complaint mechanism in relation to such content. The ABA notes action taken by some ISPs to configure their newsgroup services to reject newsgroups that appear likely to contain problematic material.

The ABA is aware of a recent initiative by the Internet Watch Foundation in the United Kingdom to address the problem of child pornography distributed through Usenet newsgroups. On 13 November 2002, the IWF announced that it had identified 51 newsgroups known to contain significant amounts of child pornography, and a further 25 groups with names that appeared to advertise such material[2]. UK ISPs have agreed not to host such groups on their servers. In an effort to reduce the accessibility of this material, the ABA is considering whether it would be practical to implement this initiative in Australia, including whether such an arrangement could be included in the Internet industry codes of practice.

Peer-to-peer services

While peer-to-peer file sharing technologies are usually associated with exchange of music files and attendant intellectual property issues, the ABA is aware that these technologies are also being used to exchange child pornography and related content. Due to the highly ephemeral nature of peer-to-peer hosted content, particularly when hosted by end-users who are connected to the Internet via a dial-up service, the content located by the complainant is often difficult to locate after the complaint is lodged. The nature of these services also limits the ability of hotlines to provide law enforcement agencies with accurate information about the identity and location of persons suspected of exchanging child pornography using these networks.

The ABA has investigated a small number of complaints about material on these services, but has been unable to complete investigations of these complaints due to the factors outlined above. The ABA understands that other INHOPE hotlines have experienced similar difficulties when investigating reports of illegal content on peer-to-peer services, and has helped to develop guidelines that assist hotlines in dealing with such material. Further information about the ABA's work in this area is provided below.

Communities

Web-based communities have become a common source of child pornography and paedophile material and the ABA has investigated a small number of complaints about such content. The ABA has assisted the development of guidelines for hotlines that assist them in investigating reports of illegal material in web-based communities and further information about the ABA's work in this area is provided below.

[1] See for example Internet Watch Foundation (2001), *Newsgroups: An Internet Watch Foundation Discussion Paper* at http://www.iwf.org.uk/about/policies/newsgroups.html.

[2] A copy of IWF's news release regarding this matter can be obtained from the IWF web site at http://www.iwf.org.uk.

Liaison with law enforcement agencies

Internationally, hotlines such as that operated by the ABA have been a key source of intelligence for law enforcement agencies investigating the production and distribution of child pornography. In a number of cases referrals from hotlines have led to arrests. The ABA understands that European hotlines are working with law enforcement agencies throughout Europe to further strengthen co-operation between these bodies[3].

As noted above, over half of all items actioned by the ABA to date have constituted child pornography or other paedophile-related material. In line with the arrangements described above for the referral of such material to law enforcement agencies, 125 items of Australian-hosted material have been referred to Australian police forces and 610 items have been referred to the Australian Federal Police or the hotline in the country in which the material is hosted[4].

The majority of child pornography items actioned by the ABA have been hosted in the Unites States. Since February 2002, by agreement with the Australian Federal Police, such items have been referred to the Cybertip Line at the National Centre for Missing and Exploited Children, a non-government agency established to assist families and child welfare professionals in the prevention of abducted, endangered, and sexually exploited children[5]. NCMEC also assists law enforcement in the prosecution of child sexual abuse offenders, and provides specialist technical training to assist police in conducting investigations. The centre has a staff of around 400, including law enforcement personnel who are seconded to it. The Cybertip Line has received some 105,000 reports of Internet child pornography since it was established in 1998, and has played a key role in successful prosecution of numerous persons involved in producing and distributing Internet child pornography.

In the case of material hosted in countries where no INHOPE hotline operates, matters are referred to the Australian Federal police, which in turn refers the details to the law enforcement agency in the country concerned. With a significant proportion of child pornography being produced and/or hosted in Russia and some other Eastern European nations, the ABA has noted with some concern the advice from the AFP that authorities in these jurisdictions have not attached a high priority to investigating such matters. The ABA shares the concerns of other hotlines and child welfare bodies that such an environment has the potential to encourage commercial exploitation of children in the production of such material.

The feedback that the ABA has received from law enforcement agencies in Australia indicates that the current arrangements for referral of content are considered to be working well, and the ABA will continue its co-operative relationships with these bodies. In particular, the ABA understands that the Australian Federal Police is

[3] For discussion of the role of hotlines in addressing Internet child pornography see Machill, M and Rewer, A (2001), Internet Hotlines – Evaluation and Self Regulation of Internet Content, Bertelsmann Foundation: Gutersloh.

[4] Some items were referred to two or more agencies (for example, where it appeared that content was hosted outside Australia and that the content had been uploaded from within Australia, or where it appears that the content may be of interest to police in two or more States).

[5] The NCMEC web site is at http://www.missingkids.com.

placing increased focus on transnational crime, including the distribution of child pornography, and the ABA looks forward to contributing to this initiative.

International liaison

The Act assigns the ABA the function of liaising with regulatory and other relevant bodies overseas about co-operative arrangements for Internet content regulation and the ABA participates in a range of relevant policy and regulatory forums, including the Bertelsmann Foundation's International Network of Experts on Content Self-Regulation and UNESCO Internet regulation symposiums [1]. Of particular relevance to the ABA's role in relation to Internet child pornography is the ABA's associate membership of INHOPE[2].

INHOPE and its member hotlines are funded by the European Commission under the hotline component of its Safer Internet Action Plan to deal with complaints about illegal Internet content, predominantly child pornography. Current membership of INHOPE includes hotlines from Austria, Belgium, Denmark, France, Germany, Iceland, Ireland, The Netherlands, Sweden, Spain and the United Kingdom, with the ABA and the Cybertip Line in the United States as associate members, and hotlines in Italy and Korea currently provisional members. The ABA understands that hotlines are being established in a number of other countries.

INHOPE provides a valuable forum for exchange of information and expertise in hotline management and operational matters. The ABA is represented at two of the four members meetings held each year, and the ABA's Hotline Manager chairs the INHOPE working group on content issues, which was established in February 2002. Issues regularly considered by INHOPE include protocols for victim identification, emerging Internet technologies and hotline staff welfare issues.

The INHOPE hotlines network also facilitates exchange of information about illegal Internet content, where a report about such content is received in one country, but relates to content hosted in another. Most INHOPE hotlines have close working relationships with law enforcement agencies and the Internet industry in their country. Referral of content to other hotlines has helped to ensure that information about illegal content can be investigated by the relevant law enforcement agency and/or removed from the Internet as soon as possible. Some 35,000 reports were exchanged in a recent six month period.

The INHOPE content working group chaired by the ABA's Hotline Manager has been established to develop technical and practical guidelines to assist hotlines in dealing with a range of content issues. The working group has so far examined peer-to-peer services and web-based Internet communities, which hotlines have found to be key mechanisms for exchanging child pornography.

[1] Comprehensive information about the ABA's activities in this area is available in the ABA's submission to the Ministerial review of Schedule 5 of the Act at http://www.dcita.gov.au/Article/0,,0_1-2_10-3_481-4_111736,00.html.
[2] INHOPE's web site is at www.inhope.org.

In relation to peer-to-peer services, the working group has noted the difficulties associated with responding to reports of such material, but has developed technical guidelines to assist hotlines in locating content and collecting information that can be used by law enforcement agencies in subsequent investigations. The working group has also noted that hotlines and other agencies that are able to be 'pro-active' in searching for such material and with sufficient technical expertise will often be able to collect the information and other evidence required to successfully investigate such matters.

In relation to web-based communities, the working group has noted that these are becoming popular forums for exchanging child pornography, due in part to the ease with which they can be established, managed and used, and the security and anonymity they offer users. Some hotlines have established co-operative relationships with the providers of web-based community services, resulting in prompt detection, removal and investigation of problematic content. In the case of 'free' services that are supported by advertising, advertisers are being alerted to the potential for their brand to be associated with illegal content, and they in turn are encouraging service providers to be vigilant in ensuring that such content is not hosted on their services. Some service providers have also introduced identification and verification procedures that have acted to discourage customers from using their services to distribute illegal content.

Convergent devices

While most Australian families currently access the Internet using a personal computer modem and standard phone line[17], the ABA anticipates that emerging technologies will provide the capacity to access the Internet and other online services using a range of devices, including mobile devices.

The ABA considers that, as with the Internet, such technologies potentially offer tremendous benefits to the community. However, the ABA is aware that some new technologies may carry the potential for users, particularly children, to be exposed to potentially offensive or harmful content.

In relation to the matters being considered by the committee, of particular concern would be the use of mobile devices to engage in behaviour that may ultimately cause a child to be at risk of assault or abuse. The ABA understands that instances of this nature have occurred in overseas markets where convergent devices have been introduced. With mobile Internet technologies yet to be widely used in Australia, the ABA proposes that the implementation of such services be closely monitored by appropriate regulatory agencies, and that such bodies seek information from relevant overseas bodies about the handling of this issue in markets where these services have operated for a period of time. The ABA also would propose that child safety concerns associated with mobile devices be addressed through codes of practice for the providers of such services, and through the provision of information to users about the potential risks associated with such technologies.

[17] Australian Broadcasting Authority (2001), *The Internet at home: a report on Internet use in the home*, page 3.