RESEARCH AND STATISTICS DIVISION RESEARCH SERIES

Borders Conference — Rethinking the Line: The Canada-U.S. Border

Child Pornography on the Internet Session

Department of Justice Canada
Ministère de la Justice Canada

Canada

BORDERS CONFERENCE — RETHINKING THE LINE: THE CANADA-U.S. BORDER

CHILD PORNOGRAPHY ON THE INTERNET SESSION

Waterfront Centre
Vancouver, British Columbia
October 22, 2000

Steven Kleinknecht
McMaster University

The Research and Statistics Division
Department of Justice Canada

November 2001

This document is available in French.
Ce rapport est disponible en français sous le titre
Congrès transfrontalier
La frontière Canada-États-Unis :
Une réalité changeante.

Also available on the Department of
Justice Canada's Internet site, at
http://canada.justice.gc.ca/en/ps/rs/index.html.

Foreword

I am pleased to introduce *Rethinking the Line: The Canada-U.S. Border — Child Pornography on the Internet* panel session. In October 2000 the Policy Research Initiative organized a conference in Vancouver, Canada, Rethinking the Line: The Canada-U.S. Border along four themes: 1) Safety and the Line, 2) Crossing the Line, 3) Working Across the Line and 4) The Virtual Line. As our contribution to the conference, John Fleischman and Suzanne Wallace-Capretta, Senior Policy Officers, Research and Statistics Division, Department of Justice Canada, assisted by student Steven Kleinknecht, organized a panel on Child Pornography on the Internet as part of the Safety and the Line theme. The panel brought together international experts from a variety of fields including criminal justice, law enforcement and academia to discuss issues arising from child pornography on the Internet. The ensuing discussion revolved around the amount and nature of child pornographic images found on the Internet, the emergence of Internet luring as a new form of child sexual exploitation and the cross border obstacles encountered by law enforcement combating child pornography on the Internet. The feedback we received on the session combined with the high level of general interest in the topic and the paucity of information available on it convinced us that we should make this material more readily available. The report that follows is summary and transcripts of the proceeding of the panel session.

Roberta J. Russell, Ph.D.
Director, Research and Statistics Division
Department of Justice Canada

About the Research and Statistics Division

The Research and Statistics Division is staffed by social science researchers drawn from a broad range of disciplines including criminology, sociology, anthropology, education, statistics, political science, psychology, and social work.

We conduct social science research in support of the activities and programs of the Department of Justice Canada. We also provide statistical data, methodological services and analytical advice and undertake public opinion research and comprehensive environmental analyses.

We recognize that to be useful research must be accessible. In an effort to make our research more accessible we have created new products tailored to the needs of a diverse group of users, such as a research series, Qs&As, and fact sheets.

For further information on our research activities, please visit our Web site at http://canada.justice.gc.ca/ps/rs.

Table of Contents

Executive Summary

As part of the conference entitled "Rethinking the Line: The Canada-U.S. Border," the Department of Justice, Research and Statistics Division, in conjunction with the Policy Research Secretariat and the RCMP, assembled a panel of international experts to lead a session on enforcement and research issues surrounding child pornography and luring on the Internet. The panel was comprised of Sergeant Emmett Milner (Criminal Intelligence Service Canada), Detective-Sergeant Wayne Harrison (Winnipeg Police), Detective-Sergeant Frank Goldschmidt (Ontario Provincial Police, Project "P"), Andrew Oosterbaan (U.S. Department of Justice, Child Exploitation and Obscenities Section), and Dr. Max Taylor (University College Cork, Ireland). Jacquelyn Nelson of the British Columbia Ministry of the Attorney General acted as the moderator for the session.

The panel addressed two main conference themes: *safety and the line* and *the virtual line*. Crime committed over the Internet is often envisioned as being borderless, thus presenting some rather unique challenges for policy makers, researchers and law enforcement. One area of Internet crime, which has been seen as particularly deserving of attention, is the sexual exploitation of children. Therefore, this panel was assembled to discuss three central issues related to this concern: (1) the scope and nature of child pornography on the Internet; (2) sexual predators using the Internet to lure children; and (3) the challenges of policing child pornography across borders.

Scope and Nature of Child Pornography on the Internet

Dr. Taylor's presentation indicated that there is a great deal of child pornography on the Internet. However, Dr. Taylor suggested that we focus more on identifying the number of children who are being abused rather than trying to calculate the volume of child pornography on the Internet. As part of the COPINE project — *Combating Paedophile Information Networks in Europe* — Dr. Taylor's research team has amassed a database of over 60,000 old and new/recent child pornography images. Approximately 43,000 of these images are of girls and 18,000 are of boys. Each week, the team collects about 1,000 child pornography images off 60 different Internet newsgroups. The majority of the material downloaded is relatively old, consisting mainly of scans from magazines such as *Lolita*, originally produced 30 to 40 years ago. While the database is occasionally called upon by police to help identify children and offenders, it is maintained primarily for research purposes.

According to Dr. Taylor's work, approximately two new children are appearing in child pornography on the Internet newsgroups each month. Another trend they are finding is that the children depicted in the images are becoming younger. The research from the COPINE project suggests that the predominant age group is children between the ages of 9 and 12. However, Dr. Taylor qualified this figure by pointing out that it becomes very difficult to ascertain the age of children after they reach puberty and, therefore, his team does not monitor pictures in this age category. Dr. Taylor noted that roughly 10 percent of female images in the database are of babies and toddlers. He also indicated that the overwhelming majority of images are of Caucasian children. He pointed out that, while it is not difficult to find child pornography on the Internet, the average user is unlikely to stumble across it. Given the fact that so much of this material is available for free over the Internet, Dr. Taylor argued that it holds very little market value.

Although still-pictures are by far the most predominant form of child pornography on the Internet, video clips will likely become more common as the technology advances to allow for faster transmission of large multimedia files.

When researching the sexual exploitation of children, Dr. Taylor indicated that it is necessary not only to look at the Internet as a medium for the distribution of child pornography, but also as a place where paedophiles are able to communicate with one another and develop the types of contacts and support that help to sustain their interest in children.

Challenges

Each of the presentations highlighted the challenges faced by legal authorities and policy makers when attempting to deal with child pornography and luring of children on the Internet. As Det.-Sgt. Harrison indicated, it is important to acknowledge that most challenges faced by law enforcement in this area are also problems encountered when dealing with most forms of crime now being conducted over the Internet (e.g., fraud, money laundering, illegal gambling). What follows is an overview of some of the main challenges faced by legal authorities.

Volume of potential investigations. The presenters indicated that the overwhelming amount of child

pornography on the Internet presents a large number of potential investigations. Therefore, police find it necessary to give priority to some cases while postponing others. For example, "Project P" (the anti-pornography unit of the OPP) maintains a backlog of some 35 to 40 cases at any given time. Given the number of cases, Det.-Sgt. Goldschmidt indicated that it is not unusual for them to delay an investigation for six to nine months.

Resource issues. Investigations may involve a number of offenders and victims in various parts of the country or the world. Thus, the amount of time needed to put together a case, identify and interview the victims and offenders, coordinate with different police agencies, and travel to the different regions can make it difficult to move a case forward. Therefore, before beginning an investigation, police have to take into consideration the large amount of resources often required in such cases.

Remote storage. Some Internet Service Providers (ISPs) store their clients' identifying information and logs (record of their activity) in locations other than their immediate premises. Additionally, Internet users may choose an ISP in a different geographical location. Information can be stored virtually anywhere in the world as long as the country is connected to the Internet, which nearly every country is. This complicates matters when police are attempting to obtain search warrants and collect client information from the ISPs. Further complicating the investigation process is the reality that other jurisdictions often have different laws or may simply be uncooperative in assisting foreign police.

ISP retention of logs. ISPs are not legally obligated to retain client logs. Logs are useful for investigations as they contain such things as when the client logged onto the Internet, client activity while on the Internet, and Internet Protocol (IP) addresses to aid in the identification of the user. Since it is costly to store these logs, ISPs usually delete this information after a short period of time. America Online (AOL), for example, will hold new unopened mail for 28 to 30 days. When AOL members go outside of AOL to do their surfing, chatting, posting, etc., it may preserve that information for about 7 days. The retention period for AOL is actually considered good compared to some ISPs which delete most of the log information daily. This becomes a problem for police because it is difficult for them to get enough information to start the investigation process (e.g., warrants, information from foreign police agencies) in such a short time frame. Therefore, the suspect's log information may be lost before police are able to obtain the legal authorization necessary to examine this important source of potential evidence.

Legal definitions. Current legal definitions did not envision the Internet and the implications it would have on future understandings of possession and distribution of child pornography. For instance, legal definitions do not adequately accommodate the borderless nature of the Internet. This has had implications for investigations involving electronic child pornography stored by Canadians in other countries, and child pornography that has been stored in Canada by individuals from outside the country. The lack of a common international definition of child pornography also makes it difficult for police to coordinate and obtain cooperation during cross-border investigations. Officers also have no expressed legal authority to possess child pornography, which may hinder investigations.

Court decisions. The Supreme Court case of *R.* v. *Sharpe*, which challenged provisions within Canada's child pornography legislation, was seen by Canadian police as a potential cause for concern.[1] At the centre of their concern was the possible loss of the possession offence. Sgt. Milner described the possession offence as a "foot-in-the-door" for law enforcement when they are developing a case on an individual who may be involved in more serious forms of child abuse. However, he noted that if the possession offence was lost, the introduction of a luring offence might help to compensate for this loss. Another concern police had about the outcome of the Sharpe case was the potential for redefining child pornography, as it would affect how they conduct their investigations.

Unlike Canada, the United States has a two-part court system with laws varying not only by federal and state jurisdiction, but also from state to state for each of the 50 states. Therefore, court decisions can vary between states and between districts, resulting in various interpretations of federal laws such as possession of child pornography.

In addition, wholly computer-generated child pornography and morphed child pornography becomes an issue in court decisions as there may be no real child

[1]A few months after this conference was held, the Supreme Court delivered its decision in *R.* v. *Sharpe* (January 26, 2001). While the consequences of the verdict are still being reviewed, it would appear that the decision will not significantly alter the existing possession offence.

actually depicted in the images. Some courts in the United States have ruled that, for the image to be considered illegal, it must involve a real child. Proof that the photograph is of a minor may also become an issue in some cases.

Encryption. Encryption allows users to "scramble" their files into unreadable computer code, which can be deciphered only by using the proper passwords. Mr. Oosterbaan (U.S. Department of Justice) indicated that encryption is becoming more prevalent. If law enforcement obtains an encrypted file, they will devote resources to the case only if it is considered a national priority or a national security interest because of the amount of time it may take to access the encrypted file. He recommended that, if police foresee encryption to be an issue in a case, they be proactive in attempting to acquire the passwords ahead of time, possibly during the execution of a search warrant.

Anonymous and Web-based e-mail. Anonymous and Web-based e-mail makes it difficult for police to trace an e-mail back to the original sender. Companies such as "hushmail" and "freedom" fully encrypt their users' e-mail and then use a re-mailing system, which deletes any "surface" information that may connect the e-mail to the sender. Web-based e-mail, such as hotmail, allows users to create an anonymous account using false user information (e.g., name, address).

Cable connections. Cable modems maintain a constant connection to the Internet, which can be a problem for police if they need to identify who connected, and when. In addition, with dial-up accounts (using phone lines) in the United States, police can subpoena information from an Internet company about a client's account without the client ever knowing it happened. The opposite is true for cable law in the United States, which dictates that the Internet company must inform its client when police subpoena information from it regarding that client's account.

Suggested Priorities

To meet the challenges faced by law enforcement and help combat the sexual exploitation of children, the panelists made the following suggestions.

Cooperation and coordination. Given the international flow of information on the Internet, the panelists indicated that it is crucial to have cooperation and coordination among jurisdictions and agencies involved in the investigation of child pornography and luring of children on the Internet. There appeared to be agreement among the panelists that the International Criminal Police Organization (Interpol), on the international level, and Criminal Intelligence Service Canada (CISC), on the national level, have done a good job in coordinating police efforts. However, the panelists also felt that both agencies could be more effective if they were given more resources and a stronger role to play.

On the national level, Det.-Sgt. Harrison suggested that CISC's role be strengthened by giving it a core mandate to oversee all Internet investigations. He suggested that its responsibilities could include heading up a national task force, which would work proactively to identify victims and offenders; developing and maintaining facial and filename recognition software; coordinating all international investigations, both incoming and outgoing; conducting training across the country using the "train-the-trainers" model; and establishing and maintaining national offender registries.

Internationally, Dr. Taylor indicated that Interpol is developing a database of child pornography that could be tapped into by police all over the world. However, for the database to be effective it will require the police to continually contribute new information.

In addition, improved cooperation between law enforcement and ISPs was highlighted. CISC has been involved in talks with the Canadian Association of Internet Providers (CAIP) and various other ISP groups. Sgt. Milner pointed out that some ISPs were not aware of what is expected of them from law enforcement. Therefore, liasing with ISPs has and will continue to create more information sharing between the industry and law enforcement.

ISP regulation and self-regulation. Panelists indicated that the technology is available for ISPs to better regulate the flow and storage of child pornography on their servers. Dr. Taylor believes that the existence of child pornography on the Internet could be controlled if the ISP industry chose to do so. Det.-Sgt. Harrison provided an example of how to accomplish this. He advocated that provincial and state regulations be instated for ISPs, which would include requiring a physical street location for each IP address assigned to their users to assist police to execute warrants.

Mr. Oosterbaan stated that one of the difficulties noted by ISPs is that illegal material is replaced almost as quickly as the ISP removes it. Thus, it is necessary that a way be developed for ISPs to channel information to the police so that individuals can be prosecuted to put

an end to this "reposting" process. He indicated that some recent legislation in the United States will require ISPs to report potential criminals to law enforcement. The U.S. Department of Justice is currently developing regulations on how this process will work. Mr. Oosterbaan stated that, while this legislation may be helpful in dealing with the big ISPs (e.g., AOL), it may not be as effective in dealing with the smaller ones.

Perhaps the most significant way in which ISPs could facilitate cooperation with police and help regulate the flow of illegal material would be through the extended retention and sharing of client log information. ISPs now delete their logs after a very short time period. Therefore, the panelists suggested the mandatory retention of logs for a minimum of three months as a development that would significantly aid police in conducting their investigations.

While it may be costly for ISPs to retain logs, Dr. Taylor argued that ISPs have a duty to exercise social responsibility. In support of his argument, he pointed out that it is not acceptable in any other setting for a commercial organization to facilitate the commission of a crime. However, he also noted that some ISPs have used the defence of being a "common carrier" of information, which is a claim used by the mail industry to protect itself from being sanctioned for contributing to the distribution of illegal material. Therefore, Dr. Taylor suggested that it would be beneficial if the ISP industry could develop a way to regulate itself, rather than having the state impose regulations.

Training and education. Internet crime is a relatively new area for policy makers and legal authorities. Therefore, the panelists stressed the need to train and educate policy makers, police, prosecutors and judges. Mr. Oosterbaan discussed the necessity of keeping all these parties informed of advances in the technology, because if there is one weak link in the chain (e.g., a prosecutor who does not understand the technology) it may result in difficulties in prosecuting a case. The panelists emphasized that training must be a continual process to keep up with the rapid evolution of technology.

In addition, Dr. Taylor stated that probation officers and social workers should be educated about the Internet. As part of his research, he has found that those working in the social welfare system often do not understand the Internet and are thus ill equipped to adequately supervise offenders. He discovered that these workers are reluctant to get involved because they are worried that the offender is going to know more about the Internet than they do.

Panelists also promoted educating parents and children about the possible dangers that may be encountered on the Internet. Det.-Sgt. Goldschmidt stated that he is shocked to hear that some parents allow their children to meet individuals they've met on the Internet in public places unsupervised.

Child-centred focus. Panelists stressed that law enforcement should focus on identifying the victims and give precedence to cases involving individuals who are victimizing children by producing child pornography. Det.-Sgt. Harrison indicated that this is the only way to prevent children from being victimized. However, panelists noted that investigations of this type can be resource intensive and time consuming. This is illustrated by an investigation conducted by Project "P," where police interviewed nearly 1,000 victims who had been terrorized by one paedophile over a 30-year period. The investigation took 13 months to complete.

Keeping legislation current. As mentioned, one of the challenges faced by legal authorities is the difficulty they face when trying to apply existing legislation to criminal activities involving new technologies (e.g., the Internet). Therefore, the panelists recommended that policy makers ensure that legislation is revised to reflect current technology.

Panelists indicated that the creation of luring legislation would be a positive development. This legislation is seen as necessary to deal with the unique circumstances surrounding the online enticement of children. Det.-Sgt. Harrison stated that:

> [Luring legislation] is a must to prevent predators from using the Internet to solicit, lure and victimize children. Currently, in Canada a child must be victimized for an offence to occur. There is no provision in current legislation for an investigator to pose as someone under the age of 18 and therefore investigators cannot be proactive in terms of actually laying a luring offence charge. We have invitation to sexual touching, but it requires the person to actually be under that age and not a person who they believe to be under that age. Complicating this legislation is the fact that in Canada the age of consent for sexual intercourse is 14 years. This means that any 40-year-old or 50-year-old in Canada can have sex with a 14-year-old child. Unfortunately, any new legislation dealing with a luring offence will have to be framed around this age of consent. I think that the age of consent issue is the subject of discussions right now and I think it's very important that it be modified in some way.

Mr. Oosterbaan added that, while there is legislation in the United States that deals with luring, it probably could be strengthened.

To update legal definitions, Det.-Sgt. Harrison suggested that *distribute* be defined to include, "Making available via a computer network that passes through or originates from Canada and is now located outside of Canada." He also suggested that possession be redefined to include "password-accessed sites or sites controlled by Canadians, even though the site is located outside the country." He stated that provisions should be built into the Canadian *Criminal Code* allowing police to possess and send images, so that officers could send exhibits and notes through secure servers. This would facilitate sharing information during investigations and thus help to identify victims and offenders.

Det.-Sgt. Harrison noted that the enactment of Bill C-40 (the *Extradition Act*) is a good example of legislation, which recognizes the necessity of not only keeping pace with, but also taking advantage of, current technology to help fight crime. The legislation allows witnesses from inside and outside of Canada to give sworn testimony in court via video conferencing. Witnesses can do this from the comfort of their own home locations, allowing them to testify without bringing them to the jurisdiction where the case is being heard. Video conferencing was used recently in Winnipeg to secure testimony from a group of seniors who were victimized by a telemarketing fraud. During the preliminary hearing, 10 seniors testified from four different U.S. states using video-conferencing technology. They gave sworn testimony, which the judge accepted. The judge also commented on how impressed he was with the use of this technology to bring in this type of evidence. Det.-Sgt. Harrison remarked that the use of video-conferencing technology to secure witness testimony is a very cost-efficient way to conduct prosecutions when the witnesses are from other jurisdictions. He also suggested that the next step will be using this technology for taking statements from other police agencies or interviewing other police officers to obtain warrants.

Making Internet crime an area of federal jurisdiction was also advocated as a way of making legislation more effective. To do this, Det.-Sgt. Harrison suggested that the *Controlled Drugs and Substances Act* (*CDSA*) be used as a model. He pointed out that the *CDSA* was made a federal responsibility due in part to cross-border issues involving the trafficking of drugs. He stated that the number of physical border crossings involving drugs pales in comparison to the number of virtual border crossings made every minute over the Internet. In his opinion, some of the benefits of creating a new and separate Act would include the specialization of federal Crown attorneys to prosecute Internet offences; access to more resources to combat Internet crime; and the development of modern legal definitions specific to Internet usage for offences such as distribution and possession of child pornography.

Developing software tools to assist in investigations. Panelists suggested the further development of software tools to help law enforcement in their investigations. A major software enhancement would be programs that help to identify children and to separate new and old child pornography. Det.-Sgt. Harrison indicated that police often spend a great deal of time identifying images of child pornography, but due to inadequate software, they spend very little time identifying the children in these images or determining when the image was created. He suggested that enhancements be made to filename and facial recognition software to facilitate this process. He suggested that law enforcement could use filename recognition software to identify new images and subsequently use facial recognition software to compare these images to a master file of children who were reported missing (or a similarly maintained database).

The maintenance of a child pornography database is a necessary part of the software-aided identification process. As mentioned previously, Interpol is developing such a database, but it is expected to require much time and input from various international police agencies for it to be effective. Although the database maintained by Dr. Taylor's research team was not created for aiding law enforcement to identify abused children, it has occasionally been used for this purpose. Dr. Taylor's database does not work on the basis of software recognition, but on the use of text-based descriptors. Dr. Taylor stated that he is sceptical of facial recognition software. Therefore, his team meticulously sifts through the images by hand to categorize them. Referring to the EXCALIBUR database used by Swedish police, Dr. Taylor noted that, while it may be effective, it is not 100 percent reliable; thus, he feels more comfortable relying on visual inspection of images. However, the process is not without its drawbacks; it is labour intensive, tedious, and can be psychologically upsetting for the students categorizing the obscene material.

Mr. Oosterbaan stated that any new software enhancements must take into consideration existing law enforcement frameworks; that is, it is important to integrate or adapt any new technologies with traditional law

enforcement methods. While it is necessary for software enhancements to fit into the existing framework, it is just as essential for law enforcement to remain somewhat flexible and receptive to the new technologies that may be necessary to assist them in their investigations.

Hotlines and tiplines. The use of hotlines and tiplines for receiving information from the public was also suggested. Mr. Oosterbaan indicated that such information sources have worked very well in the United States. For example, during a 27-month period the CyberTipline, which is operated by the National Centre for Missing and Exploited Children, received over 22,000 reports of child pornography and 3,000 reports of potential luring cases.

Summary of Recommendations

To address the problem of child pornography on the Internet and some of the challenges faced by law enforcement in dealing with this problem, the panelists made the following recommendations:

- The cross-border nature of the Internet will require international cooperation and coordination among jurisdictions and agencies involved in the investigation of child pornography and luring of children on the Internet.
- Collaboration between the Internet industry and law enforcement is also key.
- Some form of ISP regulation and/or self-regulation could help to control illegal activity on the Internet.
- Training for legal professionals is necessary for them to keep pace with advances in technology.
- Laws not only need to be updated to include the new technologies, they also need to be written in such a way as to accommodate the evolving nature of technology.
- Given the large number of potential child pornography cases, it is necessary for police to maintain a child-centred focus by concentrating on the identification of victims and giving priority to cases involving the production of child pornography. Implementing existing software tools and further developing this technology (e.g., child pornography databases, file and facial recognition software) would aid in the victim and offender identification process.
- Public education is required to ensure that parents and children are aware of the potential dangers of the Internet.
- Further implementation of hotlines and tiplines will aid in the reporting of child pornography and potential luring cases.

Participants

Moderator

Dr. Jacquelyn Nelson — Senior Policy Analyst, Ministry of the Attorney General of British Columbia

Dr. Nelson is a senior policy analyst with the Ministry of the Attorney General of British Columbia. She has been with the Ministry for 12 years, and her portfolios include offensive material on the Internet, prostitution, hate crime, restorative justice and federal/provincial/territorial justice policy issues. She has conducted research in the area of sexual exploitation of children and youth, and is currently co-chairing a national working group dealing with child pornography on the Internet.

Discussant

Dr. Max Taylor — University College Cork, Ireland

Max Taylor is a professor of Applied Psychology at University College Cork (UCC) in Ireland, and has been head of the department since 1983. He is also the director of the Child Studies Unit at UCC, which focusses on research, training and policy to address the needs of vulnerable children. Dr. Taylor directs the Combating Paedophile Information Networks in Europe (COPINE) project. His current work with COPINE involves the maintenance of a reference database on child pornography, the assessment of the dangerousness of paedophiles through their collections of child pornography, and the nature and incidence of child sex tourism and child trafficking in Europe. Dr. Taylor is also a member of the Irish government's Internet Advisory Group, and the Working Group on Illegal and Harmful Uses of the Internet.

Panelists

Sergeant Emmett Milner — Criminal Intelligence Service Canada

Sergeant Milner has been with the RCMP for 26 years, and prior to that he served with the Ontario Provincial Police (OPP) and the Royal Hong Kong Police. He is the National Coordinator for the Sexual Exploitation of Children Initiative with Criminal Intelligence Service Canada (CISC). In this capacity, he has directed the formation of a national strategy to combat the exploitation of children, implementing guidelines for all law enforcement agencies in Canada, and has been instrumental in developing an international network to ensure that investigators around the world are equipped to fight exploitation through the use of the Internet.

Detective-Sergeant Wayne Harrison — Winnipeg Police, Vice Squad

Det.-Sgt. Wayne Harrison has been a police officer for 22 years and is currently with the Winnipeg Police Services, Vice Squad. He has investigated child pornography and obscenity offences since April 1996. He has been involved in over 100 investigations of this type. Some of these investigations included linkages with officers in various U.S. centres, Germany, Australia and Sweden. Det.-Sgt. Harrison has been involved in training police personnel on issues of child pornography on the Internet, as well as making presentations at numerous conferences. In 1998, he received a provincial crime prevention award from the Manitoba Department of Justice for his Internet safety presentations. He is also a member of a Manitoba committee advocating a change to the *Criminal Code* to make Internet luring of children for the purposes of sexual exploitation an offence.

Detective-Sergeant Frank Goldschmidt — Ontario Provincial Police (OPP), Project "P"

Det.-Sgt. Frank Goldschmidt has been with the OPP for 20 years. He has been with the pornography crime unit since 1991, where he is currently the senior investigator and is in charge of operations for the unit. Det.-Sgt. Goldschmidt investigates child pornography offences in the Province of Ontario, many of which deal with computers and the Internet. He has worked in an undercover capacity on numerous occasions and is qualified by the Ontario court as an expert in the investigation and identification of child pornography and obscene material. He is also actively involved in police training and has published manuals and guides for police relating to investigative techniques.

Andrew Oosterbaan — Deputy Chief for Litigation, Child Exploitation and Obscenities Section, United States Department of Justice

Mr. Oosterbaan is from the United States Department of Justice, Criminal Division, Child Exploitation and Obscenities Section, where he is the Deputy Chief for Litigation. He handles all criminal litigation for the section, including investigations and prosecutions nation-wide involving child pornography, child exploitation, child sexual abuse, trafficking of women and children for sexual purposes, obscenity, child support enforcement, and international parental abduction. Mr. Oosterbaan is also involved in developing

and coordinating multi-district investigations and initiatives. In addition, he manages the section's training program for prosecutors and law enforcement agents throughout the United States.

Session Proceedings

Dr. Jacquelyn Nelson (Moderator) — Ministry of the Attorney General of British Columbia

Opening Remarks

Good afternoon, my name is Jacquelyn Nelson and I've been asked to introduce this session and be the moderator because I am the co-chair of the Federal/Provincial/Territorial (F/P/T) Working Group on Offensive Content on the Internet. I'm also with the Ministry of the Attorney General of British Columbia, Policy Sector.

The F/P/T Working Group on Offensive Content on the Internet is developing recommendations to address child pornography and luring over the Internet. In addition to considering options for law reform, we're also trying to examine how to work with other sectors to make the laws effective. We're considering how best to partner with industry, for example, and to ensure some cooperation from industry in matters such as keeping logs, reporting offenders, and also just raising awareness among industry itself regarding problems on the Internet. In other words, trying to link with them to develop some solutions.

We are also reviewing issues regarding the needs of the police. These issues include how to better link police and specialists who have expertise in Internet crime, how best to do training, and find out what other things are needed to support police when they are investigating Internet crime in general, and particularly child pornography and luring.

Finally, our working group has taken the approach that we need to have an integrated approach to this issue, which includes education of the public regarding what the dangers on the Internet may be, and what they can do if they encounter some of these dangers.

I know that our panel today is going to be covering many of these issues. I'm pleased to be here to introduce them to you. I will start by introducing each of the panelists by name.

To my immediate right is Max Taylor, followed by Emmett Milner, then Wayne Harrison, Frank Goldschmidt and Andrew Oosterbaan. Before I introduce the first speaker, I would like to introduce Dr. Max Taylor who is going to serve as the discussant throughout the session. Dr. Taylor, as mentioned, will be commenting on the presentations made in this session.

Our first presentation is by Emmett Milner.

Sergeant Emmett Milner (Panelist) — Criminal Intelligence Service Canada

Thank you very much. I am presently attached to Criminal Intelligence Service Canada (CISC). A lot of people may not know who CISC is. You might look at CISC as a national task force that looks at organized crime and other specific issues. We in the central bureau have, for example, an officer from the Vancouver Police seconded to us for three years, OPP members, Sûreté du Quebec, Montreal Police, Customs, Ottawa-Carleton Regional Police, Calgary and so forth. So we have a cross representation of law enforcement in our office and we look at particular issues. What we are talking about today is child pornography on the Internet. My particular project goes a little farther than that; it's to combat the sexual exploitation of children.

First, I'd like to give you a little historical background on CISC. In 1996, the Commissioner of the RCMP had a vision of where we were going to go and how we were going to coordinate investigations on the Internet regarding child pornography and the exploitation of children, and so forth. Along with the Commissioner, another person instrumental in putting this together was Chief Fantino who worked to bring law enforcement together and to rethink how we do this to ensure a coordinated effort. By 1998, the CISC executive decided that CISC would carry the mandate to coordinate law enforcement across Canada. This was when I came on board. We developed a strategy that was introduced to all law enforcement across Canada. The CISC executive is made up of the Commissioner of the RCMP (who's the Chairperson), the Commissioner of the OPP, and all major police departments across Canada. They bought into this and agreed that CISC would command a leading role.

Each province has a sexual exploitation coordinator who works for the province on a regional basis and CISC works in conjunction with them. It goes from the municipal level, to the provincial level, and then up to the national central bureau where I work. I actually work out of the RCMP national headquarters. We could be in another office, but for cost efficiency and so forth our central bureau is situated there.

I want to talk a bit about the volume of the work we have. I want to talk about our priorities and about some challenges we face.

If you look at Canada in terms of the Internet, we are the second most connected country in the world. In 1997, 31 percent of households were connected; in 1998, 37 percent; and, in 1999, 42 percent. I imagine

that this figure will increase as time passes. In 1994, for example, no schools or libraries were connected; in 1999, they were all connected.

There's an overwhelming volume of child pornography on the Internet. I think we have to ensure that we create some sort of priority in tackling the problem. It's impossible to investigate each and every case of child pornography on the Internet because it would exhaust our resources. We have a partnership that we've developed with Interpol; we meet on a biannual basis. This week, the biannual meeting is being held in Belgium. Two years ago, we hosted the meeting in Ottawa. These investigations can carry particularly heavy costs. They may go on very long and travel could be involved, so you have to decide how you're going to tackle the investigation. However, the other most important point is identifying the victims in the child pornography. Basically, the volume aspect becomes a global problem because there are no borders for crime on the Internet. It's a brand new area for a lot of us.

Our priority in CISC, which has been agreed upon by the executive committee, is the sexual exploitation of children; child pornography on the Internet is part of that priority. Also, within this priority is child prostitution and sex tourism. We in CISC put out an annual report as mandated by the government. If you're interested, you can retrieve a copy of the report from CISC or from our Web site (www.cisc.gc.ca). I have a note here on prioritizing child abuse. First is child pornography and it's a problem that most of us face. I think we have to ask ourselves: "How are we going to target it?" "Can we be more proactive by going online and working on an undercover basis?" This is something that has to be tackled on an individual basis and each department will have to look at it.

Now, let us turn to some of the challenges. We have to look at the legislation aspect. The Sharpe decision is going to be coming down probably after the election now. This decision is going to affect our possession charge. Our possession charge under section 163 of the *Criminal Code* is basically what I call a "foot in the door." If we find out that the individual has child pornography it gives us a foot in the door; from there we will often find child abuse and it will give us some extra ammunition. If we lose that section under our legislation, the Justice Minister has discussed luring, which might be a way out.

Training is an important part of keeping our investigators up to date. It's a continual thing. If you're in the high-tech field today, you'll know that people are requiring updated training as technology changes every couple of months. So the training aspect is really, really important.

Structurally, the Internet Service Provider (ISP) monitoring of Internet activity is really important, too. We have a pretty good liaison with the ISPs. Our biggest problem is tracking and obtaining the evidence required. So logs would be the most important part to look at. Right now there is no policy. ISPs are not regulated in Canada and I don't think they're regulated in very many countries. It's a very difficult thing to do. We have developed a rapport with CAIP (the Canadian Association of Internet Service Providers). CAIP is one of the groups we continually strive to keep in contact with to assist investigations and investigators.

Basically, the investigations on child pornography go from Interpol, through our office, and then to more regional offices. In 1999, we had 164 requests that came through — 103 were international, 61 were national. This year so far we are up to 180; 120 were international, 60 were national.

Dr. Jacquelyn Nelson

Thank you, Emmett. One thing that Emmett mentioned was the possibility of luring legislation in Canada, as a possible foot in the door depending on the Sharpe decision. You may or may not be aware that in early September the federal Justice Minister had committed to bringing in luring legislation. What that means in view of the federal election, I don't know.

Our next speaker is Wayne Harrison.

Detective-Sergeant Wayne Harrison (Panelist) — Winnipeg Police, Vice Squad

First, I would like to thank the federal government, John Fleischman's office and his co-workers for inviting me here to make a presentation. It's a privilege for somebody who's a street cop turned cyber-cop to be able to attend a convention such as this and actually speak to the researchers and policy makers who make the decisions that affect how we have to do our work. Hopefully our message, our concerns and what we would like to see done is acted upon in some manner, and are not simply information given to you.

Although this presentation will address child pornography, the Internet crime I refer to will also deal with other Internet crimes that are occurring, such as drug trafficking, hate crimes, illegal gambling, credit card fraud, stalking and copyright infringement. Consider

all these offences as well. Although I will speak about child pornography, all these offences are booming on the Internet right now.

I will present some of the positive developments that have occurred recently that have assisted us, and are signs that we are moving in the right direction. I will also make some suggestions that I see as an investigator that would assist us in doing our job and making children safer in Canada.

Positive Developments

First, having this topic discussed and brought up at this level, at this type of conference, is obviously a positive. As Emmett has described, CISC has taken a lead role. It has initiated the process of making the necessary contacts and developing contacts with the various outside agencies on behalf of all investigators in Canada. And for that we are thankful to CISC and the related agencies that he works with because it's a very important part of Internet investigations and it's a theme you will probably hear throughout this session. Cooperation and sharing of information is the only way that these investigations can be completed.

Another positive was the enactment of Bill C-40 in Canada. This was a recent change in Canadian legislation, which allows witnesses from in and outside of Canada to give sworn testimony in court via video-conferencing technology. They can do this now from the comfort of their own home locations. This will obviously assist in the court process by having witnesses available to testify without having to bring them to that jurisdiction. This was used last month in Winnipeg, to our knowledge for the first time, for testimony from a group of seniors who were victimized by a telemarketing scam. During the preliminary hearing, 10 seniors testified from four U.S. states using video-conferencing technology. They gave sworn testimony, which the judge accepted, and the judge commented how impressed he was with the use of this technology to get in this type of evidence. It's a very cost-efficient way to conduct prosecutions when the witnesses are from other countries. Obviously, it is something that police services will have to use for taking statements from other police agencies or interviewing other police officers for obtaining warrants. That will be the next step: sworn statements from police officers given via video conference. It's a tremendous tool for police officers. It's kind of ironic that some day an accused will be charged for distributing child pornography over the Internet and the same technology will be used to convict him. Internet transmissions will be accepted in court as part of sworn testimony, and I would say within five years the technology will be there. That's an advancement we have to take advantage of and we have to be ready to take it. For those of you interested in that particular investigation, I can give you the name of the officer who coordinated the effort and she can speak to you directly. She encouraged me to tell you to call her for some of the bumps and kinks that she went through to get all these witnesses before a court process.

Another positive development is that luring laws are finally in the process of being developed in Canada. This is a must to prevent predators from using the Internet to solicit, lure and victimize children. Currently, in Canada a child must be victimized for an offence to occur. There is no provision in current legislation for an investigator to pose as someone under the age of 18; therefore, investigators cannot be proactive in actually laying a luring offence charge. We have invitation to sexual touching, but it requires the person to be under that age and not someone who they believe to be under that age. Complicating this legislation is that, in Canada, the age of consent for sexual intercourse is 14 years. This means that any 40-year-old or 50-year-old in Canada can have sex with a 14-year-old child. Unfortunately, any new legislation dealing with a luring offence will have to be framed around this age of consent. I think that the age of consent issue is the subject of discussions right now and that it's very important it be modified in some way.

Areas for Improvement

Here are some suggested areas of improvement. The first is to make Internet crime an area of federal jurisdiction. Use a model similar to the *Controlled Drugs and Substances Act* (*CDSA*) in Canada. For the benefit of any of our American colleagues who are here, the *CDSA* covers narcotics and all other drugs and their regulations in Canada. It is not actually part of our *Criminal Code*, but a separate Act with its own definitions. The *CDSA* was made a federal responsibility due in part to cross-border issues involving the trafficking of drugs. This pales in comparison to the number of crossings made every minute across the virtual borders on the Internet. Some of the benefits of creating a new and separate Act are that it will allow for specialization of federal Crown attorneys to prosecute and allow access to more resources to combat this problem. This will also include modern legal definitions specific to Internet usage for offences such as distribution and possession.

Currently, we are bound by age-old definitions that have been established through years of case law that had no envisionment of what the Internet is. I would like to see *distribute* defined to include

"Making available via a computer network that passes through or originates from Canada and is now located outside of Canada." Secondly, I would like to see *possession* redefined to include password-accessed sites or sites controlled by Canadians, even though the site is located outside the country. I will get into some case-related specifics that make us powerless to do our job properly. I would also build in provisions for possession and sending of images by police officers, which will allow them to send exhibits and notes through secure servers. Currently, officers have no legal expressed authority to even possess those pictures. Contrary to the *Criminal Code*, under the *CDSA* officers are allowed to possess drugs and are even, in the right circumstances, allowed to exchange drugs for money for the purposes of a criminal investigation. We are not even allowed legally, other than a general phrase of "unless it is in the public good," to hold or to have any child pornography even as police officers. That's something from a police perspective that makes us a little nervous at times when testifying in court.

The second topic I would like to raise is regulating ISPs. There is a need to develop provincial and state regulations for ISPs, which should include requiring a physical street location for each Internet Protocol (IP) address assigned to them to assist us in the execution of warrants. I was recently involved in an investigation where the making of obscene materials offences were charged against two individuals. They were storing these images on a server that we believed was located in the United States. In order to locate the physical street location of a server, in order to execute a search warrant, we have to rely on the integrity of the company's employees to provide information and then rely on them not to delete this information. Further complicating this was that the laws in Canada and the United States differ. So it appeared to us that we have no legal remedy to shut down the server; in fact, this business continues to operate south of the border on a U.S. server. Also needed is a regulation requiring the mandatory storing of dial-in logs of ISPs for a minimum of three months. It's a length of time that I've concluded — based on investigations and the length of time it takes us to get the materials under the current system — to get us in a position where an execution warrant is possible. Currently, ISPs are under no regulations and we've encountered some that keep their records for as little as three days, making any type of investigation futile.

Thirdly, I would like to see software enhancements. Facial or filename recognition software needs to be further developed. It's being developed right now in Europe, but it needs to be improved. Facial recognition software will compare the faces on the computer images of child pornography with the faces of known persons or victims on a master file. Similarly, filename recognition software could compare the name of computer images with a master list of the names of images known to be child pornography. Although these names can typically and easily be changed by the person receiving it, I would say that in 80 percent of cases they do not change the names, and we're seeing the same titles over and over again. Currently, investigators are spending hundreds of hours identifying thousands of images of child pornography, but due to inadequate software no time is spent identifying the victims in these images or determining when they were created. New child pornography is being created every day, and investigators relocate these images after they have been traded and posted numerous times. We could use filename recognition software to identify the new images and then we could use facial recognition software to compare these images to a master file of children who were reported missing or a similarly maintained database. Arresting the possessors and traders of child pornography is not enough. The number one priority must be to arrest and charge the people who are creating these images and abusing children. This is the only way we can prevent children from being victimized and prevent the further victimization of other children.

A fourth suggestion would be the development of a national task force. Using a model similar to Weisbaden in Germany, Canada could create a proactive joint forces team from various regions across the country. In Germany, online investigators search the Internet for fileservers; then, if they are able to download child pornography from these fileservers, they forward a copy of the report to investigators from the country where these files were located. A dedicated national task force within Canada could do this type of proactive policing within our own country; develop virtual offices in each region, using secure servers, to allow these investigators continuous immediate contact. In other words, simply use the technology that the criminals are using for law enforcement purposes. Investigators would be responsible for regional investigations, including the provision of training to municipal services to assist them in completing their own local investigations. In the United States, I've been involved in investigations with the FBI, U.S. Customs, U.S. Postal Inspectors, and several municipal police forces. All are working hard, but certainly efficiency could be improved through a better coordinated effort.

And lastly, I would suggest the development of a national agency, perhaps using CISC, to oversee all

Internet investigations. Responsibilities could include being in charge of the national task force; developing and maintaining the facial and filename recognition software; coordinating all international investigations, both incoming and outgoing; conducting all training in the country using the "train-the-trainers" model; establishing and maintaining national offender registries; and identifying victims' lists and investigators' lists. CISC has taken on part of this role already, but giving it a core mandate as the top echelon of investigators would be a very important step in my view. Obviously, this could then be shared on a global scale. In a perfect world there would be one agency coordinating all the global efforts. Although it's physically impossible and very unlikely to occur, that's what is ultimately required.

In closing, bringing the Internet under control is a daunting task. A conference like this could be a catalyst. It will take human and financial resources, as well as a willingness of agencies to put their personal agendas aside and work cooperatively, to create a safer and lawful Internet. Any further inaction though, allows the predators continued easy access to children. As the scope continues to increase, it will make it even more cost prohibitive to provide these solutions down the road. For these reasons, I believe an investment now is simply the only answer.

Dr. Jacquelyn Nelson

Thank you, Wayne. I think you raised some very interesting points. I hope that we can have some questions about some of your suggestions, particularly making Internet crime a crime of federal jurisdiction.

The next speaker is Frank Goldschmidt.

Detective-Sergeant Frank Goldschmidt (Panelist) — Ontario Provincial Police, Project "P"

I would like to take this opportunity to thank the group for inviting me to Vancouver. It is very beneficial to be able to share some of our pros and cons of what we are doing with a group like this. My normal presentation is some two to three hours, so I've really done a lot of chopping to squeeze it down to 15 minutes.

I have been with the Ontario Provincial Police (OPP) for almost 21 years now. I've been with the pornography unit for almost 10 years. This unit has been around since 1975. Before 1993, the mandate was solely focussed on investigating the distribution, making, importing and sale of obscene material. Prior to 1993, before the child pornography legislation came into effect, child pornography fell under the obscenity section of the *Criminal Code*. When the new child pornography legislation was passed in 1993, our mandate changed. Now we solely investigate the distribution, making and importing of child pornography within the Province of Ontario. To give you some idea, before 1993, and before the Internet booming the way it is right now, it was very uncommon for us to investigate more than one or two child pornography cases in one year. Since then it has doubled, doubled and doubled as the years have gone by. In a moment I will give you some figures.

Our unit has grown from two officers in 1991 to 14 now. We are overwhelmed with the amount of child pornography that is available mainly now through the Internet. The OPP has taken the initiative to try to combat this problem, and as a result it has doubled the size of the unit in the last four years. We do assist other agencies in Ontario as well as across Canada in investigating child pornography cases, mainly because this is all we do. We are updated almost daily as to what is child pornography and what is not, and what are the most useful ways to investigate these crimes. The OPP has been considered the lead agency in Canada for investigating child pornography; consequently, we get calls from all across the country for assistance. Some of us have been qualified in the courts as experts, not only in the identification of child pornography, but also in the forensic identification of computers.

Our unit is involved in relatively aggressive enforcement. We try to do proactive policing, but as a result of all the incoming cases that we receive from other police agencies in the province and other countries, it is somewhat limited. To give you an idea, one of the guys in the unit and myself were on the Internet one evening in the Internet Relay Chat (IRC) channels, and within a three- to four-hour period we identified 44 persons in Ontario who were involved in the distribution, making, importing or sale of child pornography. People often wonder how we are able to identify where the individuals are right up front. Well, it's kind of one of our little trade secrets that I think I'll just keep under my hat for now.

Our unit's priority is to investigate child pornography. There is an overwhelming amount of child pornography on the Internet and it appears that the offenders are now a little bit braver, now that they can distribute child pornography over the Internet, rather than in person. They seem to feel a sense of security and anonymity because they are not really talking face-to-face like they used to, for example, when they would

meet me in a seedy establishment. Now, over the Internet, they feel quite free to talk about their preferences and how much material they have. The computer and the Internet have allowed individuals to store large amounts of material on their systems, as well as to trade large amounts of material in a very short period of time.

Now, I'll update you on the amount of work we're doing. In 1997, we completed 83 investigations and laid 105 charges involving 20 people. To date, in 2000, we have completed some 117 investigations and laid 101 charges involving 20 people. People often question the 20 — it seems like such a low number. Our priority, however, is not only to prosecute the offenders, but to identify the victims. In some cases, we have successfully identified the paedophiles' victims. In one case in a small southern Ontario community, one paedophile resulted in us interviewing almost 1,000 victims this person had terrorized in about a 30-year period. This is not the type of investigation you can complete in a one- or two-month period; this investigation took 13 months.

The Internet has provided the perfect tool for paedophiles to distribute their collections and it has basically become a borderless crime. The Internet has been used by paedophiles to lure children from across the U.S./Canadian border, and vice versa. It still shocks me to hear, when these luring offences take place, that there are parents who are actually allowing their 12- and 13-year-old children to go to malls and street corners to meet individuals they've met on the Internet. Quite often our officers pose as children or parents who have children, who are willing to offer their children for sex. There have been a number of cases where we've actually met these individuals in wired hotel rooms and more or less let them "say their piece" before we come through the door and arrest them.

We currently execute warrants to obtain ISP information. As Wayne has previously mentioned, a lot of the ISPs keep their logs only for a very short time. There's actually one ISP in Toronto, which at the stroke of midnight, wipes out all the information on its logs and basically starts all over again. Quite often if we're receiving information, such as through CISC which receives the information from other countries, there's a time issue. The information is very time sensitive because a lot of the log information is deleted. So when we get an investigation into the office, whether it comes from inside or outside the country, our first task is to determine how old the information is. Then we have to contact the ISP right away so that it can hold onto its log information. One of the problems we're running into is that certain Canadian-based ISPs store all their information in the United States. One that comes to mind in particular is Rogers. When we go to execute a search warrant at Rogers' corporate offices in Toronto, the information is not at that location. Rogers is, however, putting protocol in place where it can get in touch with its offices in the United States, retrieve the information we're asking for, then when we go to execute the search warrant, we get the information from a Canadian address. So far, it hasn't become an issue in the courts, but some sharp lawyer might come up with that some day.

I do agree with Wayne that there should be some sort of provincial and state regulations for ISPs, and that the mandatory storage time for log information should be much longer. We maintain a backlog of some 35 to 40 child pornography investigations at any given time. One of the other things we review when the information first comes in, is whether or not there's a child that's being victimized at the time. If there's not, unfortunately the case falls down to the bottom of the pile. If there is a child being victimized, it becomes our number one priority. Sometimes, we may not get to an investigation for some six to nine months.

Some of the other areas on the Internet we are having problems with because of the volume are the newsgroups and the Web sites. We're spending most of our time in the IRC channels. I would like to give you a sense of some of the problems we have had in retrieving information. There's one case in particular where we were working on an individual, a 21-year-old man, who was no doubt living off the proceeds of his crime. He was making in excess of US$40,000 per month. He had a Web site that not only offered adult material, obscene material, but also had this link off to the side that offered a vast amount of child pornography. To make a long story short, we completed the warrants, completed our investigation, executed the warrants and found out the information was not actually stored on his premises. He operated the Web site from his premises and stored all the information in New Jersey. We had coordinated an effort with the U.S. Customs office. Perhaps we ended up with a Customs officer who wasn't overly ambitious, but we were never able to retrieve the information to properly prosecute this individual in Canada. As a result, all the charges were withdrawn. The American authorities also told us that, although this Web site contained a large amount of illegal material, there was also a large amount of legal material and they would not be able to shut the system down. Although there are really no concrete guidelines, when we go to execute search warrants now we just shut the whole thing down.

Currently, we receive and send information and other child pornography investigations we uncover in Canada to the U.S. Customs attaché office in Ottawa and to CISC. That system appears to be working now, but I can see problems as well with the volume of information going back and forth.

Another area that I think Wayne has touched on is the transmission of illegal materials. At this time, we do not in any circumstances send child pornography across the Internet to win the confidence of the individual we're working on. If it's an fserve (file server) or an FTP (file transmission protocol) site, and the individual is not sitting at his terminal, sometimes we're able to send a picture of a car or a corrupted file just so we can obtain the credits and can download information off this individual's system. Certain paedophiles and individuals are getting wiser when they're corresponding with us and asking us for information up front. It's just like the old drug trade, when you used to buy drugs off an individual, it would be "you show me some first, before I show you some of mine." When dealing with an fserve you can get away with sending (uploading) corrupted files and that sort of thing.

As a result of only doing child pornography cases in Ontario, we've brought some test cases to the courts in the province, and they've clearly defined what is and is not child pornography.

But what is the Supreme Court of Canada going to say? Across Canada itself, there are certain inconsistencies about what certain people think is and is not child pornography. This leads me to another thing. Something that we should try to work toward is an international definition of what is and is not child pornography. Then maybe gear that up into a system, such as what Wayne was talking about, where you would have a central registry indicating what is and is not child pornography.

Dr. Jacquelyn Nelson

I think a very important issue you raised was the idea of an international definition of child pornography…

Our next presenter is Andrew Oosterbaan.

Andrew Oosterbaan (Panelist) — Deputy Chief for Litigation, Child Exploitation and Obscenities Section, U.S. Department of Justice

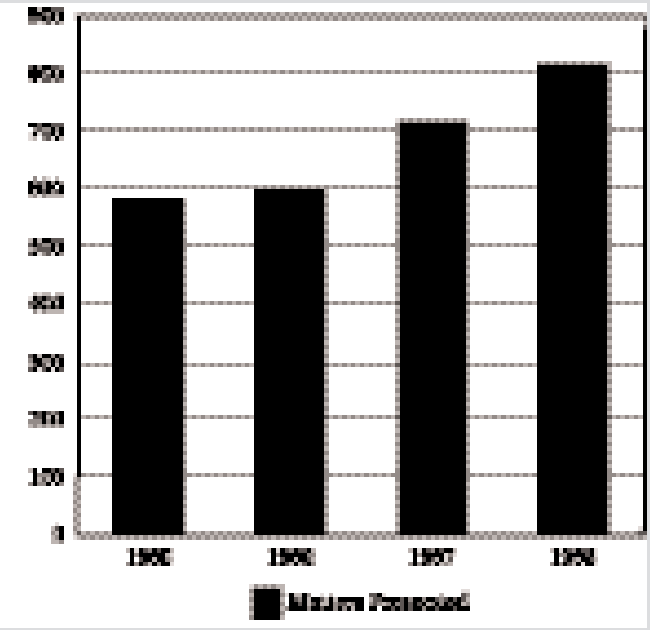
It is a great privilege to be here. This is a tremendous conference, at least in ideology, in what it is intending to do. Whether or not it can do it is another question. What it is intending to do is quite important when you consider the kind of offences we're talking about. I am the American on the panel. I am going to give you what I call the emerging challenges presentation. I think it's particularly appropriate for this conference because one of the greatest challenges we face in the child exploitation area is the fact that Internet crime is borderless. That's kind of easy to say, it's axiomatic actually. That is not the challenge. The challenge is that it's being conducted "among" the borders, it's being conducted among jurisdictions. One of the greatest challenges and complications to the work we do results from the fact that there are so many jurisdictions all over the world dealing with this borderless problem.

Let me tell you a little bit about myself to put this presentation in perspective. I am a prosecutor. My role is one of litigation and litigation support for child pornography prosecutions all over the United States. We also train law enforcement agents, detectives and prosecutors all over the country.

Legislative Review of Proposed Statutes

Congress in the United States depends on a number of people and gets its information from a number of sources, but our section is greatly responsible for the drafting of legislation and proposing legislation that is ultimately enacted in the United States, and of course the development of policy for the current administration.

Growth of Federal Child Pornography Cases



What kind of a problem are we talking about here? It's an immense problem. This graph shows you the growth of the child pornography cases up until 1998, but I can tell you that since 1998 it has grown at a much greater rate.

The CyberTipline

The CyberTipline is operated by the National Centre for Missing and Exploited Children. Between July 1998 and October 1, 2000, the CyberTipline has received more than 27,000 reports. Child pornography accounted for over 22,000 reports. Online enticement of children for sexual acts accounted for over 3,000 reports — basically we're talking about here is luring. This is something we have statutes for. Although we probably could have better statutes, we do have some statutes that take care of it in the United States and many of our prosecutions are online enticement cases. That again gives you some idea of the extent of the problem. When you have that many tips coming in on that line, you know it's a big problem.

Why the Explosion of Internet Crime?

This is an important question when analysing the challenges we face in handling this problem. There is something very unique about Internet crimes, especially child exploitation crimes. Of course, the anonymity offered by the Internet is a big element. These folks are sitting at their computers figuring because of their anonymity they are pretty safe. There's also the satisfaction that they get online. We often joke among law enforcement that if they only knew that at the other end there's frequently a 30- or 40-year-old Federal Bureau of Investigation (FBI) agent, whose online name is Suzi13. In the mind of these folks, they don't care. They're fantasizing about what they're doing. They're fantasizing about who they want it to be, and that's probably about all that matters to them. Now it obviously becomes a crime when it goes beyond that fantasy, and that's of course why we're here.

Critical Questions We Face

Can law enforcement keep pace? Child exploitation crimes are a tremendous problem. It's an immense and very expensive effort. Law enforcement has a hard enough time keeping pace with any criminal effort, but in particular this area, which is driven by technology, which is in fact driven by money.

Will legislation keep pace? This is a particular problem in the United States. I think this is very closely related to the question of whether law enforcement can keep pace. In the United States, the legislative process is very slow. It's very much driven and affected by the will of society. Of course in America, where people value their freedoms above all else, that can be a problem.

Will prosecutors keep pace? This again is closely linked to the first question. It's also a resource issue for them. But often, it's more than a resource issue, it's the "can you teach an old dog new tricks" issue. Will the prosecutor take the time to learn the technology so he or she can handle a case of Internet child pornography?

Will society allow it? Like I said, this is a very important element in the United States, because we're a society that values our freedom above all else. One of the things we consider to be an important aspect of our freedom is our privacy. It's very difficult sometimes to get the proper legislation passed when it's considered to be legislation that has an impact on privacy. There are many, many examples of that. Attempts to enhance our enforcement efforts are very much affected by that last category.

Current Issues

Remote storage. In child pornography cases, the material is often held in a remote storage area that individuals have free access to and can give free access to others. When you're attempting to issue search warrants on the individual it becomes very difficult when you really can't determine where he or she has this material, or once you do, it may be difficult to attain probable cause to get the search warrant to actually search that area.

ISP retention periods. AOL will hold new unopened mail for 28 to 30 days. This is relatively current information, but this information changes very quickly because it all depends on the volume. Mail that has been received and deleted and read mail is going to be held only for a couple of days. When AOL members are chatting in AOL chat rooms, they can hold that IP addressing information for approximately 90 days. Proxy server IP addresses — that's when you have AOL members going outside AOL to do their surfing, chatting, and so forth — you will have that information for maybe seven days. This obviously becomes a major problem for law enforcement. As I'm sure the law enforcement panelists will agree, the ability of law enforcement agents to actually get enough information to start the process in seven days is pretty tough to do.

Encryption. I think it's fair to say with regard to encryption, at least in the United States, in the average case it's not going to be breakable. By the average case I mean one that doesn't have national priority or a

national security interest. If it isn't at that level in the United States, you're probably not going to break it. That means that U.S. law enforcement has to work very hard in a case involving encryption, which is becoming more and more prevalent. For almost every aspect of these kinds of investigations, you need to know right up front that encryption might be an issue and you will need to do an investigation around that. In other words, you may have to find out a way to get passwords up front, especially if you've executed a search warrant and you're talking to the individual you may have to take that opportunity to find out what the passwords are.

Anonymous and Web-based e-mails. These are becoming more and more problematic with respect to investigations because there are companies out there such as "hushmail" and "freedom" which will fully encrypt the e-mail first of all. Then they go through these anonymous re-mailers which makes it very difficult to trace because they'll "scrub clean" the information as it goes from one place to the other. By the time you see it, you have a very difficult time trying to trace where that particular piece of e-mail actually came from. Hotmail is not an anonymous re-mailer system, but we all could create an account completely anonymously within minutes, with completely bogus information, and we'd be up and running and it would make it more difficult for law enforcement to find out who "owns" the account.

Cable connections. This may be more of an issue in the United States than in other countries. The issue here is the connectivity. You are always connected when you have a cable Internet connection. In cases where you're trying to nail down "who connected and when," it becomes difficult because they're always connected. In addition, with regular (phone line) ISPs we can subpoena information from them without ever letting the "bad guy" know we've done it. Unfortunately, with cable law it's different. The ISP has to tell the individual Internet user that we've subpoenaed information from them. Obviously that affects our ability to do things.

Court decisions. We have a two-part system in the United States. We have state laws and of course these laws may differ from state to state for each of the 50 states, and then we have federal laws that cover all 50 states. In order to be a federal crime, there has to be some interstate commerce nexus. Obviously, when you're dealing with computers and the Internet, there's a kind of built-in interstate commerce nexus, but sometimes in a possession case all you have is possession of the material, so where's your interstate commerce nexus? The courts have come down in different ways on this. In some U.S. districts, it becomes more difficult than in others to prove that element.

Proof of the victim's identity can become an issue for us. Despite Congress' best efforts to make images of child pornography not involving a real child (such as morphed child pornography images) illegal, there's at least one Circuit in the United States, the ninth Circuit where California resides, that has said that for an image to be considered illegal it must involve a real child. Therefore, we still, in many cases, must prove that a real person was involved. Again this refers strictly to a child pornography case.

Proof of victim's age. What we are talking about here is proof that the photograph was of a minor.

Sentencing issues. We have good sentencing statutes, but they often rely on enhancements that have to be proven. Sometimes that becomes very difficult. The courts have come down differently with respect to how an enhancement is proved or whether it applies. Of course, as I told you, the state versus federal becomes very difficult. States have their own laws and their own courts, and they do things a lot differently. So when we talk about border problems, we not only have different federal state jurisdictions, we also have 50 state jurisdictions to deal with and they can all be different. We're trying to coordinate and cooperate among law enforcement, which is a critical issue in this area. It is not only complicated among the international community, it is also complicated within the communities in the United Sates.

Meeting the Challenges

Staying abreast of technology is an obvious problem. That's not just among law enforcement as I said before, it's also among prosecutors and judges. As hard as we might try to put a case together and bring it to court, if we have not done a good job of educating that judge, on the record, as to how this all works then we can't hope that the courts on appeal are ever going to figure out why they should come down a certain way with respect to the offence that was committed. So it's very important for all legal authorities to stay abreast of the technology.

Developing software tools. What I'm referring to here is the development of software tools that will help law enforcement. When it comes to integrating the technology with traditional methods of law enforcement, unfortunately, we have a law enforcement framework that's pretty much set. It's important to integrate or adapt the technology that we have for those methods.

Keeping legislation current is very important.

Mutual assistance and cooperation among countries. I can't emphasize that enough, and of course that's why this conference is so important. It's critical when you have offenders who can be all over the world, when they can pass information through points all over the world, when there are different laws in different countries. It's very important that we find a way to work with one another. In our lifetime, we won't see an international police force that will be effective in the way it needs to be to deal with this issue. Interpol does a very good job. My section has been very involved with Interpol and the G-8, but I'm sure that law enforcement will tell you story after story where they tried to rely on Interpol and it didn't work, so we have a long way to go. One of the things that the U.S. Department of Justice does is conduct training programs in foreign countries; I think that's one good way to make this as close to one effort as possible.

Hotlines and tiplines have worked very well in the United States and I believe they can work very well in other countries as well.

Training is very important.

Raising awareness of the child pornography problem among Internet users can also help.

I've put some of the U.S. criminal statutes on the slides in case you're interested and because I think that they're probably different from those in Canada (*see* Appendix II). There is some current legislation requiring ISPs to report potential criminals to law enforcement and we're working out the regulations right now about how that will be done.

Dr. Jacquelyn Nelson

Thank you, Andrew. You certainly raise some interesting questions such as can law enforcement, legislation and prosecutors keep pace? This is something that we all are facing no matter what country we are in. I have to say that it's mind boggling to look at all the different legislative frameworks that you are working with in the United States. At this point, I would like to invite Dr. Taylor to make some comments on the research.

Dr. Max Taylor (Discussant) — University College Cork, Ireland

Speaking at the end of a series of presentations is always an invidious position because all the things you're going to say have already been said, and you're left wondering what on earth to say. Particularly after the people we've heard today who are very experienced and work in this area. Each of their presentations was packed with important and very significant issues.

What I would like to do first is present something about me and the work that we do (within the COPINE project), because this work is unusual. Our set-up is rather unique.

Let me give you some sense of the nature of the COPINE project. We're involved in the assessment of dangerousness and we're interested in adult sexual interest in children as it is manifested on the Internet and the implications of it. We're also interested in child trafficking and child sex tourism. Our particular interest, and this is really what makes our work kind of peculiar, is that we're very interested in the pictures. We're very interested in child pornography pictures because we believe they are the starting point. Because of the nature of Irish law, we're allowed to be in possession of child pornography. We maintain a very extensive database of child pornography pictures. We work extremely closely with law enforcement. We're regularly used as a resource by European law enforcement agencies and sometimes the National Centre and other American agencies for advice, particularly on the identification of new child pornography pictures and for the identification of new children. That, I have to say, is incidental to our business. The database was set up as a research tool and it is maintained because it is a research tool. It just so happens that it also has practical value, but it was never set up for that purpose, and we don't maintain it for that purpose. However, it is gratifying that we can help in investigations and be able to sometimes initiate investigations because we can identify material. We have done that on a number of occasions.

The database exists in two forms. First there's an archive of older material, which is indexed and searchable, but it's not greatly mulled over. By "older material" we mean older than 15 years; by "new material" we mean things up to 10 years; and by "recent" we mean somewhere between 10 and 15 years. Why these figures? Well, because it sometimes takes that long for pictures to emerge. However, I get the impression that the length between production and distribution on the Internet has been shortening. Nonetheless, in many cases pictures can circulate privately among individuals and they never get out until later on.

The second form the database takes is a searchable archive of new and recent material. About three or four years ago, Swedish police developed a searchable

archive based on software recognition. However, our database works on text-based descriptors. We use the FBI text descriptors. We did this for a number of reasons. First, we didn't have the money to invest in the software anyway, but I also feel very sceptical about the value of face recognition software now, and did even more then. We actually commissioned a computer specialist to look at software recognition programs for us, but the outcome was quite limited. The EXCALIBUR database that the Swedish police use certainly works very effectively; however it's not 100 percent reliable, it's nowhere near that. We do our work by visual inspection. So it's very labour intensive, it's tedious, and it's not very pleasant because you have to look at everything, but we find it works.

The database is made entirely of material that is posted and lifted from newsgroups. We regularly monitor postings to 60 newsgroups and download postings automatically. We also receive material from law enforcement agencies.

To categorize the child pornography, we have a system that we've developed which relates to scale of victimization. We focus on levels 6 to 10. Levels 6 to 10 are basically pictures involving sexual assaults. Child pornography at its worst is a picture of a commission of a crime, a picture of the scene of a crime. I think we have to remember that it's a picture of a very serious sexual assault. It's not some pretty picture, it's not somebody's fantasy, it's some real child being abused and photographed.

Our database underestimates the more mature children of 12 or older because we use anthropometric measures to identify and describe facial and bodily characteristics. It's very difficult once you get past puberty to be accurate about ages. So our database fizzles out at that age, and we have very little in that area.

We focus on new photographs and we have very extensive knowledge now of what is new. We probably now have in the database a very large and probably representative sample of the available material. How do I know that? I really don't, but I do know that there's quite a lot of it. The database has extensive records of pictures, probably nearly all the material that's being posted to the newsgroups that we've monitored over the past three years. We also have records of nicknames and posting IP addresses.

Here's a sample of what one of the records in the database looks like (*see* Appendix III). It describes qualities of the picture and so forth, and one of the topics is details, for example, description of environment. This picture is obviously not a picture of child pornography, but I do believe that this child is a child at risk, because that picture came from a child pornography newsgroup. We have obtained this picture, not because it is illegal, but because our gut feeling is that an illegal picture of this child may appear later on. We've been right on a number of occasions about this as well. You have to ask yourself, "Why are 20 or 30 pictures of this child posted to a child-sex newsgroup?"

The database consists of approximately 60,000 still pictures and 400 plus video clips ranging from a few seconds to our longest, which is about 20 minutes. The video clips are not very manageable. They're too big. They're not really a big area of trade at the moment. However, as compression technology improves the video clips will become increasingly important and we'll see many more of them. For the moment though, the overwhelming amount of material is still pictures. Of the 60,000 still pictures that we have, about 43,000 are of girls and about 18,000 are of boys. About 7 percent of the very obscene girl photographs are new, and about 26 percent of the very obscene boy photographs are new. I think that represents our experience. There's much more new boy material coming out than new girl material.

The slide (below) of the age range gives you a sense of what the new/recent photographs look like by age. As you can see, 7 percent of the girl photographs fall in the 13- to 15-year-old age category and none falls within the 15- to 17-year-old age range. Now that, of course, is absolute nonsense. There are, of course, thousands and thousands of pictures in these age groups, we just don't monitor them because we can't be sure about the age of the children in this range. So we stop around 12 years old or so. With boys we can be more accurate because puberty in boys is delayed somewhat. The predominant age group would be 9 to 12. But the really worrying thing about the numbers is that 10 percent of the images are of babies and toddlers.

Age Range of New/Recent Images

Age of children	Percentage of girls in still images	Percentage of boys in still images
0–2	10	1
3–5	21	3
6–8	21	19
9–12	41	56
13–15	7	14
15–18	0	7

The race of the children in these photos is predominantly white. What always surprises me is that there are very few Black children, almost none. But what we know about sexual abuse of Black children is that it occurs more or less as frequently as it does for white children, but Black kids just don't get photographed, or at least they don't appear on the Internet.

The age distribution of children in the video clips looks pretty much the same as the photographs. The predominant age group is between 9 and 12.

We are downloading approximately two new individual children a month on average; that is, approximately two new children a month are appearing in the newsgroups. However, the appearance of new pictures is very irregular. Some months there's nothing, sometimes we get a flood of them. People often ask me how much child pornography is there in existence? I think that this is a nonsense thing to ask. The origins of a lot of the material are videos. A lot of what we are seeing are video captures of the new stuff. From a 30-minute video you can take 1 to 5,000 video captures. Therefore, it just doesn't make sense to talk about the amount of the material, but it does make sense to talk about and focus on the number of children. Our impression is that the ages, especially among girls, are getting younger and younger. They are invariably, not exclusively, but nearly always very domestic in quality. The pictures are taken in houses, in bedrooms, and in children's bedrooms. What is very alarming is the growth in the number of east European children who have been appearing in the last few years.

We reckon that in our new database there's somewhere between 300 and 350 children who would be included in the new/recent category. So for pictures created in the last 10 years, we have visual records of 300 to 350 children being very seriously sexually assaulted. There are about 220 boys and about 130 girls. It's not always easy to tell the people in the pictures apart. You can have the same child with multiple pictures of them. However, you can never be certain that the pictures are of the same person because of distortions from picture to picture. Of the girls we have in our database, we know the identity of about 12 of them because the cases have been solved. Of the boys, we know the identities of somewhere between 2 and 12. I say somewhere between because there's been a recent case of seizure in Italy of pictures of boys from Russia and that will affect these numbers.

In addition to that we have somewhere between 1,600 and 1,800 pictures of children who were photographed while they were naked. These are not sexual pictures in the sense that there's an adult in the picture doing something to the child, but these are posed pictures. In many jurisdictions these kinds of pictures will be illegal, but not in all. It's a reasonable assumption that many of these children are also sexually abused. Either you've not seen the pictures of them or there weren't pictures taken. So what I've shown you there, I think, is a massive underestimate of the number of children involved, but this is the material we have.

I think it's important to stress that our impression is that the Internet is, at the moment, primarily a medium of distribution, not a medium of production. I think video remains the primary production medium. The Internet reflects this through video captures. The kg (kindergarten) series is an example of that. The kg series consists of pictures of about 30 little girls between 18 months and 6 years old. There's somewhere between 3,000 and 4,000 pictures of them around on the Internet. They've been around for a number of years, but new pictures are being added to the series. There was a recent burst of new pictures about a month ago, which were very obscene pictures of one of the little girls in this series. This is a major example, it seems to me, of serial child pornography production where a lot of little girls are being subjected to very serious sexual assaults.

Child pornography is very easy to find on the Internet, although you're unlikely to stumble across it. We look in the newsgroups and we used to look in IRC. IRC is open to the public, but there are private password-protected channels. On IRC, you've also got secret/invisible password-protected channels. You've also got server channels on IRC, which still exist; "W0nderland" was one of them.

Bulletin boards (BBSs) are very important, particularly the web-based BBSs. They're important because they give the location of Web sites to find child pornography, but even more important than that they're a medium of communication among people. The issue about the Internet and child pornography is not just that there are pictures on the Internet and that these pictures are obscene; the issue is that the Internet entwines with adult sexual interest in children, and generates, sustains and develops that interest. Talking to people is as important in this world, in the development of adult sexual interest in children, as the pictures are themselves. Web pages are also a source of the material. I still believe that what we're looking at in child pornography is a massive international conspiracy. But unlike most conspiracies, it's not driven predominantly by money. Money is made out of it from time to time, but it's not characterized by money. Why

pay, when you can download so much for free off the newsgroups? We're downloading somewhere between 5,000 and 7,000 pictures a week, of which about 1,000 are child pornography. It's mainly all older material. By older material I mean material such as scans from the old *Lolita* magazines and material that was produced when production and possession of child pornography was legal in a number of European countries about 30 to 40 years ago. It's the new material that's important, however, because it represents a current child protection problem.

I would like to make one or two other points. I just wanted to go through the previous points because I think it's important just to see what the scale of the problem is. We always say that there's a lot of material; this shows you an overview of the sample that we have. Although it's not exhaustive, it's reasonably representative of our record.

What are the priorities? What comments can we make about the presentations today? I think the first comment that has to be made is that investigations must have a child-centred focus. You've heard from the police presentations that they do that and they quite clearly regard new pictures as being a priority. But what follows from that, is that if you go to investigate these cases you're going to have to devote enormous resources to them because the investigation isn't easy.

We were involved in one investigation surrounding a series of pictures. This investigation took about a year to complete. The pictures were taken by the girl's father and he received about 12 years for it just this year. The pictures had emerged on the Internet about a year before. The pictures were traded on IRC not long before they emerged in the newsgroups. So this was lucky because this material emerged and he was caught quite quickly. They took a year to track the offender down. He was located in the south of England and there was evidence in the pictures that confirmed that location and their recency. But actually getting him involved a major investigation. What's interesting is that the information that led to his apprehension came from U.S. Customs which was monitoring IRC. This is an interesting example of the border issue. Here we had a child being abused in England, her father was trading the pictures in America, the IP address was identified, it was transmitted to the United Kingdom, and he was caught. However, he was caught by luck. First, he was caught because someone was monitoring what was going on. Secondly, he was caught because the ISP, when approached for the IP address, by chance had retained it for something like eight months. It didn't have the month before or the month after, but it did have the information for that date. It was total chance that they got him.

This just reinforces the role of ISPs — the significance of the retention of information. Terry Jones from Greater Manchester Police, who pursued that investigation in the face of considerable adversity, deserves enormous credit. And that raises another problem: Who "owns" these investigations? From the evidence in the pictures we knew that the girl in the material was English, but we had no idea where she was. So which English police force would own the investigation in this case? Greater Manchester Police took up the case against considerable aggravation from the Chief Constable who wanted to know why they were spending money on something they didn't know was a problem in Greater Manchester. They were lucky again, because it worked out the man was caught. But if he hadn't been caught, they would then have had to account for the years of very hard work without ever doing anything for Manchester, or maybe not doing anything for anybody. These investigations are hugely resource intensive and that must be recognized.

So the child focus is important and all the speakers have recognized that. Retention of logs is vitally important. I would certainly say that the ISPs should hold the logs longer than three months, but whatever is practical because of the cost-benefit aspect must be worked out.

Coordination and cooperation among police forces is absolutely vital. Interpol provides that forum to some extent. Interpol is itself constructing a database of child pornography. We, and the Swedish police, have supplied them with all our new material. I know that the Interpol database will be functional, but the problem will be maintaining it. If it is not maintained, it will be useless. It will require somebody working on it all the time. We have three people running our database. They do other things as well, but they spend hours upon hours just sorting through the pictures. It's very labour intensive and very unpleasant for the students we have working on it. Here again it's an issue of resources.

There are major training implications in all of this. Not just training for law enforcement, but for all the agencies involved, such as probation, social workers and prosecutors. Lots of people need to be trained and made aware of what the problems are. We are currently involved in the process of interviewing a lot of offenders. One of the things we're continually coming across is the inadequacy of the social welfare system and the probation service to deal with the offenders and their problems. Those working in the system need help

because they don't understand how the Internet works. They don't understand what the problems are. They don't even know, when interviewing an offender, what the right questions are. They're reluctant to get involved because they're worried that the offender is going to know more than they do. They're worried that they will look bad and not even make the right comments. Training for parents is important as well. Because the bottom line is that parents need to be aware of the risks their children face. They need to be aware of the potential of the Internet. When your husband is sitting there three to six hours a night playing on the Internet, what is he doing? Children need to be made alert to the dangers they might face looking on the Internet. So there's an issue of parental regulation, but the bigger issue is self-regulation by the ISPs.

All of this could be controlled if the ISP industry wanted to control it. It only happens because it's allowed to happen. If somebody decided that it wasn't going to happen then it wouldn't happen — because you could control it in better ways than how it's being done now. The technology is there to be able to do that. So the issue does come back to the ISP industry, which enables and allows it to happen. This is really something that we all have to address, not just in Canada and the United States.

There are many other issues as well. There are issues having to do with age and all sorts of other complicated issues. There is much work being done on the relationship between adult sexual interest in children and the Internet, and the way that the Internet sustains this interest. Related to this is the issue of the development of dangerousness and the identification of dangerousness among offenders. It's important to realize that not all sexual offenders against children collect child pornography, and not all collectors of child pornography assault children. Knowing and understanding where the boundaries are, and understanding the dangerousness of individuals, is a major challenge. Recognizing the guy whose been caught in possession of child pornography might well be a liability in going farther. Distinguishing this person from somebody who isn't going to do that or is unlikely to do that, for whom the boundaries are reasonably well established, is a big problem in the management of offenders. These are just a few of the issues that need to be addressed.

Appendix I: Questions and Discussion

Dr. Jacquelyn Nelson, Senior Policy Analyst

Thank you to everybody. At this point I'd like to open the floor to questions, comments or observations. It's been a lot to comprehend and take in, but I found it very interesting.

Myron Claridge, Crown Counsel, Ministry of Attorney General of British Columbia

What we hear from ISPs is that they can't afford to keep logs of their clients longer than just a very short period of time. What's the answer to that?

Dr. Max Taylor

You'll hear the industry say that it's not making money these days. Now I don't think that's true, but we expect agencies to exercise social responsibility. It would not be acceptable in any other setting for a commercial organization to facilitate the commission of a crime. But that's what's happening here. So I think the ISP industry really has a duty to make adequate provisions to address this problem. There is a big issue, which I'm very aware of, of the international level of the dilemma of encouraging the development of e-commerce, for example, and the requirements of freedom, which are very important. Then there's the management of the problems like we're discussing. There's a bit of a tension there, but I still think the ISP industry has a social responsibility.

Dr. Jacquelyn Nelson, Senior Policy Analyst

Dr. Taylor, you've mentioned self-regulation, why self-regulation of ISPs?

Dr. Max Taylor

It seems to be, in principle, better to have organizations regulate themselves. It's a mark of maturity. After all, that's what professions do. Doctors regulate themselves; they may not do a very good job of it, but they do. Solicitors regulate themselves. It's meant to be a sign of maturity. It's cost-effective as well. It gives the ISP industry the opportunity to influence things in ways that would maximize the regulatory process to its benefit. So I think self-regulation in that sense is desirable to move to. If you talk about regulation of ISPs, you have to talk about regulation on a much bigger scale than a national scale. But first of all, you need to address the national issues and deal with that. There's also an international problem. I don't know how that could be dealt with except through a UN agency or another large agency such as that. However, that also would necessarily need to be a consensus-based activity. You're not going to be able to impose views on the ISPs from other countries.

Sgt. Emmett Milner

We met with a group of ISPs about three weeks ago. One of the points that came out of the discussion was that a lot of the ISPs are not aware of what's expected of them from law enforcement. I think we pushed that idea forward. We're working with the Canadian Association of Internet Service Providers (CAIP) and this group does have a code of conduct for their clients. We're trying to assist the ISPs in letting them know what law enforcement wants. That's one positive step we've taken. In May 1999, the CRTC (Canadian Radio-television and Telecommunications Commission) decided it was not going to regulate the ISPs so that put us a bit behind the eight ball for the time being. Unfortunately, it may take someone getting hurt before something actually happens.

Det.-Sgt. Wayne Harrison

I find it hard to believe that there's no responsibility for an ISP that knows that some of the newsgroups they're providing access to are titled, for example, alt.sex.paedophilia.girls. To me, if that's a newsgroup that's being channelled through their service, they're involved in the distribution of child pornography. I don't see how they could avoid any type of responsibility for this.

Dr. Max Taylor

But then certainly you don't prosecute the postal service when it carries obscene mail, because it is a common carrier. We've also heard claims from ISPs that they also have this status.

Andrew Oosterbaan, Deputy Chief for Litigation

There are companies like AOL and Microsoft which are doing a pretty good job in monitoring and policing themselves, and they are looking for guidance from law enforcement on what it is they should do with the information they get. But then we have so many ISPs that don't fall into the same category as AOL and Microsoft, which are not going to police themselves as well no matter what we do and no matter what the body of self-regulation would be. So the issue is multidimensional. I've been in meetings with security people from AOL and Microsoft, and they tell us, "You know they come back up just as quick as we take them down. We take them down, they come back up. We take

them down, they come back up." So we're trying to work out a method by which they give to us the information that we need to try to prosecute the folks and hopefully terminate that endless process. I've been to the same meetings where I was told that we can give them the information but they don't have the resources to deal with the problem. There are hundreds that pop up on a daily basis and it really is too much for a law enforcement agency to handle. We have statutes and regulations that are being implemented now and we'll just have to see how it goes.

Myron Claridge, Crown Counsel

What is the penalty for not following the legislation?

Andrew Oosterbaan, Deputy Chief for Litigation

The statute was set a long time ago and we have yet to implement the regulations. I think we're going to find that it will be very easy to deal with the big ISPs and difficult to deal with the smaller ones.

Dr. Jacquelyn Nelson, Senior Policy Analyst

We'll have to wind up now. I would like to thank everyone for their presentations.

Appendix II:
Presentation Materials

Andrew Oosterbaan
Deputy Chief for Litigation

Internet Crimes Against Children

The Emerging Challenges

Presented by:
Andrew G. Oosterbaan, Deputy Chief
Child Exploitation and Obscenity Section
U.S. Department of Justice

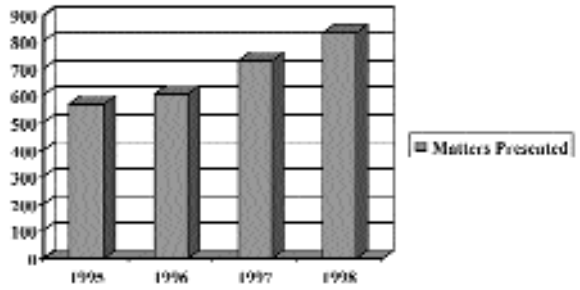
1

U.S. DEPARTMENT OF JUSTICE
CHILD EXPLOITATION SECTION

- Litigation and litigation support for child pornography prosecutions
- Training of law enforcement and prosecutors
- Legislative review of proposed statutes
- Development of policy

2

Growth of Federal Child Pornography Cases



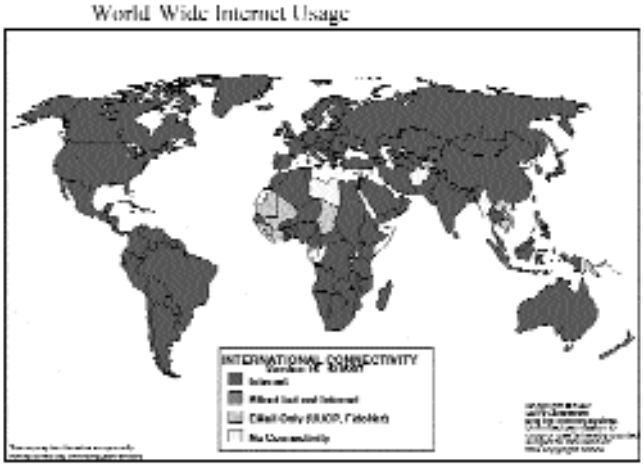
3

www.cybertipline.com

- Sponsored by the National Center for Missing and Exploited Children
- Total Reports received on CyberTipline (7/1/98 10/01/00) = 27,821
- Child Pornography = 22,638
- Online Enticement of Children for Sexual Acts = 3,012

4

World Wide Internet Usage



5

WHY THE EXPLOSION OF THESE INTERNET CRIMES?

Anonymity
Immediate Satisfaction
Fantasy
Exploration

6

Emerging Technology Creates Significant Challenges

- Can Law Enforcement keep pace?
- Will legislation keep pace?
- Will prosecutors keep pace?
- Will society allow it?

7

Current Issues

- ISP retention periods
- Remote storage
- Encryption
- Anonymous E-mail
- Web-based E-mail
- DSL/Cable Connections
- Explosion of Internet offenders
- Court Decisions

8

Retention Periods

- New Mail – 28-30 days
- Deleted Mail – 2 days (Aol 5.0 only)
- Read Mail – 2 days
- Member IP addressing – 90 days
- Proxy Server IP Addresses – 7 days

9

Encryption

- Is it breakable?
- Exportable
- Use is spreading

10

Anonymous E-Mail / Web-based

- Hushmail
- Freedom 1.0
- Hotmail

11

DSL/Cable Connections

- Always on
- Cable laws are different

12

Court Decisions

- **Interstate Commerce in Federal Court**
- **Proof of Victim's Identity**
- **Proof of Victim's Age**
- **Sentencing**
- **State v. Federal: A difficult dichotomy**

13

Meeting the Challenges

- **Staying abreast of technology**
- **Developing software tools**
- **Integrating technology with traditional methods of law enforcement**
- **Keep legislation current**
- **MUTUAL ASSISTANCE & COOPERATION AMONG COUNTRIES**

14

US Investigative Agencies

- US Postal Inspection Service
- FBI
  - Innocent Images Operation
- US Customs Service
  - Customs Cybersmuggling Center, Fairfax, VA
  - Field offices around the US

15

International Working Groups

- Critical need for nations to realize (1) the international nature of many online offenses against children and (2) the need for international cooperation to effectively combat these crimes
- CEOS has created relationships with Interpol member nations and agencies participating in the global effort against online offenses that victimize children

16

International Partners

- Interpol Specialist Group on Crimes Against Children

  Subgroup on Computer Technology
- Group of Eight Industrialized Nations

17

Vienna Commitment against Child Pornography on the Internet

- **Issued October 1, 1999 at the Combating Child Pornography on the Internet conference in Vienna, Austria**
- **Broad range of participating nations and organizations**

18

Best Practices and Recommendations

- Zero tolerance against child pornography on the Internet
- Need for global partnership among all stakeholders
- Worldwide criminalization of child pornography so that no safe haven exists for pornographers
- Improving international law enforcement cooperation

19

Recommendations

- Closer cooperation between governments and the Internet industry
- Encouraging establishment of more Hotlines and Tiplines
- Continued law enforcement training among partner nations
- Raising awareness of child pornography problem among Internet users

20

Some Important Needs

- Additional training for law enforcement and prosecutors focusing on:
  - keeping pace with changing technology
    increasing the use of Mutual Legal Assistance Treaties and extradition as tools of international enforcement
- Ongoing revision of most effective methods of fighting online crimes against children

21

U.S. Criminal Statutes

- **Production of Child Pornography**
- **Transportation, Importation, Receipt, Distribution of Child Pornography**
- **Possession of Child Pornography**
- **Production for Importation**
- **Reporting by ISPs**
- **Transfer of Obscene Materials to Minors**
- **Use of Interstate Facility to Transmit Information About Minor**
- **Travel / Transportation Statutes**

22

Production of Child Pornography

- **18 U.S.C. § 2251**
  - **Employing, using, persuading, inducing, etc. a minor to engage in or assist in sexually explicit conduct for the purpose of producing a visual depiction, IF subject knows or has reason to know the depiction will be transported or mailed, or it goes interstate.**
  - **Parents liable for permitting.**
  - **Notices or advertisements are a violation.**

23

Production Jurisdiction Expanded

- **Effective 10/30/98, now includes a 3rd jurisdictional avenue:**
  - **If the depiction was** produced using materials **that have been mailed, shipped or transported in interstate or foreign commerce.**

24

Transportation/Shipping, Receiving/ Distributing Child Pornography

- 18 U.S.C. §§ 2252 & 2252A
  Transporting/Shipping involves carrying or uploading [2252(a)(1) & 2252A(a)(1)].
  - Receiving/Distributing involves images that have already moved interstate [2252(a)(2) & 2252A(a)(2)].
    - 2252 > visual depiction
    - 2252A > child pornography

25

Possession of Child Pornography

- 18 U.S.C. § 2252(a)(4)(B)
- "matters"
- "visual depictions"
- 18 U.S.C. § 2252A(a)(5)(B)
- "images"
- "child pornography"

26

Possession – a Federal Nexus

- Either the depictions traveled in interstate or foreign commerce; OR
- The materials used to produce the depictions traveled in interstate or foreign commerce.

27

Production for Importation

- 18 U.S.C. § 2260
  - Person outside the U.S.
  - Produces (2251(a)), trafficks (2252), or possesses (2252) with intent to import into the U.S., or into waters within 12 miles of the U.S. coast.

28

Reporting of Child Pornography by ISPs

- 42 U.S.C. § 13032
  - ISPs must report child pornography occurring on their system;
  - As soon as reasonably possible after obtaining knowledge of facts or circumstances of an apparent violation of the child pornography statutes;
  - Penalty is a fine.
  - Monitoring is not required.

29

Transfer of Obscene Materials to Minors

- 18 U.S.C. § 1470
  - Use of mail or any facility of interstate or foreign commerce to knowingly transfer obscene matter to a minor under age 16.
  - Includes attempt.
  - Must prove defendant's knowledge of minor's underage status;
    Penalty: up to 10 years.

30

Use of Interstate Facility to Transmit Information About Minor

- 18 U.S.C. § 2425
  Using the mail or any facility or means of interstate or foreign commerce;
  - To knowingly transmit biographical info or e-mail address of an individual under age 16, with intent to entice, etc.
  - Defendant must know person is under 16;
  - Includes attempt.
  - Penalty: no more than 5 years.

31

Other Federal Statutes

- Buying or Selling of Children (18 U.S.C. § 2251A)
- Forfeiture (18 U.S.C. § 2253)
- Record Keeping Requirement (18 U.S.C. § 2257)
- Communications Decency Act (47 U.S.C. § 223)
- Obscenity Statutes (18 U.S.C. §§ 1460 –1466)

32

Traveler Case Example

- What is a "traveler"?
  - Person who crosses state lines for illegal sexual activity
    - Travel by either victim or defendant
    - Also includes when defendant entices victim to travel
  - Sexual contact defined by state or federal law, depending on statute used
  - Age defenses vary depending on statute used

33

Potential Federal Charge(s)

- 18 U.S.C. 2421: transporting any person across state lines with intent such person engage in prostitution or any criminal sexual activity.
- 18 U.S.C. 2422(a): persuades, induces, entices, coerces any person to travel to engage in prostitution or any criminal sexual activity.

34

Potential Federal Charge(s)

- 18 U.S.C. 2422(b): using any facility or means of interstate commerce to persuade, induce, entice, or coerce a person under 18.
- Specific intent crime
- Defendant must know that victim is under age 18, but gov't need not prove defendant knew exact age.

35

Potential Federal Charge(s)

- 18 U.S.C. 2423(a): transporting a person under age 18 with the intent that the minor engage in prostitution or any sexual activity for which a person can be charged.
- Intent must be formed before crossing state lines.
- Defendant must know victim is < 18, but gov't need not prove defendant knew victim's exact age.

36

Potential Federal Charge(s)

- 18 U.S.C. 2423(b): travel to commit a sexual act with a person < 18 that would be a violation of Chapter 109A if occurred in particular jurisdiction (basically on federal property).
- Intent must be formed before crossing state lines.
- Def. must know victim is < 18, but need not know exact age.

37

Thank You

Drew Oosterbaan

Andrew.Oosterbaan@usdoj.gov

Child Exploitation & Obscenity Section

www.usdoj.gov/criminal/ceos

38

Appendix III: Presentation Materials

Dr. Max Taylor

Child Pornography, the Internet and Offending

Professor Max Taylor
COPINE Project
Department of Applied Psychology
University College Cork

COPINE Project

1

Overview

- COPINE Project
- Child Pornography
- Offenders and Offending
- Virtual Community
- Thoughts and concerns

COPINE Project

2

COPINE Project Background

- Grew out of Child Studies Unit
- Reflected a concern with child protection issues arising from new technologies

COPINE Project

3

Project Activities

- Child Pornography
  - Assessment of dangerousness
  - Understanding qualities of offending and offenders
  - Evidential analysis of pictures
  - Identification of victims
- Nature and incidence of child sex tourism and child trafficking

COPINE Project

4

Distinctive features of the Project

- close association with law enforcement
- emphasis on forensic/evidential value of pictures
- focus on engagement with Internet
- COPINE database
  - pictures
  - posting histories

COPINE Project

5

What is child pornography? Irish Law (1)

- (a) any visual representation
  - (i) that shows or, in the case of a document, relates to a person who is or is depicted as being a child and who is engaged in or is depicted as being engaged in explicit sexual activity* * [n.b. not obscenity]

COPINE Project

6

Irish Law (2)

- (ii) that shows or, in the case of a document, relates to a person who is or is depicted as being a child and who is or depicted as witnessing any such activity by any person or persons, or
- (iii) whose dominant characteristic is the depiction, for a sexual purpose, of the genital or anal region of a child,

COPINE Project

7

Irish Law (3)

- (c) any visual or audio representation that advocates, encourages or counsels any sexual activity with children …., or
- (d) any visual representation or description of, or information relating to, a child that indicates or implies that the child is available to be used for the purpose of sexual exploitation ……..

COPINE Project

8

Interpol Standing Working Group on Offences against Minors

- Child Pornography is the consequence of the exploitation of sexual abuse perpetrated against a child……any means of depicting or promoting sexual abuse of a child, including print and/or audio, centred on sex acts or the genital organs of a child.

COPINE Project

9

Legal vs. Offender perspective (1)

- Taylor (1999) "...whilst legal definitions are …. important from legislative and judicial perspectives, approaching child pornography as a legal problem does not ... help our understanding of why child pornography is produced or collected- legal definitions do not tell us about its nature…the issue of producing and collecting child pornography is essentially a psychological, rather than a legal problem".

COPINE Project

10

Legal vs. Offender perspective (2)

- Dilemmas
  - legal specification necessary for law enforcement management of problem
    - problem of 'good' and 'bad' offenders
  - wider psychological perspective necessary for understanding and control of problem
    - problem of becoming 'thought' police

COPINE Project

11

Child Pornography

- Neither pictures nor collections are accidents
- Result from deliberate choices made by an individual to acquire and retain sexual material
- Not all material collected will fall into legal definitions of child pornography, yet may be as sexually arousing to the individual

COPINE Project

12

Child Pornography

- Not homogeneous
  - variety of different kinds of images attractive to adults with a sexual interest in children
- Typology of pictures collected
  based on COPINE reference database
  central focus - increasing sexual victimisation
  - 1 10 point scale of increased deliberate sexual victimisation

COPINE Project

13

Typology
(may not be illegal)

- Level 1 Indicative
- Level 2 Nudist
- Level 3 Erotica
- Level 4 Posing
- Level 5 Erotic Posing

COPINE Project

14

Typology
(probably illegal)

- Level 6 Explicit Erotic Posing
- Level 7 Explicit sexual activity
- Level 8 Assault
- Level 9 Gross Assault
- Level 10 Sadistic/bestiality

COPINE Project

15

Dilemmas

- Legal definitions do not necessarily include all sexually arousing photographs
- Problem of level 3 pictures (surreptitiously taken photographs)

COPINE Project

16

Typology - other factors in extent and severity of sexual victimisation

- size of collection and quality of organisation
- new/ private material
- age of child

COPINE Project

17

COPINE Database

- Database takes 2 forms:
- 1. Archive of old pictures (over 15 years)
- 2. Searchable archive of new/recent pictures (new= 10 years old, recent= 10-15 years) collected from daily newsgroup downloads
  searchable by text fields

COPINE Project

18

COPINE Database (2)

- Based on daily systematic downloading of all pictures posted to 60+ newsgroups known to carry child pornography
- Focus on levels 6 10 photographs (underestimates more mature 12+ photographs)
- Focus on new photographs
- Large and probably representative sample of publicly available material

COPINE Project

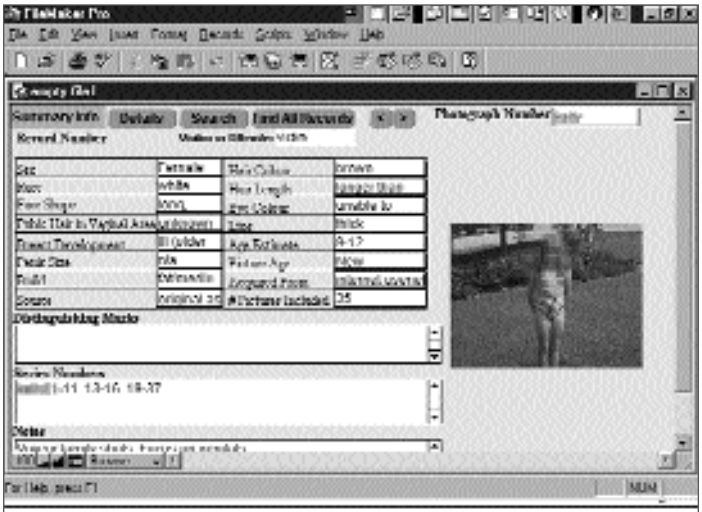
19

COPINE Database (3)

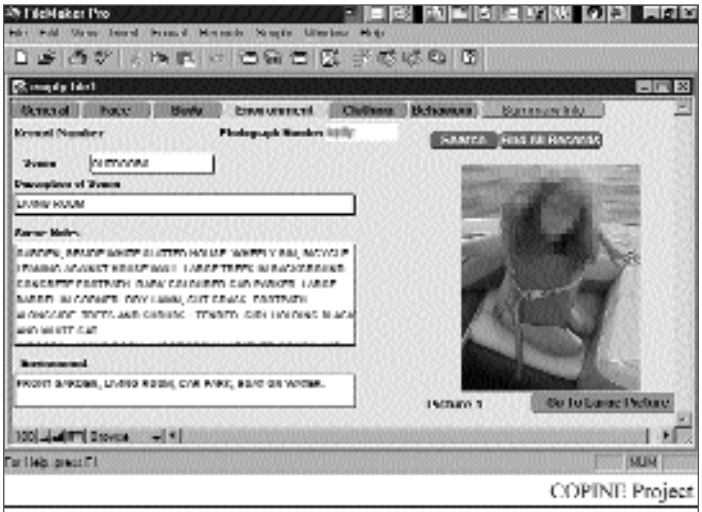
- Extensive record of pictures posted over 3+ years
- Extensive record of nicknames of posters and IP addresses

COPINE Project

20



21



COPINE Project

22

COPINE Database (4)

- 60,000 + still pictures
- 400 + video clips (5-6 secs. to 20 mins)
- about 43,000 pictures of girls, 18,000 pictures of boys
- about 7% of girl photographs (levels 7+) are new
- about 26% of boy photographs (level 7+) are new

COPINE Project

23

Age range: new/recent

Age of children	Percentage of girls in still images	Percentage of boys in still images
0 2	10%	1%
3 5	21%	3%
6-8	21%	19%
9-12	41%	56%
13-15	7%	14%
15-18	0%	7%

COPINE Project

24

Race of children: new/recent

Race of Children	girls	boys
White	70%	90%
Asian	23%	6%
Hispanic	7%	3%
Black	0%	1%

COPINE Project

25

Ages of children: new/recent video clips

Age of children	girls	boys
0-2	1%	0%
3-5	4%	0%
6-8	39%	0%
9-12	56%	92%
13-15	0%	8%
15-18	0%	0%

COPINE Project

26

New photographs (1)

- Downloading approx. 2 new individual children/ month on average - varied and very irregular
- Ages are getting younger (especially girls)
- Domestic quality
- Growth in East European children

COPINE Project

27

New photographs (2)

- Estimate 300 - 350 children included in new/recent category subjected to serious sexual assaults - about 202 boys and 130 girls (individual identities not always clear)
- of the 130 girls, the identities of 12 are known
- of the 202 boys, we are definitely aware of identities of 2, and maybe a further 12 are known

COPINE Project

28

New photographs (3)

- 1,600-1,800 children photographed whilst posing naked - it is reasonable to assume some of these will have been sexually assaulted without being photographed or photographs not distributed
- These are underestimates of the numbers:
  - usenet tip of an iceberg of privately circulated material

COPINE Project

29

The significance of videos

- Important to stress Internet at the moment a distribution medium
- Video remains principal primary production medium
- Internet reflect this through video captures
  - kg series

COPINE Project

30

Where does child pornography come from on the Internet? (1)

- Easy to find, but unlikely to stumble across it:

  Newsgroups

  IRC
  - public
  - private (password)
  - secret (invisible and password)
  - server channel (e.g. w0nderland)

COPINI Project

31

Where does child pornography come from on the Internet? (2)

- Bulletin Boards (BBS's)
  - dial up
  - web based (e.g. PGB)
- email and similar protocols
  - icq
- World Wide Web
  - free servers
  - commercial involvement
- Video conferencing
  - CU-seeme

COPINI Project

32

Who looks at child pornography?

- Unknown
- Guess many thousands of people:

  active participants posters, producers

  passive viewers

COPINI Project

33

Offenders and Offending

- Ongoing series of interviews with offenders:
  - downloaders (no assault)
  - downloaders and assault (no production)
  - downloaders and distribution (no assault)
  - downloaders and producers (assaults)

  downloaders, producers and distributors (assaults)

  sexual assaults

COPINI Project

34

Offenders and Offending

- Emergent interview themes:
  - offending behaviour
  - setting events

    initial engagement with Internet

    engagement with Internet
  - process of collecting
  - virtual relationships to real relationships

COPINI Project

35

Offenders and Offending

- Analysis of interviews involves:

  thematic analysis to establish broader picture

  discursive analysis of individual to look at how individuals negotiate their accounts

  Supplemented by police records, interviews with probation officers, social workers, spouses

COPINI Project

36

Quotations from an interview with the creator of 'w0nderland' (1)

- "The Internet was basically a doorway…..to the dark side." → focus on medium
- "I lost my best friend when I lost my computer." → focus on individual

COPINE Project

37

Quotations from an interview with the creator of 'w0nderland' (2)

- "It's kinda like an art collector who finds a lost Picasso…." → focus on collection
- "I'm like a virtuoso pianist…….but the instrument I play is a computer"→ focus on computer skills

COPINE Project

38

Quotations from an interview with the creator of 'w0nderland' (3)

- "It was the most important thing to me…. I had almost no friends in real life and what few friends I had……..I kept at arms length" → focus on centrality of Internet experience to everyday life

COPINE Project

39

Appeal of the Internet

- changes communication patterns - self-present from relative safety
- social contact can be anonymous (lessen risk and lowers inhibitions)
- can try out new ways of relating, roles identity and even gender
- allows for the control of presentation

COPINE Project

40

Appeal of the Internet

- social connections can vastly expand
- communities provide safe haven and yet can control social distance and intimacy
- allows sense of mastery and increase in status and prestige
- such skills generate a sense of power
- users gain social confidence
- suggestion of altered states of consciousness

COPINE Project

41

Why is this a problem in relation to sexual interest in children?

- Increased socialisation allows for normalisation of interest
- Enables engagement through reduction in outside social contacts which might otherwise challenge the acceptability of the interest

COPINE Project

42

Avoidance of personal responsibility

- allows for the safety of anonymity
- facilitates identity choices
- allows for the movement through identities

COPINE Project

43

Impact on sexual behaviour

- Lowers sexual inhibitions and engagement in sharing/trading acts as a form of strong social reinforcement
- increases level of actual sexual activity, both in relation to pictures and text
- places emphasis on control, in relation to production and manipulation of materials

COPINE Project

44

Participation in a community

- Offender gains credibility with group by:
  - amassing large quantities of material which are systematically organised
    finding and providing bits of missing series of photographs
  - providing advice to newer members of technical and safety issues
    distributing new pictures
    re living and sharing sexual experiences

COPINE Project

45

Pictures have multiple functions currency

- Sexual arousal
- Reinforcement of successful collecting
- Currency
  - trading for other images
    maintaining existing on line relationships
    giving credibility

COPINE Project

46

A Case Study:Aims

- Understand the role that the Internet may play in offending behaviour
- Examine the process of engagement
- Look at the diverse roles that pornography plays
- Look at the role of the Internet in creating new personas
- Possible links between downloading and assault

COPINE Project

47

Case study: 11

- Male, convicted of downloading (currently on probation)
- Large collection of directories relating to child pornography as well as adult pornography
- Not in treatment at time of interview
- Married 18 years, no children
- Diagnosed as having 'obsessive-compulsive disorder'.

COPINE Project

48

Setting Events: 1

- Social isolation
  - " … friendships that had been established over a period of years were … basically evaporating and I was feeling somewhat isolated at work and er marginalised …"
  - " … there was part of my personality that wanted to do something quite different"

COPINE Project

49

Setting Events: 2

- Inadequate sex life:
  - "And I wasn't also having a fulfilling sexual relationship with my wife … I didn't find her sexually attractive"

  responsibility for which is placed with her for gaining weight and refusing to use the contraceptive pill.

COPINE Project

50

Setting Events: 3

- Illness (reflux oesophogitis)…"
  - "So social activities were being restricted … I couldn't enjoy drinking. I couldn't enjoy eating. I wasn't in a job that I found enjoyable and I was in a relationship I had doubts over…"
- Limited sexual experience

  earlier sexual experiences were confined to "pornography and masturbation"

COPINE Project

51

Engagement with the Internet

- Initially accessed non-pornographic web sites
- Moved on to access adult porn "out of curiosity"
- Rapid skills development allowing access to material for free
- Started to save pictures because might not be able to access them again

COPINE Project

52

Changing nature of material accessed:

- Became more extreme
- Normalised by taking pictures into work
- Feeling of no limits to what might be available and no body to police his activities (cf. Granic and Lamey, 2000)

COPINE Project

53

Moving on to IRC

- Fascination and pleasure from Internet
- Chou and Hsiao (2000) talk of the Internet as providing:

  escape,
  - interpersonal relationships,

  pleasure from use, pleasure from interacting with text and information

  pleasure of being anonymous.

COPINE Project

54

Transition from Virtual to Real Relationships

- Looked for people to chat with whom he could meet
- Kept records of their "vital statistics" that facilitated the emergence of a relationship
- Behaviour resembled aspects of 'grooming behaviour'

COPINE Project

55

Pictures giving credibility

" So I'd send them that material and that's where … I got sort of drawn into logging on the system, going into IRC, seeing who was around, talking about their sexual experiences, believing everything they told me and then also exchanging material, as kind of proof of my credentials you know … to say, right, I've got this material … erm…it backs up that I've got an interest in that area of sexual perversion, let's say … so therefore it's Ok for you to talk to me about it…"

COPINE Project

56

Life on-line

- Increasing amounts of time spent on-line
- Mood change when not able to access material
- Sub-culture of danger and excitement - highly mutually reinforcing
- Relationships act as catalyst and facilitate emergence of deviant sexual interest

COPINE Project

57

Move to Child Pornography

- part of a continuum of engagement:
  - " and … slowly but surely then … got … to the point where … I … had really accessed every sort of pornography you can think about … so … it eventually got to like teenage and then child pornography and … erm … it was I was being turned on … because … erm … there was this idea I suppose of like breaking taboos …erm …but there was also a sense of like … I … can go where a lot of other people can't … it was kind of like … the idea of keeping the images was like trophies …"

COPINE Project

58

Images as Currency

- Denies primary interest in child pornography (at odds with his collection)
- H talks of child pornography as "much to facilitate the on-line relationship as an end in itself". He says:
  - " … these images were currency … because it allowed me to maintain my relationship with the people … I didn't want the material MORE that I wanted to talk to them. I wanted to sort of wallow in their experiences."

COPINE Project

59

Control

- Emerging sense that H was losing control:
  - "I'd sort of opened Pandora's box and couldn't get the lid shut. I'd sort of uncovered …some… aspect of my personality that I couldn't control… If I questioned what I was doing with the people I spoke to on-line… they would shut me out … because they'd think Oh … he's not part of our group … so … all the kinds of messages … all the dialogue was reinforcing".

COPINE Project

60

Changing Persona

- H describes his engagement with the Internet as rapidly growing, allowing him to change as a person:
  - "… through the relationships I was establishing on the Internet … there was part of me that was kind of growing … was developing … whereas my normal sort of … off-line life … was kind of boring and going nowhere ..there was kind of this excitement that erm on line I was a different person …"

COPINE Project

61

Child pornography and sexual arousal

- Emphasises the role of images in maintaining relationships
  - "Well … eventually … it probably got down to … I mean some of them were babies … there was a woman from I. … and she said she was into babysex … and erm … I was sort of again claiming that that was of interest …. Because I wanted to …. maintain contact with her …."

COPINE Project

62

Legitimising the material

- Lack of objective measure
- Lack of experience of personal abuse
- Smiling faces
- Exhausting the potential
- Fantasies of being abused

COPINE Project

63

Using child pornography

- Masturbation

"I was with the masturbation … almost avoiding coming … because if I was on-line for an hour or so I would actually be masturbating on and off for an hour … and wanting to maintain the state of arousal"

"Actually, once I'd come I'd then almost be … I'd I'd I'd be … I'd find it distasteful. That what had been … that what had been acceptable during a state of sexual arousal … afterwards wasn't acceptable".

COPINE Project

64

Collecting

- Completing a series
- Changing names to fit with classification
- Obsessionality

COPINE Project

65

Significance of collecting

- important
- constant in the way that he systematically sought out images to add to it
- highly organised in the way that it was stored

  permanent (he rarely deleted images)

  concealed it from others
- shared with others who expressed an interest in similar material

COPINE Project

66

Points of Concern

- Reasons for not crossing boundaries:

  "… I'd wondered what it would be like … but then I knew that … if I were to cross that barrier … That everything would have been lost. That I would have transgressed and entered an area where I would have been totally out of control … that up until that point I was still somewhat in control … but once I'd sort of crossed that boundary and lets say had sex with an underage girl … then it would have been a no going back situation …"

COPINE Project

67

Justification

- Normalisation
  - "And so there was a wondering what it would be like … and imagining that lots of men have fantasises about having sex with erm .. prepubescent girls".

    "talking to friends, to my wife … that some 13 year old girls do seek out sexual experiences"

COPINE Project

68

General vs. specific statements about fantasies

- Reluctance to talk about specificity of fantasies
  - "I suppose I fantasised about having sex with underage girls … but there wasn't any sort of … erm …any one story line as it were … although I clearly recognise that … if it were to be enacted in real life … there would only be … certain opportunities or situations that would arise … so clearly it had to fulfil a theme that was within the bounds of possibility…"

COPINE Project

69

Resolution through new persona

- Art student (including photography)

  "there's no … association between this and what I'd done before … because I've sort of reinvented myself now … I'm a different person"

  "…. The personality I adopted was restricted to the room at home… where it all took place. And that personality didn't have a proper existence outside of that room."

COPINE Project

70

Move to abstinence

- Feels he's resolved problems by becoming sexually abstinent
- Substituted other high rate behaviours
- Move from high level sexual activity to none
- Still justifying:

  "maybe I was acting out more honestly what a lot of men secretly desire".

COPINE Project

71

Conclusion

- Emergence of behaviour not previously part of repertoire and ability to access and use material
- Community that normalised and reinforced behaviour
- Disassociation of images from real children
- Importance of issues of control
- Changing persona

COPINE Project

72

The context - Virtual Communities

- Adults with sexual interest in children constitute a 'virtual' community on the Internet
- Evidence - plethora of supportive material
- COPINE project explored this through text analysis of Bulletin Board postings

COPINE Project

73

FGB Board (The Professor's Board)

- Been in existence for number of years
- Located in Japan
- Major source of information on postings, security advice, etc.

COPINE Project

74

Analysis

- What sense is there of a virtual community?
- How do members legitimise identities and activities
- How can this contribute to understanding dangerousness
- 'insider accounts' located within complex relational and interactional contexts

COPINE Project

75

Analysis

- 120 hours interaction with Board
- Discourse Analysis of text

COPINE Project

76

Virtual Community?

- 2 patterns emerge from data supporting notion of 'virtual community':
  - evidence of group dynamics
  - concern with status and apprenticeship

COPINE Project

77

Group Dynamics

- Differing member status
- Protection of themselves and board from infiltrators - Security

COPINE Project

78

Member status

- Icarus - All the regs are gone. All here is left is "wannabe members of Pu even I have never posted anything". Board is full of newbies who don't know anything and certainly will not post anything. I've been around 1, years and seems that this is the end of this board. Only technical chat, newbies and spammers left…….

COPINI Project

79

Member status

- Sleeper > icarus Abit harsh don't you think? There's Always Hope. And there are Still "Wise Ones" from the Past Here (different nicks) if you would look > take care

COPINI Project

80

Member Status

- Members are valued on basis of:
  - frequency and quality of 'on topic' postings
  - technical or security expertise
    length of time involved with Board

COPINI Project

81

Security

- Gandalf: If I post the URL to a site here using a proxy server what likelihood is there of the cops requesting the logs of a company in the Far East or a European university to see who I really am?! The site I put up I did at an Internet café so even if the proxy-stuff fails nobody could prove it was me….

COPINI Project

82

Security

- Pirra8> I..feel that the fact we don't post much is because we have a lot of diligent 'observers' that watch what we put up, and quickly tell the servers to pull the site. Its tough spending 2-5 hours posting, only to have it pulled in 10 minutes. What is the solution?….Do we need a secret "club" that will allow you to get files? >>

COPINI Project

83

Security

- (continued) ….News is very easy to post and download from. Maybe we should concentrate on using news, and leave web sites to go to h*ell? This board can still be useful in that case. But, a revision of policy has to be done gradually. I really see no alternative.

COPINI Project

84

Security

- Flatgirls> Torture? Can anyone else (besides dark lurker) see the techniques of I.T. on this board? The idea is to spread doubt about the morality of this hobby of ours….anyone who asks for l*liforture etc. is looking to dissuade visitors with the impression that we are a bunch of child killers….I'm with you…..

COPINI Project

85

Board Status

- Necrolord> Close this board down? What are you nuts icarus?! This board is the best place for us pervs to communicate with each other and share thoughts, opinions and information on the subject we all luv (but are afraid to admit) And I'm sure all the regulars are still lurking around, cuz there's no better place other than the newsgroups.

COPINI Project

86

Boards value

- Presence of regulars or 'wise ones'
- quality and frequency of posts
- development of 'newbies' to ensure further postings

COPINI Project

87

Apprenticeship

- HeLLioN > Hey Icarus, thanx for the contributions but think about even you get something or other from this board, the newbies will get their share, will collect the oldies pix and get knowledge about how to protect themselves this is the main reason for this board to make newbies grows wise and increase our community…….

COPINI Project

88

Critical quality - legitimising activity

- Present as victims - use of discourse of oppression and intolerance
- parallels with gay movement/ civil rights
- comparisons to racist or survivalist groups

COPINI Project

89

Pulling together (1)

- Interviews and BBS's analysis complement each other, emphasising significance of Internet in notion of a 'community':
  - processes of validation
  - legitimisation
    - sense of community
    - support

COPINI Project

90

Pulling together (2)

- Engagement with Internet and Communities very flexible and dynamic
- Internet allows for multiple engagements through differing kinds of self representation.

COPINE Project

91

Similarities with other sex offenders

- sexual fantasy, arousal and masturbation to pornographic images and text
- situationally specific lack of empathy towards the children involved
- distancing himself from taking responsibility for accessing the material
- attributing possible collusion to the children in the images
- blaming his mental state for his behaviour

COPINE Project

92

Functional Addiction

- Salience
- mood modification
- tolerance
- withdrawal symptoms
- conflict and relapse

(Griffiths, 1998).

COPINE Project

93

Current sex offender programmes

- CBT appears to be the most successful and targets include:
  - denial and minimisation
  - damage to victims
  - justification and distorted thinking about offending
  - deviant sexual fantasies
  - relapse prevention
  - lifestyle and personality
  - sex education

COPINE Project

94

Current programmes

- Based on largely static model:
  - innate characteristics (personality)
  - prosocial behaviours (social skills)
  - self control behaviours (fantasy training)
- Ignore process model of offending
  - engagement and maintenance
  - high rates of reinforcement
  - control of stimuli

COPINE Project

95

Issues arising from project

- Results to date from project activities emphasise:
  - significance of context
  - dynamic qualities
  - move from virtual to real
  - pictures as currency

COPINE Project

96

Issues for treatment

- Internet facilitates attribution of blame/responsibility lying outside the individual
- enables user to cast about for identities
- generates received accounts for roots of paedophilia
- enables changing definitions of paedophilia
- allows for emergence of virtual community which can be transformed into real community
- can act as vehicle for working out of fantasies

COPINE Project

97

Internet and therapy

- Need to address social as well as sexual function
- Challenge to community identity
- Address 'addictive' qualities to behaviour
- Tackle issue of whether it enables or reduces the likelihood of actual offences against children

COPINE Project

98

Clinical as opposed to conceptual typologies

- "The classification, diagnosis and assessment of child molesters are complicated by a high degree of variability among individuals in terms of persona characteristics, criminal histories and reasons for offending. There is no single profile that accurately describes or accounts for all child molester." Prentky et al. 1997

COPINE Project

99

Clinical as opposed to conceptual typologies

- It appears the same will apply to Internet offenders
- Need to look at how the Internet functions for the individual within a social context
- It appears to be a dynamic rather than static process

COPINE Project

100

'Good' and 'Bad' offenders

- a simple but important point - once a picture is in the public domain, it remains in circulation regardless of the fate of the producer
  - Salt and Louise pictures
  - Lucy
- downloading and accessing photographs in itself is a source of continuing victimisation

COPINE Project

101

Thoughts/concerns 1

(in no logical or particular order)

- Law Enforcement - Child protection focus or offender focus?
  - catching downloaders
  - focussing on producers
  - identifying children
- The problem of ownership of investigations
  - pictures are international
    - e.g. kg

COPINE Project

102

Thoughts/concerns 2
(in no logical or particular order)

- Training for Law Enforcement and other professionals:
  - evidential issues related to pictures
    - referral onto to specialist units
    - tracing the chain of postings
    - picture content
  - understanding the processes
  - knowing the language

COPINE Project

103

Thoughts/concerns 3
(in no logical or particular order)

- What to do with Internet offenders
  - assumptions about offenders?
  - participation in mixed sex offender groups?
    Removal of computer?

COPINE Project

104

Thoughts/concerns 4
(in no logical or particular order)

- The evolving Internet
  - Specific
    - developments in computer generated 3D graphics
    - notion of community of learners
    - 'good' and 'bad' offenders
    - improved video compression
    - encryption and availability of strong security
    - growing commercial involvement and organised crime and links with child sex tourism and child trafficking

COPINE Project

105

Thoughts/concerns 5
(in no logical or particular order)

- General
  - cognitive functioning and the Internet
  - changes in beliefs, values and cognitive styles
  - changing states of consciousness, and changes in involvement in more extreme areas
  - decentralisation of conventional hierarchies and empowerment of marginal groups
  - changing boundaries as a product of range and variety of information

COPINE Project

106

Thoughts/concerns 6
(in no logical or particular order)

- The role of the ISP industry
  - national self regulation/statutory control
    - mandatory reporting of child pornography
    - monitoring/censorship/freedom issues
    - holding records
  - international control
    - common standards and values
    - 'rogue' countries

COPINE Project

107

Final thoughts - quotations from operator of w0nderland (1)

- "So… I'm still wearing the mask in effect…I'm still having to hide who I am. I can't be myself, and I miss being on line for that more than anything else 'cause there's no where I can be myself now"

COPINE Project

108

Final thoughts - quotations from operator of w0nderland (2)

- "…if society isn't going to let me be anything other than a paedophile and I've lost the computer….the only thing that's left that I can console myself with is sex….and I know its going to lead to people getting hurt"

COPINE Project

109

The COPINE Project
Department of Applied Psychology
University College
Cork, Ireland
Dr. Max Taylor (stay@netcom.es)

COPINE Project

110