Parliamentary Joint Committee on the Australian Crime Commission

Inquiry Into Cybercrime

Submission No:3

Mr Doug Stead
President
Tri-M Systems Inc.
100-1407 Kebet Way
PORT COQUITLAM BC
CANADA V3C 6L3
☎(604) 945 9565 (604) 945 9566
E-mail: dstead@Tri-M.com

McMahon, Rosalind (SEN)

From: Doug Stead [dstead@Tri-M.com]
Sent: Wednesday, 23 April 2003 5:38 AM
To: ACC, Committee (SEN)
Subject: Submissions

April 22, 2003

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

Subject: Written Submissions

Dear Sir or Madam,

I would like to provide to the attention of the members of the Parliamentary Joint Committee on the Australian Crime Commission, the attached submissions.

1) **"Amber's Secret"** This white paper highlights the use of cyber technology in the creation of child pornography and child sexual abuse. Prior to 1992 and the inception and wide spread adoption of the Internet as a means of communication, children could not have been preyed upon in what is termed "distance remote" abuse. The paper outlines how a predator in Australia co-opted a child in Canada using inexpensive video and computer technology. It also highlights how Australian and Canadian "operational" law enforcement officers cooperate in the international investigation and interdicted further sexual abuse.

2) **"Pedos and Child Porn in the News"** Is a regularly issued report covering 7 to 10 day periods, of English news media reports, compiled from world Internet sources. As such, it provides a "tip-of-the-iceberg" indication the exponential growth and pandemic nature of child pornography and child sexual exploitations. Cyber felons in general and pedophiles and child pornographers in particular, are early adopters of new technologies, as these technology facilitates and obfuscates their criminal endeavors. Open source intelligence gathering and review of material of this type, can forewarn legislators and law enforcement agencies. Knowing and understanding how technology is beneficial to criminals, in one part of the world, leads to understanding how the same technology may be being used in ones own back yard.

I would like to commend the Australian government in take a proactive approach to dealing with how technology is used by pedophiles and child pornographers. These crimes and criminals are widely misunderstood and much more common than popularly believed. Sexual predators of children operate in a vail of cyber secrecy, are well organized, using sophisticated technology and methods to gain trust of victims and society. Their crimes of rape, molestation and photo/digital documentation of the sexual abuse is only the beginning of the life long devastation suffered by the victims. While first world country such as Australia are addressing the problem, countries such as my own, Canada, have done very little finding it easier to look away, denying the problem, while at

Amber's Secret:

An International, Distance-Remote Child Sexual Exploitation Case Study

February 12, 2002

By Doug Stead
dstead@eap.ca

Director, International Society for Policing of Cyberspace
www.POLCYB.org

Director, American Anti Child Pornography Organization
www.antichildporn.org

Founder, Entrepreneurs Against Pedophiles
www.eap.ca

Abstract

Amber's Secret is a case study that examines and recounts how Canadian and Australian Law Enforcement conducted the multi-jurisdictional investigation of an adult male living in Australia who, using computer, digital video and Internet technology, sexually lured and groomed a developmentally challenged female child living in Canada.

Aim

The purpose of a case study is to generate interest, stimulate discussion, convey knowledge, and affect attitudes using a relevant and current real-life example. “Amber’s” story is typical of the dangers children face in our ever technologically advancing world. The not only typical but also atypical response of police officers and their respective agencies is relevant for it exemplifies how direct communication and cooperation in an ever shrinking global village successfully facilitated an effective and quick resolution.

Who

Victim

Amber (not her real name) is a l6-year-old disabled female, with the mental and maturity level of a l3-year-old. She lives with her mother in Port Moody, British Columbia, Canada. Amber, like many teens and preteens, is an avid player of “Creatures,” a very popular Internet game and e-community. Amber created her own “creatures” with which she entered and played various virtual-reality games. These, however, are games that also allow and encourage players to converse with each other using real-time chat relays together with web video camera images.

Perpetrator

David, known to police, is a 26-year-old unemployed male who lives with his parents in South Australia. He lives in a rural crossroads, consisting of a few homes with no shops or other services. The closest township of any size is Loxton, a considerable distance drive. David is also computer-skilled and an avid Internet user and “creatures” player. David uses the game “Creatures” to meet children, and to develop trusted, friendly relationships with children such as Amber.

What, When, Where, and How

On October 30, 2001, Officer Jim Burton of the Port Moody City Police, a department with 32 sworn Police Officers serving a quiet suburban community, returned a voice mail left by Amber's mother. The mother, after consulting several family friends and a therapist, selected this officer because of his long service in the community and his good reputation in working with troubled youth. Amber's mother disclosed that she found Amber nude, posing in front of her bedroom computer web camera. As well, Amber’s estranged father, a computer professional, examined the computer and found a computer video of an adult male, nude and masturbating himself.

Amber's father removed the hard disk drive from Amber's computer and provided it to police. The hard drive was subsequently brought to a local computer engineering company that made a sector-by-sector, track-for-track duplicate copy of the entire drive. Information gathered from the hard disk included the predator’s email address, his home address and a copy of his resume as well as the sexually explicit video-image file(s) and chat-logs indicating that the predator was not only in touch with Amber but with many other children world-wide.

On November 1, 2001, Port Moody police forwarded a summary of this information to Interpol requesting that David be investigated and dealt with by the Australian Police. Interpol acknowledges receipt of this request.

On November 19, 2001, out of a concern that other children were at risk of being victimized in a similar manner, Port Moody police arranged to hand-deliver this same Information to Commander Barbara Etter of the Australian Northern Territory Police and Director of the Australasian Centre for Policing Research, who, coincidently, was attending the annual Conference of the International Society for the Policing of Cyberspace (www.polcyb.org) being held in Richmond, BC, about 45 kilometers west of Port Moody.

On December 5, 2001, upon returning to Australia, Commander Etter, passed the file to Chief Inspector Bronwyn Killmier of the Bern Police, her department being responsible for the "Riverland" area in South Australia, an area that includes the Loxton township.

On December 6, 2001, Detective Senior Constable Geoff Carson of the "Riverland" Investigation Unit opened an Australian criminal investigation into Amber's case. As a professional courtesy, Carson conferred with Officer Burton by phone, catching him at home enjoying a hot tub, and confirmed details of the offense.

"I have been praying hard for something like this to happen, thank you for answering my prayers"

(David's father on inviting police into their home.)

On December 10, 2001, during the early morning, Detective Senior Constable Geoff Carson, together with other officers, went to David's rural residence. David's father invited the officers into his home, stating that he knew of his sons sins but, being a good Christian, he didn't want to get his son into trouble. "I have been praying very hard for something like this to happen; thank you for answering my prayers."

At that very moment, David was engaged in a long distance phone call to Canada – talking with Amber!

David's computer equipment was seized together with other letters and movies related to child pornography. David was arrested and taken into custody and subsequently charged with three criminal offences:

- Indecent Behavior (his masturbating over the internet),
- Causing a child to expose her body for prurient interest,
- Causing a child to commit an indecent act for prurient interest.

David was subsequently granted conditional bail, guaranteed by his father, the terms of which included:

- He will attend the Sexual Offenders Treatment and Assessment Programme,
- He will not use electronic mail, the Internet, or cause either to be used on his behalf,
- He will not to be in the company of any child under the age of 16 years,

Epilogue

On February 12, 2002, David is awaiting trial. The file, passed through Interpol, seems to have gone astray. Amber is getting on with her life, and is not thought to have had any further contact with David.

Lessons learned / Discussion points:

The ideas and thoughts below are those of the writer, perceived from his vantage point (outside of Law Enforcement or the public sector). The writer is a deeply concerned, high-tech private sector executive, interested in better protecting children from sexual predators and sexual exploitation. Consequently, the discussion points listed below are not an exhaustive or comprehensive interpretation of all that may be learned from this example. Rather, the hope is that the following will serve as a model from which, viewed from individual perspectives, additional ideas will be provoked and a better understanding of these types of criminal issues will emerge. Your ideas and comments are welcome; please email them to dstead@eap.ca.

1) Risk Factors: Amber lives in a single parent environment, and is developmentally challenged. She is possessed with technical skills, has her own computer with high speed Internet connection, and has long hours of unsupervised use of these technologies. Therefore, she is especially vulnerable to attack by sexual predators using the same technology to target their victims.

2) Locating Amber's computer in a family room or common room, as opposed to the child's bedroom, might well have provided an earlier warning of the “grooming” Amber underwent, and perhaps could have provided interdiction prior to her being lured into nude video transmission.

3) Pornography is an important part of the grooming cycle used by pedophiles and other sexual deviants to lure children into posing for the creation of Child Pornography. Once created and transmitted on the internet, there is no way to erase or remove it or to stop its propagation. This factor alone may create life-long psychological problems for the victim.

4) Police persons, when they are “active in the community”, build trust which better serves society in the long run. This case came to the attention of Law Enforcement only after the mother was able to find, and was satisfied with finding, a police officer who had an acknowledged reputation for dealing with youth.

5) Technology allows sexual predators, pedophiles and other sexual deviants to assault children from half-way around the world. The Internet invites the rest of the world into your home.

6) What was perhaps not a crime in Canada was a chargeable criminal activity in Australia. All such investigations (involving sexual exploitation of children) which identify a “potential predator” in another country, should be shared with the appropriate Law Enforcement agency.

7) Although it was an international investigation, this case was successfully concluded in a remarkably short time, due to the information being handed directly department-to-department, country-to-country. Even more interesting, very little of this unusually short total time period – from receiving the complaint to an arrest in this case – was used by the police officer working at the rock face. This question, however, still needs resolution: How can nations better facilitate direct communication between their operational police forces?

8) Even unsophisticated or a less experienced sexual predator, one stupid enough to e-mail a resume, builds an incredibly strong relationship with the child victim. So powerful, in fact, as to be able to continue his assault on the victim, 6 weeks after the predator's criminal activities had been exposed.

9) Law Enforcement can build trusted relationships with local businesses, which when needed, can be drawn upon to supply, at little or no cost, specialized technical expertise and/or equipment.

10) As the use of inexpensive, real-time, Internet video conferencing technology becomes more ubiquitous, so also will distance/remote sexual exploitation of children together with the creation of child video pornography.

11) Criminals are early adopters of new technology, especially technologies which better facilitate and obfuscate their criminal activities.

12) For police departments to achieve their mandate – to protect and serve law abiding citizenry -- they must be properly resourced with staff, current technology and training. Failure to provide these essential elements, inevitably leads criminals to the belief they will not get caught. We must shatter this belief, leaving no doubt whatsoever, that our society will do whatever is necessary to protect that which is unarguably our most valuable resource: our children.