

IMPLICATIONS OF THE AUSTRIAN CHILD PORNOGRAPHY INVESTIGATION

“The discovery of the crime being perpetrated against our children must become part of our conscious awareness. What we do must have a single aim: to ensure that all children are protected from abuse and exploitation by all of us. No individual can delegate to anyone else this responsibility that each one of us must acknowledge, accept and act upon wherever we may find ourselves. For the crime is not only the abuse and exploitation of children: it is also the silence from those who can speak out but choose to avoid the sense of horror which should form the basis of everyone’s perception of the world we are creating for our children”.. lyavar Chetty

Introduction

The alleged international paedophile ring exposed by Austrian law enforcement authorities is a tragic reminder of the ease with which criminal syndicates are able to exploit the Internet and inconsistencies in national laws to make huge profits from the sexual abuse and torture of children. It is stark evidence and confirmation that the multi-million dollar industry, based on the torture and rape of children, involves, not harmless individuals but criminal syndicates. The involvement of criminal syndicates is a disturbing trend. While most individual collectors would rely on increasing their collections mainly through a share-and-exchange relationship with others on the Internet and do not, as a general rule, become producers and

distributors themselves, criminal syndicates are active producers and distributors and not collectors *because their interest is only in the commercial benefits of child pornography and not in any sexual gratification for themselves.* In other words, criminal syndicates are not necessarily syndicates of paedophiles but syndicates of equally depraved people with paedophiles as their target-market. This does not mean, of course, that paedophile rings do not exist. The infamous “w0nderland club” is an example of a highly-organised syndicate of paedophiles. (The “0” in the name “w0nderland” is not a typographical error. The club was named after Lewis Carrol, a notorious collector of nude pictures of little girls and the alphabet “o” was replaced by the numerical “0” as part of an elaborate security system.) The Austrian case follows a long line of similar investigations, beginning around the late 1990s.

In September 1995, in *Operation Innocent Images*, the FBI made several arrests and searched 120 homes nation wide, concluding a 2-year investigation into the use of America On-Line to distribute child pornography and arrange sex with children. FBI agents in Baltimore first became involved in the investigation in 1993 while attempting to find 10 year old George Stanley Burdynski, who was abducted from his Brentwood, Maryland neighbourhood. The child was never found, but the investigation led to the discovery that both adults and juveniles were routinely using computers to transmit images of children aged 2 to 13 showing frontal nudity and sexually explicit conduct.

A federal grand jury in San Jose, California, in 1996, has 16 people from the US and abroad for their participation in a child pornography ring called the *“Orchid Club”*, whose members used the Internet to share sexual pictures and conduct online chat on child molestation.

In 1998, *Operation Cathedral* was the first international investigation of a paedophile syndicate trafficking child abuse images on the Internet. This investigation in 12 different countries resulted in the arrest of 195 paedophiles and the seizure of over 750 000 child abuse images and 1 800 digitised video clips of child abuse.

In *Operation Starbust*, British police were involved in the investigation of an international paedophile ring using the Internet to distribute graphic pictures of child pornography. Nine British men were arrested as a result of the operation, which involved other arrests in Europe, America, South Africa and the Far East. The operation identified 92 paedophiles worldwide.

In 1997, in *Operation Rip Cord*, US Federal and state authorities arrested 120 paedophiles and identified a further 1 500 worldwide involved in the distribution of child pornography.

In 2001, in *Operation Landmark*, a further 60 000 images were seized and in 2002, *Operation Ore* investigated over 7 300 credit card transactions involving child pornography originating from Russia and Indonesia. *Operation Ore* led to the arrest of 1 600 paedophiles in the UK, including teachers, care workers, social workers, soldiers, surgeons and 50 police officers.

The Facts in the Austrian Investigation

- 1 According to the information, Austria's Federal Criminal Investigations Bureau (FCIB) uncovered "a major international child pornography ring involving more than 2 360 suspects from

77 countries", including South Africa, "who paid to view videos of young children being sexually abused" by downloading videos from the Internet. The USA, Canada, the UK, Germany, France and Australia have all begun investigations based on information provided by the Austrian authorities.

- 2 According to the FCIB, the videos included images that showed "the worst kind of child sexual abuse", including scenes of little girls screaming as they were being raped. The images were believed to have been shot in Eastern Europe, uploaded to the web in the UK and posted on a Russian website hosted by an Austrian company¹. Investigators said that, over a 24-hour period, they recorded in excess of 8 000 visits to the site from computer addresses in the 77 countries.
- 3 The Russian site charged a fee of US\$89 (around 45 pounds sterling or about R630) for access by "members only". At around 8 000 "hits" per day, and even assuming that only about a quarter were by members, the amount the site generated would have been in excess of R1.2m over a 24-hour period. Criminal syndicates are not about to turn away from this opportunity to rake in millions of dollars from the abuse and exploitation of the world's children.
- 4 According to BBC News, experts have described this type of criminal activity as "fairly routine" and have become very much a part of the activities of criminal syndicates for two main reasons: *firstly*, it is highly profitable and, *secondly*, because

¹ Raises relevant jurisdictional issues

they are difficult to detect and close down because of the ease with which they can move their operations around the world. Criminal syndicates, it is reported, maintain databases of paedophiles and direct them to pay-per-view sites via e-mails. Files containing child pornography are difficult to detect because everything that transverses the Internet looks the same in transit. Traffic gets broken down into packets of data that do not identify what they contain, so an e-mail containing child pornography looks the same as an innocuous e-mail. In this case, law enforcement authorities got a "lucky break" because a technician employed by an Internet company in Vienna noticed that a series of violent videos involving children had been downloaded onto his computer by criminal who had hijacked his computer to hide their trail as they transmitted the images to Russia and the technician immediately alerted the police. (According to the Internet Watch Foundation, the bulk of the world's child abuse sites are located in the USA and Russia.)

- 5 Apart from the support modern technology offers criminal syndicates, paedophiles have access to the Internet not only from their own home and work-place computers but also from the thousands of Internet access points, often free, offered at educational institutions, cafes, hotels, airports and other public places. (It is estimated that there over 46 000 access points across the USA.) FBI agent Kevin West admitted that they have not yet developed a way to combat that. "Free wireless spots are everywhere and it makes it easy for people to sit there and do their nefarious acts.....we need to figure out a way to solve this problem."

- 6 The way it works is quite simple. Anyone who has wireless card installed in a computer or a mobile cellular phone can access the Internet from any of the "public" WiFi "hotspots". Getting online has never been easier – both for criminals and paedophiles – changing the profile of perpetrators to include not only family members, friends and neighbours but also strangers operating via chat rooms. One police officer described open wireless systems as the same as leaving one's front door open for anyone to enter and help themselves to one's possessions. Law enforcement is often frustrated because tracing an IP address originating from a wireless signal often leads back to the owner of the network instead of the criminal user. There is no legislation that requires anyone offering wireless connections to maintain some system to track users, such as filtering measures that can scan to see who is accessing the network.

Conclusions

The Austrian case highlights the need not only for more, better and increased international cooperation and international harmonisation of anti-child abuse laws, but also for a more effective response to the problem within South Africa by recognising that the investigation and prosecution of Internet-related crime, and especially child pornography, is not an "every-day" police matter. Those involved in the investigation and prosecution of such crimes require very specific technical training and expertise. Both institutional and structural reviews of the relevant institutions are necessary.

And national legislation must be reviewed to assess if the liability of Internet content hosting and e-mail service providers are properly and adequately articulated to maximise measures aimed at the protection of children.

The Austrian investigation provides evidence that criminal and paedophile syndicates are operating from within South Africa. Given that information communication technology is continuously being refined and advanced, and given that the trade in child abuse materials is almost entirely technology-driven with respect to production, distribution and possession, it is necessary to ensure that anti-child pornography legislation is, if not technology-neutral, constantly reviewed and amended to accommodate changing technology.

Iyavar (2007)