



A special presentation delivered by John Carr

Round Table on Respect of the Rights of the Child on the Internet

Professional Investigation and Prevention Tools for Schools and Home

Palais de Luxembourg, Paris – November 20, 2003

Imagis Technologies Inc.
1630 – 1075 West Georgia St
Vancouver, BC, Canada V6E 3C9
www.imagistechnologies.com

Phone: +1.604.684.2449
Fax: +1.604.684.9314
info@imagistechnologies.com



About John Carr

John Carr is a world-renowned expert on Internet safety and has presented lectures and seminars to a wide range of organizations including the NSPCC, ECPAT (the Bangkok-based, global campaign to end child prostitution and trafficking), Save the Children in Iceland, and Kinderfreunde in Austria.

He is a board member of the Internet Watch Foundation and the principal Internet Consultant for the NCH Action For Children. Founded in 1869, NCH is today one of the UK's largest children's welfare organizations with projects in over 400 locations across the country. On Internet policy NCH works closely with an established consortium of the UK's main children's organizations: Barnardos, ChildLine, Children's Society, National Children's Bureau, National Council for Voluntary Child Care Organizations and NSPCC.

John has represented the European Federation for Child Welfare on the EU's INCORE Steering Group, and was the Director of an EU Internet Action project which aimed at raising awareness of Internet child safety issues in the UK, Italy and Finland. He is a member of the Working Group of the Ministry of Justice for the Protection of Children on the Internet and a Member of the Administrative Council of Innocence in Danger. John has also been a frequent contributor on TV and radio and has written on Internet safety for children in *The Observer*, *New Statesman*, *The Guardian*, *The Independent* and *Prospect*. John also wrote one of NCH's most successful publications: "*A Parents' Guide to the Internet*".

This document is a direct transcript of John's presentation at the *Round Table on Respect of the Rights of the Child on the Internet* and has been re-published with his permission.

Palais de Luxembourg, Paris

20 November 2003

John Carr is a world-renowned expert on Internet safety and has presented lectures and seminars to a wide range of organizations including the NSPCC, ECPAT (the Bangkok-based, global campaign to end child prostitution and trafficking), Save the Children in Iceland, and Kinderfreunde in Austria.

The arrival of the Internet in our midst, as a mass consumer product, has had a profound impact on society in many different ways. I do not think there is any doubt that the emergence of the Internet has been hugely beneficial for people in general and children in particular. It offers to enrich children's lives and their education in all kinds of ways. Perhaps if the Internet had been around when I was younger, I could have gone into French chat rooms, learned to speak contemporary French more fluently, and today I could stand in front of you and deliver this speech without the need for translators.

However, the arrival of the Internet as a mass consumer product has also brought in its wake some problems that we have still not managed to solve – but I am confident we will. We have to.

The internet has allowed criminals to commit old familiar crimes in new and unfamiliar ways. Nowhere is this clearer than when we look at what has happened in the field of child abuse and child pornography.

Now the simple truth is that we have never really known how much child pornography has been in existence or how much has been circulated between paedophiles. Except for a brief period in the 1960s in Scandinavia, in virtually every country in the world, child pornography has been illegal for a very long time and so the only occasions we ever got any real insights into it was when the police made arrests and the men responsible, and they are almost always men, were brought to justice. But that never gave us the complete picture. It only ever gave us a partial picture. People who trade in child pornography do not co-operate with market researchers. They do not notify the state's central statistical office about the volume of business they are doing this year, as opposed to last, or what their expansion plans are for the following year.

In January, 2004, I will be publishing a booklet in which I set out the now extensive evidence from the UK which I think shows conclusively that the Internet has facilitated a gigantic increase in the production and circulation of child abuse images. I also argue that this, in turn, has almost certainly led to an overall increase in the number of children being abused.

I say this for two main reasons: firstly, the internet has allowed many men who perhaps only had a latent or suppressed interest in child pornography to go and find it and start collecting it, whereas previously they would have been too frightened, or just too lazy. The internet has opened a door for them that previously they would never even have dared to approach. Once they start to get involved with the images, for many it starts to fuel their sexual fantasies and this, in turn, will eventually lead some of them, not all of them, to start abusing children in real life. These are children who, therefore, in all probability would otherwise never have been abused.

A very distinguished psychiatrist in the UK put it like this "People who collect child pornography do so because they want to have sex with children, but some of them may not have realised it yet." There have now been several studies which show that people who are arrested simply for the crime of possessing child abuse images, are also actively engaged in abusing children. There is a very definite link between the two activities for many people, but I must stress that knowing there is a link is not the same as knowing the cause.

The second reason why the internet is also contributing to an increase in child abuse is because organized crime has realised that there is lots of money to be made out of it. One of the sad consequences of Operation Avalanche in the USA is that news went around the world that the company involved took US\$1.4 million in its last month of trading, before the police shut it down. 70% of that cash – all paid for by credit cards – went to the producers of the images and 30% was retained by the company simply for hosting the web site. So now we know that criminals are systematically arranging for new children to be abused so they can produce new images for their customers to buy.

In other words, every time someone downloads a child abuse image from the Internet, not only is it a way of re-abusing the child shown in the picture, potentially it is also a disaster for another child as well because whoever produced the first image will believe that you want a second one, but you will only want it if it is new and different.

At one point earlier this year the British Internet Watch Foundation, of which I am a Director, was tracing up to 85 new pay-per-view web sites per week, where child abuse images were for sale. Before Operation Avalanche there were virtually none.

I make these points, and I am publishing my booklet in January, because while to many of us it will seem obvious that the internet has facilitated a huge increase in the amount of child pornography, and that more children are being abused because of it, not everyone agrees. Indeed in my booklet I will say that nobody can prove the point conclusively one way or the other. Nobody can ever prove anything conclusively where what you are talking about is unreported or unrecorded crime. I simply assemble all the available evidence and say that any reasonable person who looks at it can only reach one possible conclusion.

I want now to return to this question of the volume of images currently in circulation, because this has had a major impact on policing this area.

Arguably 1995 was the last year of the pre-Internet world in the UK. In that year the police force in Greater Manchester seized the grand total of 12 indecent images of children. All of these were on paper or on video tape. In 1999, the same police force, covering exactly the same area, seized a total of 41,000 images: all except 3 of these had come from the Internet and were on computers. Today, four years later when the Internet's presence in the UK has doubled in size twice, this police force does not bother to count all the images they seize. There are too many.

In pre-Internet days a typical police seizure of child abuse images from a private individual would yield a handful of pictures. To seize a hundred or more images would have been sensational. A thousand was almost unheard of, and all of these images would have been on paper or on video. The police required no special knowledge, skills or equipment to look at the images. Many of them had come out of Scandinavia, especially Denmark, when for a brief period in the 1960s they abolished all pornography laws and this led to the creation of a legal child pornography industry whose images are still circulating on the Internet and are collected by paedophiles.

Today in a typical arrest one person's computer might contain tens of thousands of images. Earlier this year a man who lived near Oxford was caught in possession of 250,000 images on a single machine. In the famous Wonderland case the police in 14 countries seized 750,000 images from 100 or so club members whom they arrested. Someone in New York has just been found with 1,000,000 images. I mention these as specific instances of how the whole dynamic of this sort of crime has changed. There has been a complete step change.

Look at what has happened in the UK. Following Operation Avalanche in the USA, the British Police mounted Operation Ore. The American authorities gave them, in a single day, the names of 7,200 men who had used their credit cards to buy child abuse images from that American web site. When fraud and duplicate entries were eliminated this list came down to about 6,500, of whom now over half have been arrested and their computers seized. That's over 3,000 men being arrested for child pornography offences when in previous years they might only ever have arrested a few hundred.

As you may know, in the UK we do not have a national police force. We have 43 local ones covering England & Wales. Scotland is a different country entirely for legal purposes, and Northern Ireland has its own police force as well. They all work together in various ways, and between them they run several national policing operations, but each local force sets its own policy and they have all been close to breaking point when it comes to processing the sheer volume of images that all of the arrests under Operation Ore have generated.

We know for sure that some police forces have abandoned the idea of looking at every image on a computer they might seize. They look at enough to establish that a crime has been committed and to bring charges, but because they do not look at everything it is entirely possible that they are missing something, a new image of a new child perhaps. In addition, the backlog of computers waiting to be fully examined can now be very substantial. In some police force areas if, after an initial examination, your computer is seized today, it might be May or June of next year before it is thoroughly examined. If there was any fresh evidence of new crimes on there, it might by then be of little use. And finally, think about the potentially huge waste of police time and resources. A local policeman seizes a computer. It might only have a few hundred images. He might start to investigate, make enquiries about this or that child, without knowing that the pictures are at least 30 years old, they came out of Denmark, or they are 10 years old and they came out of California, the child has already been identified and rescued, and the man responsible for making and distributing the image has been arrested and is still in jail.

This is where ChildBase is going to make a huge difference. Put very simply ChildBase is a computerised database that deals with child abuse images and images of people suspected of being involved in child abuse.

Up to now tracking and cross-referencing images and different features within an image was largely a manual process. It was slow and laborious. What ChildBase is doing is digitising every child abuse image that comes into the possession of the police. The software associated with ChildBase can then, in minutes, look at any images that might be seized in a new police action and then tell, again in minutes, which of these images are already known about and therefore it can also tell which are new. Apart from giving us, for the first time ever, valuable information about the real volume of new images coming on to the market, obviously these new processes will allow the police quickly to find the any previously unknown images, isolate them from the rest and see if there is anything that can be done immediately to identify the child and apprehend the perpetrators.

At the end of the day, this whole exercise is about protecting children and up to now there have been comparatively few successes in locating child victims in real life, to rescue them from the situation there are in and the abuse it involves, and also to arrest those responsible for the abuse or for selling or distributing the images.

It is a very difficult area and everyone agrees that the success rate is low everywhere. One academic has estimated that there might be images of over 10,000 different abused children on the Internet and, as of today, fewer than 300 have been identified in real life, and even fewer perpetrators have been linked to those images.

So this is where we all hope ChildBase will score heavily. As I have already mentioned, apart from recording the image of the abused child, it can also recognise, store and cross-reference data about the

surroundings in which the abuse is taking place – there might be a certain kind of clock or television visible in the background, or the room may have specific architectural features.

It can also store any visible details of the perpetrator. In an early example of this type of functionality one man in the UK was caught because an unusual tattoo on his arm was visible. He got 12 years in jail. In another case a box of household tools was visible on the floor and the room had an unusual ceiling. An architectural historian was consulted. He recognised the type of ceiling and gave the police a list of the areas of the country where houses with that kind of ceiling might be found. The police then cross-referenced those locations with the locations of the chain stores that sold that particular brand of household tools. They found a small number of matches but then they learned there was a marking visible on the box which identified an individual store. They showed the warehouse manager in that store a picture of the box and he agreed it had come from there but also added that not that many had been sold because it was quite a new and expensive line. He was able to pull off a list of everyone who had bought those goods using a credit card. Only one of these people lived in a house with that kind of ceiling. He was arrested and later received 6 life sentences for offences involving his 5 year old daughter.

What else will ChildBase be able to do? Obviously it will be able to cross-reference any information about suspects, objects, locations and so on. But what if the image has been edited or changed slightly? What if it is an entirely different image of the same child, maybe in another place, or maybe even when the child is a few years older. The software should also be able to cope, partly because it uses some very clever facial recognition software that can pick up on particular characteristics that may not change, no matter how a picture might have been edited, and even allowing for a child having aged. In fact the software will even pick up siblings – brothers and sisters – of children who are in the database if their facial characteristics are similar.

In the not too distant future we can see a time when it will not be necessary for the police to look at any child abuse images in most cases. Let me explain.

Every image has a unique digital signature – sometimes referred to as a “MD-5 hash”, but there are other kinds. ChildBase could construct a database just of these signatures and then you simply run a programme which compares the signatures on the database with the signatures on the confiscated computer. Voila. Either it identifies only new images which you then look at and act on straight away, or it provides you with an inventory of every image on the machine. In the UK we now have a system for classifying child pornographic image. They are, of course, all bad and all illegal but the English judges have graded them into 5 different levels of awfulness. This is to assist the judiciary when it comes to sentencing in specific cases, and tags could be added to the file of each image to show what kind of image it was. This also will save the police and the courts a great deal of time and

money so once again they can focus on the really important business of victim identification and rescue.

Looking a little further forward, but not too far, I can also see a time when we could send out on to the Internet an intelligent agent, a web crawler, a software robot of some kind, with instructions to look for images that share the same digital signatures as those on the database. Once located the robot could then report its whereabouts to the police in the country concerned, or destroy it, or it could do both of those things.

Of course there are all sorts of legal issues that would need to be resolved first, but the technology is bringing us close to that point. A robot of this kind would not help deal with the problem of new images, but as soon as an image fell into the hands of the police it could become part of this automated system.

Of course the criminals will find new ways to do their terrible deeds and the forces of law and order will then face a new challenge to get ahead of them. Already there is evidence that criminals are turning more and more to using encryption to hide their images and their transactions, and they are moving towards peer-to-peer networks in the hope that they can keep out of sight, but the key point is that the forces of law and order are now not far behind and they are proving to be more than their equal in many ways. Often it comes down not to technology or know how, but to resources.

So what, finally, of ChildBase? It is an experiment. It is not fully operational yet but it is working and helping with cases already. The British Police are working very closely with colleagues in Interpol, and with police forces in other countries that are also conducting similar technological experiments in pursuit of the criminals who are abusing children or are circulating child pornography. I believe the French Judicial Police have such a system, for example. The idea in the end that we have one big, highly secure database which police personnel all over the world can access in appropriate ways to help in the global fight against these terrible crimes. That is still a very long way off but the sooner it arrives the better it will be.

Technology has created a lot of problems, but we are also showing that technology can solve them too.

John Carr

About Imagis Technologies Inc.

With an extensive background in providing facial recognition identification solutions to local and national law enforcement agencies, Imagis develops software that bridges the gap between islands of disparate data. This includes software that allows you to transform critical information into knowledge, providing immediate business value to the end user.

The firm's foundation is based on two robust and easy-to-use software technologies. The first is a standards-based data sharing toolkit and development platform known as the Briyante Integration Server. Briyante enables the rapid creation of solutions that provide users with consolidated views of information held and maintained in disparate databases. This technology is enhanced by Imagis' unique ability to access textual information as well as facial and other biometric or non-biometric imagery. To this end, Imagis develops and maintains proprietary algorithms dedicated to biometric facial recognition and image matching. We also use our deep experience in biometrics to help customers identify tools that meet their operational needs.

In addition, Imagis provides a suite of customizable software applications that deliver immediate business value for specific market needs and verticals. This includes:

- **InForce Justice Suite™** -- enabling criminal justice information sharing;
- **ChildBase®** -- for investigating and prosecuting child pornography cases;
- **CABS™** -- a computerized arrest and booking system for law enforcement; and

At Imagis, our mission is to *simplify*, *accelerate*, and *economize* the process of connecting existing, disparate information assets, and unify access to this knowledge with a single, integrated user interface enhanced as appropriate with a variety of biometric tools. Contact us today to learn more about how we can help you simplify your identification and data sharing requirements.