

HOUSE OF LORDS
MINUTES OF EVIDENCE
TAKEN BEFORE
THE SELECT COMMITTEE ON SCIENCE AND TECHNOLOGY
(SUB-COMMITTEE II)

PERSONAL INTERNET SECURITY

WEDNESDAY 10 JANUARY 2007

MR JIM GAMBLE, MS SHARON GIRLING and MR TIM WRIGHT

MR JOHN CARR

Evidence heard in Public

Questions 197 - 260

USE OF THE TRANSCRIPT

1. This is an uncorrected and unpublished transcript of evidence taken in public and reported to the House.
2. The transcript is not yet an approved formal record of these proceedings. Any public use of, or reference to, the contents should make clear that neither Members nor witnesses have had the opportunity to correct the record. If in doubt as to the propriety of using the transcript, please contact the Clerk to the Committee.
3. *Members* who receive this for the purpose of correcting questions addressed by them to witnesses are asked to send corrections to the Clerk to the Committee.
4. *Prospective witnesses* may receive this in preparation for any written or oral evidence they may in due course give to the Committee.

WEDNESDAY 10 JANUARY 2007

Present

Broers, L (Chairman)
Erroll, E
Harris of Haringey, L
Hilton of Eggardon, B
Howie of Troon, L
Mitchell, L
O'Neill of Clackmannan, L
Sharp of Guildford, B

Witnesses: **Mr Jim Gamble**, Chief Executive, and **Ms Sharon Girling**, Team Leader and Law Enforcement Officer, Child Exploitation and On-line Protection Centre; and **Mr Tim Wright**, Head of Computer Crime, Home Office, examined.

Q197 Chairman: Welcome everybody, particularly our witnesses today. I would like to welcome Mr Wright back and Mr Gamble and Miss Girling, and welcome members of the public who are attending this session. There is a document available that describes this inquiry. I am Lord Broers and I am Chairman of the Committee. Everybody should note that we are being webcast today, just for your information. If we could start with our witnesses please introducing yourselves and then, if you wish, making a short statement. Shall we start with you Mr Wright?

Mr Wright: Good afternoon. My name is Tim Wright from the Computer Crime Team in the Home Office.

Mr Gamble: My name is Jim Gamble and I am the Chief Executive of the Child Exploitation and On-line Protection Centre and I am the Association of Chief Police Officers lead for countering child abuse on the internet.

Ms Girling: I am Sharon Girling and I am a Law Enforcement Officer from SOCA and I work within CEOP.

Q198 Chairman: Would you like to make an opening statement?

Mr Wright: Just briefly. The internet offers real educational and social benefits to children, as well as being a source of entertainment and helping develop skills they will need in the future. The Government is committed to ensuring that they can exploit those benefits safely. To do this, the Home Secretary set up in 2001 a Task Force to bring together Government, law enforcement, industry and child protection organisations to work on child protection on the internet. That partnership approach has been effective over those years and in that time has delivered good practice for different companies that provide a variety of on-line services: chat; moderated chat; instant messaging; web-based services; and most recently social networking services. It has very nearly delivered a BSI kitemark for products to help parents manage how their children use the internet. It has delivered training packages for police, prison, probation and social work professionals. It has delivered various public awareness campaigns aimed at parents and children to identify the risks and provide practical advice on how to manage them. The UK ISPs and the Internet Watch Foundation have effectively ended the hosting of websites containing illegal images of child abuse in the UK and the majority of the biggest broadband and 3G mobile network operators have put in place technical measures to stop UK customers accessing these websites when they are hosted abroad. Obviously the biggest development over those years has been the creation of CEOP which we will talk about. The Government set up CEOP to build on that partnership approach and to deliver a step change improvement in our operational capacity to protect children.

Mr Gamble: I do not wish to add anything just simply to associate myself with the comments that Mr Wright has already made.

Ms Girling: And I the same.

Q199 Chairman: We were told by the Government in November the importance of individuals taking personal responsibility for their own internet security. Who is responsible for protecting children on the internet?

Mr Wright: Broadly the same answer. It is a shared responsibility in exactly the way as off-line safety is, and that underlines part of the partnership approach we have talked about. Obviously the Government has an overarching responsibility to provide a framework of legislation and agencies to ensure that everything is done. Law enforcement and National Offender Management have a responsibility to reduce crime, to investigate offenders and to manage the risks those offenders pose in the community. Any company or individual providing a service to children has a responsibility to ensure that their children can use that service safely. Finally parents themselves and children have a responsibility to make sure they are safe. As professionals, I think we have a responsibility to help parents and children in this, through ensuring that on-line services have clear links to safety advice and how to report abuse but also by raising awareness of the risks and providing practical advice. Over the last five years a number of organisations have delivered awareness and advice both to parents and to children. We have worked to ensure that these efforts are consistent and complementary as well as running our own campaigns. While the services that children use change over time, the three key underlying messages remain the same. It is more difficult to check out who you are talking to on-line than it is off-line and there are people out there who will exploit that. This is particularly important when children think about meeting on-line friends in the real world. Personal information you give out or a child gives out can then be used to contact them in a way later on that they cannot then control. And finally parents need to engage as much as they can in the way that their children use the internet, both to understand what the children are doing, who they are talking to, but also so their child is more confident in turning to their parents if something goes wrong.

Q200 Chairman: That brings to mind the fact about parents themselves and who is responsible for educating parents. The evidence that we have had from the Children's Charities Coalition says that while a third of children regularly use blogs two-thirds of parents did not know what blogs were. Similarly almost 80 per cent of children use instant messaging but only a third of parents knew what instant messaging was. Given the rate of technological change can adults be expected to keep pace with the risks facing their children on-line?

Mr Wright: There are a number of questions in there. I think parents will always be behind their children because children are early adopters and tend to have more time to pick up new services. So parents will always be behind and older generations will always be behind their children. I think in terms of the detail of specific services and how kids use them - and certainly that research is consistent with everything else we have seen - the core safety message is that parents understand about safety and protecting their children, what they find difficult is applying that in the on-line environment. In terms of whose responsibility that is, it is a shared responsibility. Government, education, law enforcement, service providers all have a role in helping do that. It is an on-going battle for us.

Q201 Chairman: You do not think it would be valuable to have specific proposals that schools for example should run classes for parents, voluntarily of course?

Mr Wright: Some schools have tried but, anecdotally, take-up amongst parents has brought that to a close. I think it is a good idea. From people I have talked to it is difficult to get parents to come into schools after hours and do it. Some parents will come and do it but they are the parents who already understand the issues. It is a good idea but we have not found a way of doing it successfully.

Mr Gamble: I think the issue here is demystifying some of the terms that we use about technology today. Tim is right, parents will understand a threat as it manifests itself to their children in the world that they grew up in and that they understood - the threat in the public

place after dark. Talking about blogs sometimes is not helpful; talking about a diary, a parent understands that. So how do we engage them in a way that helps them develop a better understanding? We should be through our role encouraging them to be good parents in the sense that parents always were - to communicate with their children in a way to achieve better understanding. From the schools' point of view they need to imaginatively engage with technology so that the child's school report is delivered to the parent in the 70 per cent of homes that has on-line access in this country via e-mail as well as in the written form so that we are engaging them using the technology that we are speaking about in a positive and influential way. I happen to know that BECTA in the competition that they run to identify those schools making the best use of ITC, identified two schools who were joint winners and one was school was Ballyclare High School in Northern Ireland, and one of the questions that they asked the panel and one of the probing issues that they sought out was how they engaged with parents about the use of technology and how they used that technology to engage the parents. I think that is one of the ways that we see by being imaginative and engaging parents they are indoctrinated into the technology. The National Children's Homes' survey has shown that there is a massive gap between the knowledge that children have on-line and the knowledge that their parents have. We are never, ever going to be able to run technology classes to the degree that the parents can close that gap, but we can encourage them to understand it more effectively by simplifying it.

Q202 Chairman: You could almost get value, if these numbers are correct, by sending each parent half a sheet of A4 explaining what some of these things are.

Mr Gamble: Let me give you an example of one of the initiatives that we are running at the Child Exploitation and On-line Protection Centre. We recognise that we cannot police the internet so as a serving police officer I recognise that the police cannot make all of our citizens safer on every corner of the information superhighway. Social services cannot, even

industry by and of themselves with “safer by design” technologies cannot do that. We can no more be on every street corner in London than we can be on every street corner in the internet. What we can do however is identify those individuals who are at the greatest risk and we can empower them by engaging them in a way that delivers information that makes them safer. We are currently running an education campaign which is modern, it is contemporary media, using modern music and modern film in a way that engages young minds emotionally and intellectually, so that when the one million children we will engage by the end of this school term leave the classroom they will understand the nature of the threat. They will understand yes, go on-line, have fun, learn - those are the skills that are going to enable you to develop careers in the future - but they will also know where to go and when to report and, more importantly, what to report. Through that programme we are asking schools that when we engage with those children face-to-face that they are given a homework which involves sitting their parent down at the computer and saying, “This is what I have been asked to do today,” and simply asking the parent to spend ten minutes through the Think you Know education campaign by allowing their child to take them for a walk on the internet and showing them that site. By simply doing that and by reviewing the top tips, a parent and a child will engage in a constructive conversation that will leave the parent better informed and the child reassured and perhaps given some more advice by the parent. I think that is the type of programme of work that we need to be involved in and we need to be influencing as many schools as possible to take it up.

Q203 Chairman: Do you think more can be done through regulation, for instance the Children’s Charities Coalition argue for filtering products to be pre-installed on all computers and set to a high default security setting. What is the Government’s view of the regulatory approach to these issues?

Mr Wright: The Government's approach is self-regulation where self-regulation is the best approach. In terms of filtering and safety products, we are close to finalising a BSI standard which will apply for these products to be accredited against because at the moment there are a lot of products out there and they vary in clarity and quality and parents are not well-equipped in choosing between them, so by having products that are accredited against a standard parents understand parents will be better able to choose between them. In terms of pre-installation, the next thing is to look at making sure that as many parents as possible are using them. Pre-installation is obviously one way of doing that and the Task Force is setting up a new group within that to look at how we drive the take-up of safety software, and pre-installation is one of the options on that.

Q204 Lord Mitchell: What is the view of manufacturers to that, are they co-operative?

Mr Wright: The manufacturers of the safety products have been very co-operative in developing the BSI standard. We have not got as far as talking to manufacturers and retailers of PCs about pre-installation yet, but understandably the people who provide these products have been very co-operative in developing this BSI standard.

Mr Gamble: The reality is that there is a commercial imperative in delivering software which is safer for families. People go and buy software on the basis of it being utilised positively by the whole family and the children in particular. So if you are someone that is selling something that people know is inherently safer then there is a benefit to doing that. In the Child Exploitation and On-line Protection Centre we partner very closely with industry and we have found that partnership to have massive benefits for us whereby we develop an ethical mutual interest in making children safer and we develop an ethical mutual benefit through that sharing of knowledge that allows us to inform them about where the risk manifests itself. Let me give you an example. Through the reports that we get into the Centre we are able to identify trends, themes and patterns. From that we are able to talk to manufacturers about

where the threat perhaps manifests itself at any particular time. So that we know that internet relay chat, instant messaging, is the environment where children are most likely to come into contact with a predator who wants to engage them. By working with one of our partners - Microsoft - very, very closely we were able to get them to sacrifice a space where they could advertise and gain a significant amount of revenue over a year to put our “report abuse” button in so that if you are a child in that environment and you are threatened by an inappropriate advance you are able to click on that button, initially get direct advice from us and then secondly report your suspicions. In the week that mechanism went on-line our reports went up 113 per cent. By working constructively with industry - we work very closely with Vodaphone, BT, AOL, Microsoft and others - we have found that we are able to gain a mutual benefit that I am not sure would be gained in the same way if we went for a regulatory approach. I have to say at this stage with my experience in the recent past, I do not support regulation per se.

Q205 Lord O’Neill of Clackmannan: Given that a lot of schools have pretty old computers and do not replace them very quickly, how confident are you that you can ensure that the software of the kind you have just been describing can be incorporated into school IT systems on a regular basis? Can you disseminate that information? Can you get it out? Are teachers able to load it onto the computers for the youngsters in their classrooms?

Mr Gamble: There are two different issues. The first is the stuff that can be bought commercially and we are working with the Home Secretary’s Task Force and others to encourage manufacturers to meet certain standards so that people can be simply reassured and understand that that is safer. In the institutional environment, be it schools or care homes where many children are very vulnerable, we are working with some of the boards so that they better understand the nature of the threat. I know working with Vernon Coaker’s office we are keen that by the end of 2007 at source many of the industry partners will have some

form of blocking technology, and we are developing other initiatives which recognise that every provider will not be able to deliver that in the same way. In schools I can tell you this week the DfES have advertised for a grade seven member of their staff to work within our environment in CEOP so that they can engage with schools and ensure the safety messages that we are delivering and the guidance we are giving about what you should and should not do in schools goes direct to them. More importantly, I think in the longer term one of the key recommendations from this must be that this type of safety message is embedded in the national curriculum, and not just under information communication technology because it is about social responsibility. Let us not forget that technology is neutral. It is people who will abuse it or use it for positive means.

Q206 Baroness Sharp of Guildford: I wonder whether you could tell us a little bit more about CEOP since its inception in 2006. For example, precisely what is its role? What sort of resources are available to it? Are those resources adequate to the tasks that you face in this programme of trying to reach one million children with the message that you are trying to get over?

Mr Gamble: CEOP's primary aim is to identify, locate and safeguard children and thereby reduce the harm that they might otherwise face. It was built on the back of lobbying from groups not dissimilar to this one. It certainly represented the Home Secretary's Task Force, children's charities and the Police Service and industry itself. It was built to be different. We have constructed around three principal faculties. The first one is recognising that information in this area needs to be better managed and better shared, so the principal faculty is the intelligence faculty where we bring information in from police forces in this country and from abroad, from NGOs in this country and abroad, from industry partners in this country and abroad, and (since the launch of CEOP) directly from young people themselves. When we first launched we were getting about 21 per cent of the reports that came in from

people below the age of 18. Today that number is up to over 40 per cent so bringing that information in, applying that analysis, identifying where a child might be at risk and identifying where an individual represents a risk to that child has resulted in national child protection operations where we have rescued eight children from contemporary hands-on abuse and arrested many, many more offenders. Bear in mind that academic studies will tell you that the average offender in the real world will offend against about 73 children, and I would say that is a conservative estimate, in the span of their offending career. The information, how we manage it and how we share it is critically important and are areas that we need to improve on. From that collection of information we create our second faculty which is our harm reduction faculty. Now that we better understand the nature of the offence, the nature of offender and the environments on-line and off-line where that is committed, it is about how do we create a safer by design technology, and we touched on that earlier. We have a safer by design team that works with industry and works with the Home Secretary's Task Force to encourage the sharing of information that can be translated into safer technology tomorrow, and we do that working very constructively with industry. That faculty deals with our education campaign. We could never reach one million children by ourselves so we cascade it out and we create and validate the product working with industry, working with charities and working with others. We make sure that it is contemporary and we have a youth panel presently of 60 young people made up of all of the diverse communities that represent the UK and we intend that to grow to 150. They come in and they advise us - does this touch you, does it grab you intellectually and emotionally in a way that would change your behaviour - so we listen to what young people say and we construct much of the stuff that we do on-line with their advice. That is situated in our harm reduction faculty. We have trained over 1,300 specialists in the UK from the Police Service, social services and charities around issues about understanding sex offenders on the internet, interviewing sex offenders,

and other training courses that we deliver. Our victim identification team is based in the harm reduction faculty. Those are the individuals that will take information from a police force, so seizing a computer in Manchester with thousands upon thousands of images and apply the lessons that we have learned in some of the operations that we were associated with earlier on to say how can we identify and locate and rescue the child. That is done by taking that information, applying an analysis on the clues that are available, and so far we have identified five children from that and we have 19 on-going investigations in that regard. That all sits in the harm reduction faculty with our academic team who work on a research basis to help us better understand why people commit these offences and how we can interdict with them at an earlier stage to make a difference. The final faculty is our operations faculty and that is where we house our financial investigation team, supported by Visa International. We would be unable to deliver that on the basis of our core funding were it not for the significant financial and intellectual support that Visa International bring to the table. That is where we would target those individuals that operate in a pay-per-view environment treating child abuse images as a commodity. We now attack them in the same way we would have before a drug dealer who uses cocaine or heroin as a commodity. We also use that specialist resource to identify patterns of life. If you are a sex offender, where are you going, what are you buying, what are your intentions about travelling? So we build that picture up and it helps our offender management team help the multi-agency public protection panels when they look at the most high-risk offenders. We have a second team which is our covert internet investigations. They at this moment in time are engaged with counterparts across the world - Canada, America, Australia, Italy, with Interpol - where we are engaged in infiltrating those paedophile groups in the real world who use and abuse the technology to share information with one another to minimise and self-justify the behaviours that they enact, and to help identify, interact with and locate children they can reach in the real world. So that group is

infiltrating as we speak and you will see over the months that follow the results are going to be outstanding and the evidence will be available in the public arena in the not-too-distant future. Finally we have an operations support team there that go out to forces providing forensic behaviour analysis support and also providing co-ordination support in this country and abroad where we are able to raise levels of awareness. After all I have said you probably think I am going to say we have got several thousand people. The Centre is about being more intelligent as opposed to being simply larger. There are between 80 and 100 people currently working in the Centre from a variety of backgrounds including the Police Service, the Serious Organised Crime Agency. The NSPCC has embedded a significant number of its personnel in our premises. Microsoft has embedded a significant number of their personnel working for us within our premises. Different government departments are represented within the premises so it is a partnership that manifests itself in reality every day across a desk and not at a meeting you might or might not attend once a month. Hopefully I have not gone on too long and that has given you a feel.

Q207 Baroness Sharp of Guildford: In terms of resources, which was of course one of the questions I asked, I take it from what you say that it is a mix of public and to some extent private sector resources that you are getting? You were talking about Visa but you are also getting resources in from Microsoft and some of the children's charities.

Mr Gamble: That is correct and we could not operate without that support from industry, from the children's charities, and from others.

Q208 Baroness Hilton of Eggardon: Carrying on from that, clearly a lot of your work is reactive to information that you receive. To what extent are you able to be proactive and go out looking for paedophiles for example or other people who may be pursuing children and grooming them?

Mr Gamble: Through our partnership with the Virtual Global Task Force, which is a collaboration of international law enforcement agencies which I chair, we operate 24/7 on-line on the internet. That is undercover officers from Canada, America, Australia and the UK, shortly to be joined by a new partner I hope in Italy, sharing the patrolling time that we need where we will visit the locations where intelligence indicates to us that people are gathering that represent a threat to children so we engage them. That is low cost and high impact. What it means is that whilst we are working the Canadians are sleeping, they then take on the next shift, the Australians the one after, and we have the overlap with the Americans. It means as well that we are able to engage paedophile networks in a much more holistic way than we ever could before and we can call on resources to reinforce our activity that are not simply within our own jurisdiction because where we are proactive - and we are very proactive at present - we do that on the basis of attacking the threat, not on the basis of the geography of where it manifests itself. You cannot do that on the internet. You have to sacrifice a little bit of your own sovereign territorial responsibility. What people need to understand is as a child if I am a 15-year-old girl who exposes myself on a web camera to someone I believe is a 16-year-old boy, the offence has taken place and that image will be forever shared and as a 47-year-old paedophile I will use that image when I am engaging a 15-year-old boy to pretend that I am a 15-year-old girl and I will share that image pretending that it is me. So the perpetrator in that regard can be in Canada, America, Russia or Australia and can capture that image and that child is revictimised every time that image is shared or sold or swapped. We are looking in that regard at the value of an image, so when we capture someone who has a huge collection we can quantify what does that mean in a financial sense and can we use the Proceeds of Crime Act to remove the benefit that they have accrued from them and to make an investment in child safety in the future using those ill-gotten gains.

Q209 Baroness Hilton of Eggardon: What other organisations do you liaise with, the Internet Watch Foundation for example?

Mr Gamble: We work very, very closely with the Internet Watch Foundation here in the UK, and with charities large and small. We met with Barnado's yesterday about post-incident trauma counselling for children. We work with every government department, very closely with BECTA, very closely with DfES, very closely to the National Offender Management Team and all of the charities that you would imagine, headteachers' associations, the Football Association, anywhere where children will go we are able to engage and influence them. If you were to visit the CEOP centre, which I would really encourage all the Members to do, and test the DNA when you were there, the DNA would reveal partnership. There is nothing that we do that we do by ourselves. It is about this mixed ingredient that builds something which is significantly different, and the results that we have had to date evidence the fact that the proof of the concept that we have delivered in this first year needs to be significantly reinforced in the years to follow so that we can capitalise on the early success.

Q210 Lord Harris of Haringey: I want to pursue the question of whether there are adequate resources available working in the area of on-line child protection? Are there sufficient police officers? Are there enough police officers with the appropriate training? Is there enough appropriate equipment in the Police Service? Are there enough other staff, other agencies? Could you give us some indication of that?

Mr Gamble: First of all, let me say about the Police Service, do we need more police officers to be engaged in this work? Yes we do. Do they need to be in our building for example? No, they do not. Are the police of themselves necessarily the right people? What we need is more people with the right skills. Some of them will be police officers, others will be members of industry, others will come from social services with a particular understanding about the impact of harm on children, and some of them will be from government. We do

need more resources. We do not need massively large amounts or significant amounts of reinforcement. What we need is the right people in the right place and a more intelligent approach to co-ordinating our activity. The benefit the criminal sees in the internet is that they can be in many places at many times representing themselves in many different guises as different people. We can turn that against them. A small group of highly trained covert investigators can be many people in many places targeting many criminal entities, and we need to make sure that we get the best use of UK resources by more effectively focusing what we do around a tasking and co-ordination process, and we in ACPO are currently working on just that thing through our Countering Child Abuse on the Internet Group.

Q211 Lord Harris of Haringey: Operation Ore led to something like nearly 1,500 convictions in the UK yet I have also been told that it could have been a lot more but there was a resource constraint. What impact did Operation Ore have on police resources and on the wider criminal justice system at the time and what were the pinch points?

Mr Gamble: I think there is a lot of misinformation about Operation Ore and I welcome the opportunity to address some of those issues now. Operation Ore was a wake-up call. Operation Ore and the seeds for it were planted in the late 1990s when a couple in America who sold pornographic images to customers through acting as a web conduit found out quite by accident that they could make significantly larger amounts of money by selling abusive images of children, so they are organised criminals who are good business people because they divert to an area where they see the risks being lower and the profits being higher. We were not prepared for that in UK policing. I do not think social services, I do not think any of the institutions, even the academic ones, would ever have foreseen the fact that we were going to be hit with that number of suspects. Let us be clear, did we learn lessons in Operation Ore as a service? Of course we did. I think it is important to recognise that the volumes were unlike anything anyone had seen before in a single crime type and it was complex.

Sometimes people were seduced by the complex nature of it because it is the internet and you see it as a labyrinth and where do you go. I think historically there has been a tendency to say, “We cannot do anything about it because it is the internet. We cannot make a difference because this technology is something we cannot understand.” The principal lesson we learned from Operation Ore is this: the internet is simply another public place, it is like this room, and the internet is not good or bad; the people who occupy it at any given time will decide how good or bad it is. From a UK policing point of view, the lesson we learned is when you look at the suspects in these cases you have to categorise and prioritise them on the basis of those who represent the greatest potential risk to children. We did that and to date there are over 2,300 cases that have been dealt with through the judicial process and there has been a finding of guilt either through conviction in court or in just over 600 cases cautions. Police cautions are not given out on the basis of it being an easier route to reconcile and draw a line under a case. Police cautions are given out under national guidelines where there is a realistic likelihood of conviction and where the individual concerned has made a full and frank admission in the full understanding of the consequence of that. Anyone that accepts a caution for a criminal offence is guilty of that offence. Make no mistake about that. It is the same as if I am convicted today and say, “Actually I am innocent, I only pled guilty because I wanted to get it over in time to go and do something else or to move on beyond it.” Anyone who has had a caution administered is guilty. Operation Ore represents a success. Let us be very clear, 132 children were rescued from actual live time abuse. That is a success. The police however began to view it in a different way: should we in the future be focused simply on finding where images are? I do not think so. We need to adopt a different approach. It is people that put the images on the internet, it is not the technology. We need to be focused on the people who create the harm by taking the images in the first place because every image represents a victim. Every child is a victim in the first instance and revictimised in the second

instance. I think Operation Ore was great work by the British Police Service and I would want to give them credit where credit is due for that and dealing with a difficult and complex area of a new crime type or an old crime committed in a new environment whereby they were able to do something that rescued that number of children.

Q212 Lord Harris of Haringey: Could I stop you there. Certainly I was not trying to criticise the work you have done on Operation Ore; it is a question of whether more could be done. If it happened again with a similar sort of situation, could you take us through a little bit who takes the lead on this? Is it yourselves, is it SOCA, and I know SOCA has been criticised for allegedly downgrading its response to internet crime, or is it the individual police forces? How is that responsibility allocated?

Mr Gamble: The national responsibility as a single point of contact would be the Child Exploitation and On-line Protection Centre. The lessons that we have learned in dealing with Operation Ore have meant that it will be processed in a much more effective and efficient way. We learned lessons when we began to deal with what was an old crime committed in a new way previously, so that would come to us now. We have the mechanism and the infrastructure now to allow initial assessment of the intelligence and intelligence development to happen in a processed way. If you were able to visit I would be able to show you how that works, where we take the intelligence in, we establish whether there is a potential live time threat to a child and process it as a priority. Where there is not that immediate evidence, that information is then developed to a degree that we can decide whether or not a person has committed an offence. Let me give you one quick example. I mentioned to you that we are working on pay-per-view sites. We looked at a pay-per-view site facilitated in the UK. We were able to operate to a degree using undercover officers as well as financial investigation so that we were able to test the evidence prior to making arrests. Without going into the detail of cases that are still in court, I can say that in those cases the full and frank admissions that were

made immediately evidenced to me as a serving police officer that that is an improved process, an improved way forward. We would not have got there without experiencing Operation Ore. Also it is worthy of note that in many, many cases where we have investigated, and we are duty bound to investigate them all, we have taken no further action where there is a doubt. We have given the benefit of that doubt to the suspect, as is right.

Q213 Lord Howie of Troon: You have partially answered my question which was, was this a new crime or an old crime using a new medium?

Mr Gamble: When I knew I was coming here - and this question is asked a lot - one of the interesting issues, and I do not want to waste your time, is that in 1874 a local photographer in the Pimlico area, Henry Hayler, had over 130,000 photographic images seized held on 5,000 glass plates. Those pornographic images included images of him, his wife and his children, so it is a crime which has been with us I think always. It is a crime that the internet allows those who are motivated to do so to exploit to a different level and to a different degree, but the good thing is this guy Henry Hayler left the jurisdiction and we believe he either went to Berlin or New York where he continued to share images for some time and in today's world the forensic contact with the on-line environment would give us many, many clues to track him. The relationships that we have through the Virtual Global Task Force, through our participation in G8, and through our partnership with Europol and Interpol would mean the likelihood of him remaining at large until he wrote his journal and subsequently died would be strictly limited.

Q214 Lord Howie of Troon: If it is an old crime in a new way, do you need new laws or can you catch the perpetrators using the laws which exist?

Mr Gamble: In most instances we can use the laws that currently exist. If you take the public place analogy, people will go to and frequent a public place, sometimes on payment or

otherwise, but it remains in essence a public place, and the common law and the precedent that has been set over the years is something that we should not easily move away from. Where we have needed law that is more flexible and that understands the technology, such as grooming and the sexual offences legislation, then we have found Government and others very willing to be flexible and to look at that in a different way. Through the Home Secretary's Task Force a particular subgroup continues to look at that and we are considering cartoon images, for example. In the future we are going to have to look at the written word and the harm that can be conveyed by an obscene publication in that way in the on-line environment. You might want to consider for example as a question, is it right that as a 47-year-old man I can go onto the internet tonight and pose as a 14-year-old to talk to a girl who is 13? Forget about sexual intent, is it right that I should be able to do that? Why would any 47-year-old man ever want to engage with a 13-year-old girl whilst masquerading as a 14-year-old boy. I think without lawful authority or reason you should not be allowed to do that. So do we need to look at other aspects of the law? Yes we do. Have we found the system to be willing to consider and contemplate how those could be developed? Yes we have.

Q215 Lord Howie of Troon: Have you any proposals for new laws?

Mr Gamble: I have a number of proposals that I would like to make before the end but none of them relate to new laws. To be fair, it is not about new legislation. It has got to be about new thinking in this environment and that is what we have found to be far more effective.

Mr Wright: We have been very keen to review the law and see whether it is fit for purpose. Just to clarify what Jim said, the Home Secretary is currently consulting Cabinet colleagues about whether to ban the possession of computer-generated images of child abuse, including cartoons and other graphic illustrations of children being abused.

Q216 Lord Howie of Troon: So possession rather like possessing cannabis?

Mr Wright: Yes and at the moment the possession of real images is illegal but the possession of computer-generated images is not illegal.

Q217 Lord Howie of Troon: Is that really because e-crime is scarcely recognised?

Mr Wright: I think it is because the original legislation was about protecting children and an image of a child being abused is directly related to protecting that child because the child is harmed and abused in the creating of the image. In computer-generated images it is rare for a child to be harmed in the creation of the image so the legislation grew up differently but now we think we should ban the possession of those as well.

Q218 Lord Howie of Troon: Could you give me some notion of the size of the problem? Is on-line child abuse getting worse or increasing? You mentioned something like 132 children. I do not wish to disparage your work but that is not terribly many children.

Mr Gamble: But that is Operation Ore and if you look at the number of individuals arrested and acknowledge the fact that over their lifetime of offending academic evidence would indicate to us that they offend against many children. Let us look at a recent case. Lee Costi was convicted in Nottingham last year, a young man who had gone on-line and habitually engaged with 13 and 14-year-old girls and whose method of operating was to engage them on the internet and then to meet them at a train station where he would engage in sexual activity with them. If you look at the computer hard drive and you examine it, you will see that he had conversations with many, many, many young people all of which, given the right circumstances at the right time, could have led to offending, so the preventative technology here is important. Secondly, people sometimes become confused by saying you are misdirecting child protection activity here because the real harm takes place in the home or in the broader family circle. They need to recognise the fact that a computer (which is in 70 per cent of homes which gives on-line access) allows children to form intimate relationships in

the way they once only did with close family and friends living in the proximity. So is it a problem that is growing? I do not think it is. Is the profile of it growing because people are becoming more aware? I think that is the case. Our job is more about child protection however than about technology and one of our great fears is that sometimes we become so seduced by the technology in these issues that we lose sight of the issue which is protecting children no matter which environment they happen to be in at any given time.

Q219 Earl of Erroll: I was going to ask about whether the existing laws were adequate for dealing with people acting illegally on-line dealing with people accessing illegal on-line content but I think you have really answered that. One of the things that concerns me is that some of the evidence of some of the stuff that is going on can be discredited if you start accidentally bringing innocent people into the net, and it was said that there were a certain number of people whose credit card details were held by Landslide Productions (which led to Operation Ore) where there was no evidence they had accessed any illegal content and yet they were in some cases apparently hounded. There was also I heard word that some of the images that were found on computers may have only been sitting in temporary internet files because they were hidden behind thumbnails on the front page and people had not actually gone into that part of the website. Do you have any comment on that?

Mr Gamble: In order to access the Landslide website there was a process that you had to go through. Let me say for the record I am speaking generally now because it would be inappropriate when there are still some cases pending for me to go into detail. The principal operation of Landslide was simply this: you went on; you identified what you wanted; you handed over your credit card details and you were sent a password back to your e-mail address which you had; you then went back on-line using that password which had been sent to your computer and then accessed your chosen choice. People have said, "Well, it said here 'click child porn', and it did not." In some cases of course it did not; in some cases it said

'click here for child rape'. Where those people have been investigated, they have been investigated first and foremost because there is a reasonable ground to suspect that they may have committed a crime. They are not guilty in the first instance. That case came to what was then a paedophile investigation team and went out to an individual police force. The individual police force independently assessed the evidence and independently investigated it. At the end of that independent investigation that information, including the process by which they accessed the site allegedly, went to the Crown Prosecution Service which independently assessed the veracity of the information placed before them and whether or not there would be a likelihood of prosecution. Once they had made their decision it went to the court system where a judge made a decision independently about the veracity of the evidence produced by the prosecution and the information provided by the defence. It is common practice in many cases - and I have been a law enforcement officer for over 26 years - to try and discredit an operation of any type, not least this type in a new area. I would not want to associate myself with any investigation that manifested itself in the way you described, and that does not bear any resemblance, in my view, to my actual experience of this investigation.

Q220 Earl of Erroll: Can I just say this was not an attack on the police or the police involved or you yourself at all. It is perfectly possible, given the technology involved and the complexity of the way some things would be accessed, that mistakes can be made, particularly as this was a new area for many of the investigating police so therefore it is quite possible that these things could have happened. A very quick question then, there was no other sort of pornography on that website, it is purely child pornography? I have never visited it so I do not know.

Mr Gamble: I am glad because we would have met under other circumstances perhaps! Let me be very clear here. Without going into too much technical detail, which I think would be unhelpful, was there ever a doubt about a particular aspect of a particular part of Landslide?

Yes. Were they ever pursued or prosecuted? No. So where we identified in that investigation a doubt we then took action to make sure that those individuals were removed from that cloud of suspicion. The difficulty here is we understand, and we understood at the time, you cannot make this allegation and then withdraw it easily and put somebody's life back together. We understand that and that is why there is a lot of due diligence and that is why it takes a lot of time.

Q221 Earl of Erroll: Is there possibly going to be a problem with the amount of credit card theft - identity theft as people have re-named it - that is going on at the moment? Is that going to be an increasing problem in future investigations firstly making sure that the credit card details were not stolen?

Mr Gamble: We never prosecute someone simply on the basis of their credit card being used. You are going to look at all of the circumstantial evidence which when taken together provides overwhelming evidence. No, I do not think so and I also think that the pay-per-view industry is moving away from the simple credit card transaction. We are looking at other mechanisms whereby they can hide the activity they are involved in. So I do not think that that will be a problem in the future.

Q222 Lord Mitchell: I was interested in your view on the emerging threats to child safety, for instance as a result of the extension of connectivity to an ever-wider range of devices. By that I am sure we mean mobile phones, wi-fi connected iPods, devices like that.

Mr Gamble: It does not matter what the technology is. We need to move away from looking at the apparatus that actually delivers it, whether it is the mobile phone that is the brick or the new one that you can listen to your music on and also get onto the internet and check the football scores with. What this is about is the threat that will emerge which is one of ignorance and perhaps arrogance on behalf of the Police Service and others in positions of

responsibility where we assume that we have done enough and where we assume that children know enough. I go back to what I said before, I believe the best way of dealing with the emerging threat is through education. It is through engaging with children and actually listening to them. The youth panel work that we are doing, listening to academia, listening to young people about the way they occupy this new space and capitalise upon it in a way that helps them identify what the risks are and helps them contribute to the solution. 30 per cent of the reports we receive in the Centre are not about the technologies themselves and are not about something that industry creates; they are actually about the way children behave in that particular environment where they are given scope. It is about some of the self-generated content that they will share with others, and that is about education. That is about what you talked about earlier, talking to parents. A parent may not understand what a social networking site is. A social networking site is a fantastic place for young people to keep in touch when they go to university with their friends at home and elsewhere. Some criminal element will try and take advantage of it. I ask you this and I say this to parents: would you allow your child to wear a billboard or sandwich board, or whatever you want to call it, with their home telephone number, all of their personal details on it, and some handout photographs that they would walk from Victoria Station down to Oxford Street with whilst every Tom, Dick and Harry in the street could see them? You would not. That is about educating people and simplifying and demystifying the aspects of technology that we tend to lean towards in these debates.

Q223 Lord O'Neill of Clackmannan: You mention that because of international co-operation you can now have 24/7 sharing of a lot of the monitoring. How much further do you think you need to go in this area of international co-operation?

Mr Gamble: We need to build on the Virtual Global Task Force partnership because one of the questions about the numbers involved means that the long arm is able to be that much

longer. I can say, without divulging too much, that we are currently investigating hundreds of suspects in on-line environments at present who are trying to access children because of that partnership. I believe Italy will be full members within a short period of time. We are working through the G8 initiative and those infrastructures that are already available to see how we can expand. The key in the next phase of development is going to be engaging countries that are not as technologically advanced as we and some of our partners are and recognising that what we see here are symptoms of crimes, and the root cause sometimes in their jurisdictions, and we need to support them build an infrastructure that means they can play a full part.

Q224 Lord O'Neill of Clackmannan: Are you getting the co-operation from all of the countries that are as technically advanced as we are? Are other countries within, say, the EU that have fairly sophisticated IT environments all playing their part or are there still some people who perhaps are not as conscious of the nature of the problem?

Mr Gamble: I think there are some places that are not as conscious but everybody plays a part in protecting their own children. I have been involved in my career in many types of crime ranging from terrorism to organised criminality and I have not been involved in any area where you get such a degree of enthusiasm and willingness by agencies, voluntary and government, in jurisdictions because protecting children is something that everybody can relate to. We do need to get better at it and some individual states need to recognise that they cannot protect their own children within their own geographic boundaries. The partnership needs to rise above that.

Q225 Lord O'Neill of Clackmannan: If you think about it, the creation of CEOP is in itself a recognition that this is a particular type of crime, but is there still a danger or are we still in the position where this form of crime is seen as part of the general e-crime agenda?

Mr Gamble: I think there is a danger that it is seen as part of that and we would not want it to be perceived as such. I think the label e-crime is unhelpful. E-crime should relate to those new crimes which are truly facilitated by the technology - the phishing and those types of attacks that you will see perhaps. From my point of view, and I was previously the Deputy Director-General of the National Crime Squad and I have some experience with the build of the National High-Tech Crime Centre, the Child Exploitation and On-line Protection Centre is about protecting children, it is not about the technology. The technology assists us and we use it to positive effect but I would not want the work that we do to be seen as e-crime.

Q226 Lord O'Neill of Clackmannan: In the international context does that position prevail as well? What you said holds good for the UK but is it the case across the forces with whom you are in most close contact?

Mr Gamble: No, it is not the case. In some areas I think they are moving to that more holistic approach. We have had visits from other jurisdictions from some other parliaments to look at the UK experiment with CEOP and that has been extremely positive. Our colleagues in America through the National Center for Missing and Exploited Children again are focusing on the child aspect and bringing technology to bear as a constructive tool, but no, it is not recognised, and one of the problems with technology is everybody always defaults to it. The technology itself is not relevant. It is like trying to place a certain crime in a particular geography. It is about how we capitalise on the techniques that allow us to protect our children because very often technology will be used to lure a child from the virtual world into the real world and if you divide the way you deal with that then you undermine the activity.

Q227 Lord Howie of Troon: You mentioned the United States a moment ago. We are told that more than half of child abuse image websites are hosted in the United States. What is being done about that over there?

Mr Wright: I think it is fair to say that despite best efforts and the sophisticated tracing techniques used by the IWF it is not always possible to be categorical about where a site is hosted. A lot of websites, particularly the commercial ones, move frequently between jurisdictions as part of their efforts to avoid disruption or detection. This is a subject that the UK Government and agencies continue to raise with other governments, including the US, for example, through the G8 where justice and home affairs ministers gave a commitment to redoubling our efforts to combat the availability of these images. It is always difficult to judge other countries' approaches but the US Government over the last few years is attaching increasing priority to this issue. Nearly a year ago it launched its Project Safe Childhood to enhanced its national response to "combat the proliferation of technology-facilitated sexual exploitation crimes against children". The project brings together federal resources, NGOs, and state and local law enforcement through a national network of Internet Crimes Against Children Task Forces with additional federal funding. The project includes integrated federal, state, and local efforts to investigate against individual people exploiting children, better community awareness, better education and better training for law enforcement and has led to every law enforcement agency developing significant operation initiatives against child exploitation. The US House of Representatives' Committee on Energy and Commerce conducted recently a hearing on "Making the internet safe for kids: the role of ISPs and social networking sites", which has looked in detail at the hosting of images in the US and taken evidence from ISPs and NCMEC about this issue. Additionally, the National Center for Missing and Exploited Children has begun sharing the signatures of known child protection images with ISPs so those ISPs can start to eliminate the individual images from their systems. In summary, a lot of images are still hosted in the US but we are starting to see from the US Government a different and a much stronger approach to attacking it.

Q228 Lord Howie of Troon: Our Government presumably is encouraging the United States to deal with this?

Mr Smith: Absolutely. I have seen it on a number of occasions. It is diplomacy and you can only encourage but we have been encouraging them for longer than I have been in this job and we are starting to see action on the ground.

Q229 Lord Howie of Troon: How long have you been in the job?

Mr Wright: I have been in this job for nearly five years.

Q230 Lord Howie of Troon: Are there any other blackspots apart from the United States?

Mr Wright: In terms of hosting of images, it moves around quite a lot. Russia sometimes and increasingly Japan and increasingly Spain now are part of the problem, but I think there is a danger in focusing too much on in which country the server is where the images are because it is trivial to host any form of website in any country around the world, and moving it is \$30 and half an hour's work. These sites will always be moved to the places where they think it is the safest for them, where the ISPs will provide less information to law enforcement, so even if a poor country is identified overnight, in terms of people accessing the images there would be no disruption because they will all be hosted in four different countries. I think it is about building co-operation globally, it is about attacking the people behind the images, the companies putting the images up, and most people are not based in the countries in which the website is hosted. The other thing which we have done in the UK very strongly is looking with the ISPs at blocking access to images wherever in the world an image is hosted. The majority of UK ISPs will now block access to images wherever they are hosted because while we have pretty much eradicated the hosting of these websites within the UK they were still as accessible to UK residents as they were before, so what the UK ISPs have done is said, "You tell us where these images are and we will block access to those images wherever in the world

they are,” so even if those four countries cleaned up their act and it is four different countries next week, people in the UK will find it harder to access those websites.

Q231 Lord Howie of Troon: In records, does the style and taste of the images depend on the country from which they come?

Mr Wright: No. I do not think there is a difference between the country from which it comes and the country where it is hosted, but I think Andrew has more knowledge about the images.

Mr Gamble: Let us be clear, to adopt a position whereby we were to suggest that the United States was in some way well behind everyone else would be fundamentally unfair. The vast majority of the internet infrastructure is based in the US, so the key word here is that a majority of those sites will ‘appear’ to be hosted in the US, and I think technically we need to be very careful what we say there, they will appear to be hosted in the US. Images will be the same. They will be horrific and that is why we in the UK are very positive about not using the term ‘child pornography’. We do not believe that what we are talking about is child pornography. Pornography is something which, depending upon your moralistic view, may be legal or not. This is not about consenting adults performing an act for the gratification of a third party on payment. This is about children as young as weeks old, sometimes unfortunately even younger than that, up to their early teens where they are physically abused in the most horrible sense by adult males. One of the things I find most disturbing, and we see a lot of images to put this in context, is a young teenage girl in a video we currently are working on who talks as if she is a 40-year-old prostitute. That child has been so badly treated and so heavily indoctrinated into the darker side of producing these types of images that she now behaves in a way that you would imagine if you were looking at it for the first time, that she was somehow complicit, but she has been victimised over so many years. The US in many senses has led the field in some of the initiatives it has brought together, partnering with industry. When we built the Child Exploitation and On-Line Protection

Centre, we looked at the model of the National Centre of Missing Exploited Children to see how they did what they did and how we could apply the best parts of that here in the UK. They are active partners, they are members of the Virtual Global Task Force. On Monday of next week, an agent from the Department of Homeland Security will begin in the Child Exploitation and On-Line Protection Centre here, a physical manifestation of that partnership. We work in close partnership with them and we are able to use the technology to make that partnership a day-to-day exchange of information.

Q232 Lord O'Neill of Clackmannan: You mentioned what you thought would be desirable in incorporating internet safety in the National Curriculum. The impression I got was, therefore, that it seems a somewhat patchy process at the moment. Is internet safety covered in the school curriculum in any organised way and at what age do the signals start being sent, the warnings?

Mr Wright: There is flexibility in the ICT programme of study to include teaching about internet safety to pupils. Schools are encouraged to integrate e-safety messages across the curriculum and implement policies and safe practices on internet use, and teachers are provided with the resources to reinforce responsible use of the internet. The Qualifications and Curriculum Authority have adapted ICT schemes of work and guidance to strengthen the message about internet safety. DfES have worked with the QCA and Becta on developing resources and guidance for schools, for example, under the Internet Proficiency Scheme, and the *Signposts to Safety* publication provides advice on teaching internet safety at Key Stage 3, which is 11- to 14-year-olds and Key Stage 4, which is 14- to 19-year-olds. The scheme is a specific way of developing safe and discriminating behaviours when using the internet.

Q233 Lord O'Neill of Clackmannan: So it does not start until the age of 11?

Mr Wright: It can be taught earlier. It fitted into the curriculum there, but I do not think that it is taught at every school.

Q234 Lord O'Neill of Clackmannan: At the moment you are saying it is taught through the medium of the subject ICT and it is not taught as children are learning to use computers, as they are, at primary school? It does not seem to be happening there. It may well be happening, but it is not happening in any organised way. Is that right?

Mr Wright: It is taught as part of ICT, but it is up to individual schools and it is not taught across the board.

Mr Gamble: It is not sufficiently well indoctrinated into the National Curriculum and it needs to be part of the personal, social and health education programme as integrated into everyday lessons about child safety. If it is dealt with as an isolated specialism, it will be delivered or not delivered and listened to or not listened to. We are working at the minute on a secondary programme which targets children between the ages of 11 and 12 and 15 and 16. Those are the ones that Ofcom say to us are most likely to have on-line access in their bedrooms or in private. That is this year, a school-year programme. The next one we are looking at, and we are working with all of the partners you would imagine here, is looking at how we engage primary education. Beverley Hughes visited the centre and we met with her officials and, as I said earlier, they are now actively seeking to employ a full-time member of the DfES to work within our education team so that we can further indoctrinate this in a sensible way.

Q235 Lord O'Neill of Clackmannan: You have the target of reaching a million schoolchildren. It has been suggested to us by the children's charities that this is rather ambitious, hugely ambitious in fact. Given the resources at your disposal, are you confident that you will be able to achieve this figure?

Mr Gamble: It is an ambitious target and we could never deliver it by and of ourselves. We are delivering it by cascading. We have trained 1,355 different teachers, school liaison officers, some librarians and some student teachers in other places and, just as an aside, I think student teachers are the people we need to be targeting most effectively in this area because they are tomorrow's generation of schoolteachers. Those 1,355 cascade that information out into schools, so a member of staff does not stand in every school, but those local police liaison or local safeguarding body personnel or others who have a relationship go out with the content which we have created and deliver it in the way we have trained them to, so do I think we will make it? Yes, I do. The way we are looking at it at the minute is that nearly 400,000 packs have been delivered to particular schools so far and we have until June, the end of the school year, and I believe yes, it is a big target, but our website is getting three million hits a month. We need to engage children in the right way and in fact if you could say it was banned, we would probably increase that to about 20 million hits a month.

Q236 Lord O'Neill of Clackmannan: The National Education Network have said that they do not really like the idea of devolving broadband funding to schools because they think this would diminish the good work which has been done on security and standards by the regional broadband consortia and local authorities. What is your view on this? Should Whitehall be intervening in setting standards so that this potential gap is bridged?

Mr Gamble: Well, we work with those consortia and I think that I have to give credit where credit is due and say they have done a great job in a number of areas and we have learnt a lot of lessons about that. I am not sure about the way forward in that regard at all. We need to speak to them, we need to engage with schools and it needs to be a collective discussion that makes sure that, by simply moving from one process with the broadband consortia to another, we do not undermine our ability to deliver a safer infrastructure because that is what might happen if it goes down to the individual school.

Mr Wright: I cannot answer that. It is DfES policy, as far as I am aware.

Q237 Chairman: We will have to cut it off there. Thank you very much for your answers. I think it is very interesting listening to you; it reinforces the view that, as you have said, technology is neutral and this is largely a social problem. It is almost ironic to me that the three-dimensional nature of a web means that we do not have fingerprints on images which probably made the old world easier, did it not?

Mr Gamble: But we actually do have fingerprints.

Q238 Chairman: But you really do not because you do not know where these images have come from in general and it is almost impossible to trace them back to the origin.

Mr Gamble: We can. Through the child-based technology we have, we are able to take 750,000 images, run them through our computer and it will tell us if we know these images or if we do not know them. It will also give us the history of the images that we know. What that does is prevent us from having to spend valuable time in looking at old images so that we are not duplicating effort, so we can fingerprint the image insofar as we can identify it and re-identify it and it is that fingerprinting technology in the IWF.

Q239 Chairman: That is not what I meant by ‘fingerprinting’. What I meant was that each image would not contain a fingerprint from the person who had sent it originally.

Mr Gamble: And where that does happen is in the more modern digital photography where we are able to get that information, but I accept entirely what you say. I wonder if I could just ask you to bear with me and let me make the four recommendations I wanted to make to you very quickly. The first one I would like to see this Committee ask is that child protection be a national policing priority in the National Policing Plan, and the fact that it is not is a significant problem and I do not know why it is not, but I think this Committee could perhaps

bring some focus to that. The second one is that internet safety be a requirement in the National Curriculum. The third one is that we have a requirement on local safeguarding boards to have designated posts with responsibility to co-ordinate internet safety across children's services. The fourth one is that you encourage the use of various types of blocking technology to meet the requirements of protecting children, whilst recognising the limitations of some of our industry partners.

Chairman: They are useful suggestions and it is valuable evidence you have given to us and thank you very much.

Memorandum submitted by the Children's Charities' Coalition on Internet Safety

Examination of Witness

Witness: **Mr John Carr**, Executive Secretary, Children's Charities' Coalition on Internet Safety (CHIS), examined.

Q240 Chairman: Mr Carr, thank you very much for coming to talk to us. You have been sitting there, so you have seen how we proceed. Would you like to introduce yourself, first of all.

Mr Carr: I represent the Children's Charities' Coalition on Internet Safety. That comprises all of the UK's largest child welfare charities and child welfare organisations, the NSPCC, Barnados, NCH, the Children's Society and so on. I am technically an employee or a consultant, I should say, to NCH and their contribution to maintaining the coalition is, as it were, to lend me as a resource to it, so I am an independent consultant, I work for the children's organisations, but also for other people as well, and I have been working particularly in this area of child protection on-line for just over ten years now.

Q241 Chairman: Is there anything you would like to say as an opening statement?

Mr Gamble: Beyond that, no. I endorse certainly the recommendations that I just heard the police make; I think they are sound and would be very useful, particularly the first one about getting child protection made a national policing priority and it is a mystery why it is not.

Q242 Chairman: Let me start by opening up questions for you and the first one is: who do you think is responsible for protecting children on-line?

Mr Carr: There is no silver bullet, there is no one agency or group which has this responsibility exclusively. I think the industry certainly has a key responsibility, and that covers a range of different players. The education system absolutely has a responsibility, as it

does to educate children about a whole range of civic and personal things within the context of education. Of course the Government and the public services have a responsibility in terms of promoting a healthy society to make their part, make their contribution to that process. Again, just to underline the point that was made before, parents, above all, have a responsibility and children themselves do as well.

Q243 Chairman: Do you have any thoughts about what we should do about this? You have identified a significant gap between what children are doing on the internet, blogs and instant messaging, et cetera, and the level of knowledge of parents, who in most cases have never even heard of these technologies.

Mr Carr: Yes, without a doubt, I regard one of the most important things that public policy needs to address is how we close that gap because parents are always going to be the first, and best, line of defence and support for their children. No-one knows or no-one ought to know a child better than their parents do and no-one is going to be in a better position to help a child deal with a whole range of things, but if the parent lacks the knowledge of certain fundamental things or things that their children are doing, it is very hard to see how they are going to be able to help their child to the best effect, so bridging that gap is a huge challenge for public policy. We, as NCH, were commissioned by the DfES two years ago now to run, and this addresses a question I heard you ask earlier, internet safety classes for parents working through individual schools and we in fact set these things up in 200 schools in different parts of England, in middle-class, rural areas, in inner-city areas and so on, and the response was very, very diverse. At some of the events we turned up to, one parent came along. At other schools, 250 parents came along. Schools are the logical or obvious way to try and reach out to parents, but the attendance of parents at these sorts of events seemed to depend largely upon how successful the PTA in that school was in attracting parents to a whole range of other things as well. It seemed to me that relying only or even principally on

schools as a means of reaching parents to help them bridge that gap was not going to work because you would be in effect devolving the responsibility to agencies that we already know are very patchy in terms of their effectiveness, so obviously it would be worthwhile continuing to try and make that work better, but we also need to find other ways of reaching parents as well.

Q244 Lord Harris of Haringey: In your evidence, you refer to two principal security threats, exposure to what you describe as ‘egregiously age-inappropriate content’ and then the exposure to predatory individuals. Can you give us some sort of indication of the risks, the relative frequency and the gravity of it?

Mr Carr: This may shock some of you, but I am in my 50s now, I know I do not look it, but I can remember with crystal clarity the first time I saw what you might generally call a ‘hard-core’ pornographic image. I was 19 years old and I was on holiday in Denmark. Now, that type of image, and I still have a vivid recollection of that particular image because I had never seen anything like it before in my life, that type of image is now kind of commonplace on the internet. I will give you numbers in a second, but it is seen not infrequently by children as young as six, seven, eight, nine and so on. There are a whole range of possible views that one might take about how bad the impact of those types of images might be on children. Some people think they are absolutely inconsequential and that they do not do any real damage at all. Others, and I would associate myself with this second category, think that this can be very scarring and very damaging and very shocking particularly for younger children to be exposed to. Just to turn to the numbers, the most authoritative source of data, by the way, in this field is, without doubt, the survey done by Professor Sonia Livingstone of the London School of Economics and I ought to make clear that I was a member of the advisory group that helped devise this survey and helped as an adviser generally with that project. What they found in the LSE survey, and this is all available on-line in a publication called *UK Children*

Go On-Line, was that 57 per cent of youngsters between the ages of nine and 19 who were regular users of the internet had come into contact with on-line pornography and 38 per cent of those had seen it as a result of pop-ups that had appeared on their screens, so again unsolicited, unsought, unlooked for, 36 per cent had found it accidentally and 25 per cent had seen these types of images as a result of opening up spam which they had received, unsolicited email. The scale and frequency is not, I think, really in dispute any more. One would hope that, as anti-spam technology improves, as the messages get through about the importance of not opening spam if you do not know the source and so on, these will reduce, but I still think that, however successful those sorts of initiatives are likely to be, the residual component of that type of activity is still going to be substantial. How scarring and how bad could the exposure to this type of material be for an individual child? It is very hard to say because these are subjective things and there are no objective criteria that you can refer to that are of any great assistance. For a particular child seeing a particular image in a given context, it may have very little effect, but at another time being exposed to those sorts of images, for a different child, a more sensitive child, a more sheltered child, it could be very, very damaging indeed, very scarring indeed. I am happy to develop on that if you want me to, but I will move on now to the question of contact and communications. Again if I refer to the LSE study, one third of regular users of the internet between the ages of nine and 19 said that they had received unwanted sexual messages and 31 per cent said that they had received “nasty comments” on-line or through their mobile phones. In this study, by the way, which was done face to face where they interviewed the parents of the children afterwards and separately, only seven per cent of the parents were aware that these types of things were happening to their children. A significant proportion, in the LSE study again, around about eight per cent of children who had met people for the first time on-line went off to meet them in real life. Now, that is obviously potentially the most risky thing that can happen, a child

meeting somebody in a chatroom or in a virtual environment and being invited to go and meet them in real life and then actually going off to do that. There was one case which was documented by the University of Central Lancashire where I think a nine-year-old boy, who lived in Preston, went off to meet somebody whom he had met on-line and got on the bus and went to Blackburn to meet the person. As it happens, it turned out they were both great football fans of Manchester United, so nothing bad came of it, but it does illustrate the possibilities that can arise from this.

Q245 Lord Mitchell: You have advocated the compulsory reinstallation of filtering systems on computers, and the police have called them ‘nanny programs’, to be set at a high level of security. Do you have any measure of the effectiveness of such filtering systems?

Mr Carr: The short answer is no, but we will do soon. The Home Office speaker previously referred to the fact that there is a government working party, of which I am actually the Chairman, by the way, which is looking into developing a kite-mark, working with the British Standards Institute to give a quality assurance mark for filtering products.

Q246 Lord Mitchell: Do they work?

Mr Carr: Yes, they work. The question which we have not yet finally resolved is what numerically will be an acceptable level of false positives essentially, which is what it will come down to. We would hope that the filtering software will work at the same type of level of efficiency as anti-spam and anti-fishing programs already do. Whatever filtering program that you might imagine will be used in this environment is never going to be 100 per cent perfect; it will over-block or it will under-block. The question is: what is an acceptable level?

Q247 Lord Mitchell: If I wanted to turn on anti-spam on my computer, I would be doing it because I wanted to do it. If a parent turns it on, the parent knowing probably a lot less than

the child as to how the computer works, the child can then turn that off quite easily presumably.

Mr Carr: Only if the parent has done it badly. Sadly, it is worse than that because typically what will happen is that the parent will say to the child, “Here’s the blocking software. Would you mind installing it, please”, so the child will invent the password or, alternatively, the parent will tell the child the password. This gets to one of the issues and one of the problems with the blocking software, that the software has to be very good, otherwise parents will simply turn it off. If a parent is being called up to the child’s bedroom or study every five minutes because a site is being blocked and the child cannot read it and the parent needs to make a decision about whether to override it or not, they are going to get fed up of that pretty quickly and they are going to stop using it, so the software has to work at a very high level of efficiency and be very smart. Some of the software products which came out in the early days were very poor and that is why the take-up of them, in part at any rate, has not been as good as it might be. What we hope is that, if we develop a BSI standard which will be on the boxes in the shops or on the websites when parents go to it, when parents see that BSI kite-mark on the products, this will give them some level of confidence in the quality of the software and it will encourage them to download and use it. I might just say, you asked a question earlier about what the response from the industry has been, and obviously the manufacturers of this software are very keen on this initiative because they imagine it will mean that their products will sell more, but the really difficult bit of the equation is getting the computer manufacturers to agree to the pre-installation because it is at the factory where these settings are first put on the machine. One manufacturer has already done it and that was Comet. Now, Comet are a major electrical retailer, they are not major computer manufacturers, but they do have their own brand, they are a manufacturer of computers and they did do it on their own-brand machines. That demonstrates (a) that it is possible, but only

if (b) you want to do it. The cost of doing it is negligible. I went to the factory to see the whole process being done and the manager of the factory that I visited said quite frankly that it is impossible to compute the cost of that extra step in the manufacturing process because, in essence, all they do is make the settings once, they put them on the goldmaster disk and that goldmaster disk is then copied along with everything else, the operating system, the office software and what-have-you, on to the hard drive, so in terms of additional cost in the manufacturing process, it is nearly nil.

Q248 Baroness Sharp of Guildford: In your evidence, you express support for the UK's self-regulatory approach, but are there areas where you think regulation might be more appropriate?

Mr Carr: No, but a qualified no. Self-regulation is always going to be a better approach because it is more flexible and quicker. Leaving aside acknowledged national emergencies and so on, if you look at the typical gestation period for an idea coming into the public policy arena and ending up as a law, it will typically be four or five years or something like that. If you have a self-regulatory environment, it is possible to move a lot more quickly and of course self-regulation, by definition, means that you have got the co-operation of industry and, if you have got the co-operation of industry, then you have got access to their expertise and they are going to be much more enthusiastic about getting on and doing it. Self-regulation has worked very well in the UK up to now, but I have to say, and I do not want to be disingenuous about this, I think one of the reasons it works so well is because the industry believe that, if self-regulation is not seen to work, the Government will step in and legislate, and that is what they want to avoid and for very well-known reasons that we need not rehearse. It is very much in the industry's interest, I believe, to continue to make the self-regulatory environment work.

Q249 Earl of Erroll: How does the risk of going on-line actually compare to the general risk in society?

Mr Carr: Of living, you mean?

Q250 Earl of Erroll: Yes. There is a risk out there anyway of children being kidnapped and abused, et cetera, but is that risk greater on-line?

Mr Carr: Well, I do not mean to be facetious, but more people get killed falling down stairs every year than do, I think, crossing the road or something of that kind, but do we all live in bungalows? No, we do not. If you are a parent and you are aware of an avoidable risk to your child, you will want to avoid that risk if you reasonably can, so in that sense, whether the risk is one in ten billion or one in 10,000 or one in 100, it is irrelevant from your point of view as a parent. What you want to know is: is my child at risk, what is the risk and how do I avoid it? With the internet, what we are talking about are a number of risks which are, to a greater or lesser degree, avoidable and that is why the search is for solutions which help minimise, or eliminate, these risks.

Q251 Earl of Erroll: I suppose I was thinking of how does the frequency of abuse as a result of someone they have met on-line compare to the abuse which comes from friends, family and neighbours, which we actually know is significant as well? Do we have any figures on this?

Mr Carr: There is no comparison between the two. The level of abuse in real life far, far outweighs and outnumbers the number of cases of on-line abuse of children, as far as we are aware, if I can put it that way. Let me, however, issue one caveat. First of all, the way the crime figures are collected does not help us with an objective determination or in providing an objective answer to your question. I think I am right in saying that even today in the crime statistics it is not recorded whether or not a computer was a key part of the way in which the

crime was committed. For example, if a child is sexually abused as a result of an on-line contact, it will not show up as an on-line offence, it will simply show up as a contact offence. We do have some numbers which we can point to relating to child pornography offences and I have published them in a document which came out two years ago. If you look at the incidence of child pornography offences, the line is absolutely straight up and correlates almost entirely with the growth of the internet. That is not to say that the internet is the cause of child pornography, it has been around for centuries, but what is undoubtedly true is that the internet has provided a readier means of people with a latent, or already acknowledged, interest in child pornography to act upon it and gain access to it, and the numbers are very striking and there is no doubt that the internet has played a part in facilitating that growth.

Q252 Baroness Hilton of Eggardon: Several responses have mentioned bullying as an on-line issue. Have you any idea about what the incidence is?

Mr Carr: We do. At NCH, we carried out a survey which was in 2005 and those are the figures I have here, but we did a kind of check last year as well and they were broadly the same. Bearing in mind that the ownership of mobile phones is almost universal amongst the teenage group from about 11 or 12 upwards, what we found was that 20 per cent of all children have experienced some sort of digital bullying, 14 per cent by mobile phone text messaging, five per cent in internet chatrooms and four per cent by email, so one in five basically of all children, because they are all on-line and they have all got mobile phones, is being bullied in one way or another through the on-line environment.

Q253 Baroness Hilton of Eggardon: Bullying is normally by someone that you know or by a group of people that you know, so it is probably more likely to be on mobile phones perhaps where you know who the perpetrators are.

Mr Carr: And the numbers do suggest that.

Q254 Baroness Hilton of Eggardon: It is not normally a matter that the police can deal with.

Mr Carr: There are potentially three different crimes involved in bullying. One is an offence under the Malicious Communications Act, one is an offence under the anti-stalking laws and one is an offence under the Telecommunications Act, but you are right, that these matters are not traditionally police matters. Perhaps I could just say a word about on-line bullying. When I was a lad in Leeds, there was bullying going on in our school and I can remember being the victim of it myself on one occasion, but pre-internet, pre-mobile phones a kid knew that, when they got home and they closed the street door behind them or they went up to their room and closed their bedroom door, the bullying stopped and they had found a sanctuary. That is no longer true. The whole point of having a mobile phone is that it is on so that your parents or your mates, whatever, can get you as and when they need to. The whole point of having a computer and the internet is so that you can use it to do your homework or whatever, but it also means of course that the bullies can get at you 24/7 too, so in some ways it is a very insidious, intrusive development in the way bullying works.

Q255 Lord Howie of Troon: I am told that there are a number of social networking sites and two names have been suggested to me, with which I am unfamiliar, I have to say, Bebo and MySpace. First of all, what is your general view of these sites and, secondly, do the sites do enough themselves to protect children?

Mr Carr: I should declare an interest here. I made it clear at the beginning that I work not just for children's organisations, but for companies as well and I am an adviser to MySpace, so I have some inside knowledge, as it were, of that particular company.

Q256 Lord Howie of Troon: Open up then.

Mr Carr: The phenomenon of social networking sites is huge. In the on-line stats which were published last month, I think, MySpace finally overtook Yahoo as the most visited in the United States. MySpace has six million subscribers here in the UK and Bebo has also a very substantial number of members too. The social networking sites in general are not an entirely new phenomenon. What they have done in a very clever way, which is why they have become so popular so quickly, is brought together a number of different technologies that previously people used discreetly or individually, so you have now got in one place, in a very convenient way, access to video, access to messaging-type services, access to pictures and photographs and they have all been brought together into this single place, so they are very, very attractive and that is why they have been hugely popular with youngsters. All of the social networking sites are very keen to ensure that their users are aware of some of the risks. We heard Jim Gamble earlier speaking about the image of a child walking between Oxford Circus and Tottenham Court Road with a billboard giving all of their personal information to any potential passer-by. That is the kind of thing that could happen on a social networking site and it is why each of the companies that I am aware of anyway is putting a great deal of energy, effort and resources into getting the messages across.

Q257 Lord O'Neill of Clackmannan: You have raised the question of Solo cards being issued to very young children in the absence of visual checks, which means that they can enter into transactions and the like. What do you think needs to be done? Do you think the banks need to stop issuing them? What would be your answer to this problem?

Mr Carr: I certainly do not think the banks will stop issuing them, and I am an agnostic as to whether they should or not. My own children both got them when they were 11 because we opened up bank accounts for them with NatWest and they were part of the package that they got. What we need is a reliable means of age verification. Children tell lies about their age and they have done since time immemorial. Traders should not take it for granted that people

make truthful statements where the product that they are selling is an age-sensitive or an age-restricted one.

Q258 Lord O'Neill of Clackmannan: So how can service providers do this?

Mr Carr: Well, as you know, the Gambling Bill, which went through last year, has increased the penalties on gambling companies and I think we are going to see similar things happening in other areas of policy as well. It is technically possible to do it, but they need to be made to do it.

Q259 Lord O'Neill of Clackmannan: I had a son who was once two years older than his older brother!

Mr Carr: There you go!

Q260 Chairman: Mr Carr, thank you very much indeed. If there are any other thoughts you might have for us, please submit them in writing for us.

Mr Carr: Will do. Thank you.