



Child safety online

A digital manifesto

Children's Charities' Coalition for Internet Safety

Contents

- Why a manifesto? 1**
- The origins of the task force 2**
- The task force’s achievements 2**
- Strategic questions**
 - political leadership and management 5
 - the limits of self-regulation 5
 - capacity building 6
 - the internet has changed 6
 - giving consent in the digital age 8
 - sentencing guidelines 8
 - filtering solutions 9
 - pre-installation is the best route 9
 - new technical solutions needed for new problems 9
 - incentives to industry 9
 - the international dimension 10
 - cracking down on cyber havens 10
 - location-based services on mobile phones 10
- Challenges to policing and to the child welfare system 10**
- Legal reforms 12**
- Summary of recommendations 14**
- Appendix Agenda for Action, March 2001* 16**

Why a manifesto?

It is still not quite ten years since the internet began its dramatic transformation from obscure technology to mass consumer product.

The Children's Charities' Coalition for Internet Safety (CHIS) wants all children and young people to be able to share in the huge advantages of the internet, and therefore strongly supports the government's continuing efforts to encourage mass take up. But at the same time CHIS also wants to ensure that such access is as safe as it can be. Almost nothing in life is ever 100 per cent safe, 100 per cent of the time, and the internet is no exception to that rule. But the internet can, and should, be a lot safer than it is at present, particularly for children and young people.

The creation of the Home Secretary's Internet Task Force on Child Protection in March 2001 was a pivotal moment in the development of internet policy in the UK. Several members of CHIS are directly represented on the task force. The task force was a world first and the British government has now become an acknowledged leader in the on-going, increasingly global, efforts to make the internet a safer place for children and young people.

With a general election fast approaching, and with several years' experience of the task force under our collective belts, CHIS thought it would be timely both to reflect on the many important, positive achievements of the task force, and some of its difficulties, and then to put forward our suggestions about how internet policy in this area might be further developed.

Many of the proposals made in the manifesto have already been or are being put to government, both through the mechanisms of the task force and more directly, but it seems clear to us that there is also a need for wider public debate, particularly around some of the broader policy issues that we raise.

The manifesto contains a mixture of both highly strategic and more detailed points. It updates and becomes, in effect, version two of the *Agenda for Action* that CHIS first published in early 2001 and which is reproduced as an appendix to this document. Gratifyingly, many of the points from the *Agenda* have been taken up, but a number

remain unfulfilled although still highly relevant. They are therefore repeated here.

The task force has enjoyed very broad political support, with both the Liberal Democrats and the Conservatives directly represented on the task force by MPs. CHIS very much hopes that this kind of consensus will be maintained. CHIS further hopes that the publication of this manifesto gives all the political parties the opportunity to think about where the UK goes next with this important area of public policy, and encourages them to lend their weight to help get there.

In the second quarter of 1999 only nine per cent of the UK population, 2.2 million people, could access the internet from home. www.statistics.gov.uk

In the period 2000–04 internet usage in the UK increased by 126.5 per cent. Today 35 million UK residents now access the internet. That is roughly 58 per cent of the total population.

In the same period the total number of internet users worldwide increased by 121.6 per cent, to over 800 million, or about 12.5 per cent of the total population of the world. www.internetworldstats.com

In August 2003, OFTEL found that 50 per cent of all families in the UK had internet access at home, but in 2002, Becta had found that 68 per cent of all families with children aged 5–18 had internet access at home. Families with children are much more likely to have internet access at home.

The origins of the task force

In March 2001, the British government announced the formation of the Home Secretary's Internet Task Force on Child Protection. Its declared intention was, and remains, to make the UK the best and safest place in the world for children to use the internet. Such an initiative had been urged upon the government by CHIS and others, and when it was announced it received a very warm welcome across a broad spectrum of opinion.

The task force was established in the aftermath of extensive media coverage of several horrific cases of child sex abuse, where the internet had played a key part in facilitating the crime. There had also been several major police actions against child pornography rings that revealed both a wholly new scale of this type of offending, and underlined its now global nature. In addition, concerns were increasingly being expressed by parents, teachers and others about the unprecedented and unrelenting way the internet was exposing children to a range of websites that displayed certain kinds of sexual imagery or published materials about, for example, suicide, drugs, bomb-making and so on. While almost certainly legal, these were very far from being age-appropriate and indeed could be harmful to very young or vulnerable children.

The task force's achievements

Unique platform

One of the major successes of the task force was simply to bring together, for the first time ever, all the key stakeholders. There is little doubt that, within the UK, this has completely transformed the climate within which much of the debate takes place about how we are to achieve our commonly agreed goal of making the internet a safer place for children and young people.

Several of the UK's leading internet service providers (ISPs) and the major web portals are directly represented on the main task force, as

is ISPA, the principal trade association for ISPs. Sitting alongside them, either on the main task force itself or on one or other of its several working groups, are also representatives from software houses, mobile phone companies, credit card companies and, more recently, search engine companies. All of these private sector players have been working extensively and co-operatively with the police and other parts of law enforcement, with a number of the children's charities, and with different arms of central government. Representation from computer manufacturers and retailers has been there, but not as strongly as many would have liked. This underlines the importance of keeping the membership of the task force actively under review.

The task force has therefore created a unique platform. It facilitates the development of positive, proactive, broadly based plans to take the internet safety agenda forward but also, as the occasion demands, it allows for problems and issues to be identified at a much earlier stage. This in turn has helped key players to establish shared understandings, and encouraged the emergence of a common approach to risk assessment and to finding solutions. The task force has consequently fostered a range of partnerships, both within and outside the framework of the task force, which otherwise might never have happened or would ordinarily have taken a great deal longer to build.

Chatrooms and public awareness

The Home Office financed a substantial piece of research into the use of chatrooms by children and young people. Off the back of that the task force organised a major conference on chatroom moderation.

The Home Office has funded four major public awareness campaigns about chatroom dangers, at a total cost of £3.3 million. In September 2004, figures produced by the Home Office showed that 89 per cent of young people were now aware they should not give out personal information in chatrooms and 94 per cent realised that people they met online may not always be who they say they are.

Internet awareness training

NCH and NSPCC have jointly been commissioned to prepare internet awareness training materials for the probation and prison services, as well as those parts of social services that work with abused children and young people.

Criminal Records Bureau checks

New rules have been created to allow chatroom moderators to be made the subject of Criminal Records Bureau (CRB) checks.

75 per cent of all 9–19 year olds have accessed the internet from a computer at home.

19 per cent of 9–19 year olds have internet access in their bedrooms.

In homes with internet access, 46 per cent of parents claim that filtering software has been installed, yet only 15 per cent of parents said they knew how to install a filter. Only 35 per cent of children said that a filter had been installed.

Professor Sonia Livingstone, LSE, UK
Children Go Online, July 2004

Sex Offences Act 2003

Several key reforms were made in the Sex Offences Act 2003, including the introduction of the offence of sexual grooming, among other things, to help deal with the improper use of chatrooms. The Act also made 18 the legal minimum age to participate in pornographic depictions to be published in any forum.

Good practice guide

The task force has published a good practice guide for ISPs and anyone else providing online services via the web. The guide covers a wide range of website management issues. The impact of the good practice guide is currently being evaluated.

The work involved in developing the good practice guide was substantial and time-consuming, bringing together parties whose

interests, at least initially, appeared to be a long way apart. The development of the guide therefore played an important part in building relationships and mutual confidence within the task force.

Filtering software

An advisory note has been published setting out what filtering and safety software can do to help parents and others protect children when they go online.

Mobile phones

The task force played a key part in facilitating discussions with the mobile phone industry around a range of safety issues. The mobile industry has now adopted a code of practice on content and new services that was very broadly endorsed and welcomed, including by CHIS.

The new code of practice on content and new services includes plans to develop an age verification system that will be used to determine the type of content and services that might be supplied to a specific handset.

The code also requires all publishers of content on the mobile phone companies' own networks to classify it as either universal or adult. A new, independent body is being created to be responsible for overseeing the new classification system.

The mobile phone companies are also installing filtering software on their servers so that parents can exercise some control over what their children might access, should they choose to go outside the phone company's network and, for example, use their mobiles to go on the internet. Some of the mobile phone companies have indicated that this safety software will be the default option. Interestingly, this means that some of the mobile phone companies have, from a child safety point of view, leapfrogged over their colleagues in the fixed internet world, the great majority of whom do not provide safety software as a default option.

Detailed discussions also took place between the mobile industry and the children's organizations, the Home Office and the police about a code of practice on passive location services, ie a new type of service that works through mobile phones to allow parents to track

the physical whereabouts of their children. This code of practice is now agreed and is being phased in by 1 January 2005.

Law enforcement

Several other initiatives have spun off the task force, particularly within the police where, for example, the Association of Chief Police Officers (ACPO) has now established a national committee on combating child abuse on the internet (CCAI), to co-ordinate strategy across all the local forces in England, Wales and Northern Ireland. The Scottish Police take part in this committee as observers.

The Police On Line Investigation Team (POLIT) was formed in early 2003 and based within the National Crime Squad. An extensive training initiative for police personnel has been developed at the National Specialist Law Enforcement Centre, and a revolutionary digital database of child abuse images has been created that promises to act as a major aid to police investigations of child pornography offences. Above all, it will assist police efforts to identify victims depicted in the images. This database, known as 'ChildBase', is also at the centre of a major attempt by police across the world, through Interpol, to improve co-ordination and intelligence sharing. The emergence of the Virtual Global Task Force, initially bringing together police forces in the UK, USA, Canada and Australia, is also a very exciting development that is being closely watched.

'In 1995 the police in Greater Manchester seized the grand total of 12 indecent images of children. All of them were on paper or on video. In 1999 we seized 41,000, all bar three of which had come from the internet. Today we don't bother counting. There's no point.'

DI Terry Jones, Greater Manchester Police

In 2003 one North American man was arrested with 1,000,000 images in his possession. A man from Lincolnshire in the UK was arrested with 490,000 images in his possession.

A Memorandum of Understanding has been developed jointly by the police, the DPP and industry to advise on how systems administrators and the Internet Watch Foundation (IWF) might handle illegal images in the course of investigations.

The education system

In the educational world a substantial investment, in excess of £1 billion, was made in bringing internet access into schools and training teachers in how to utilise the internet to enrich the curriculum. Considerable attention has also been given to the safety agenda within schools. Via the British Educational Communications Technology Agency (Becta), the DfES has its own structures in place for dealing with internet safety issues but the safety measures taken within schools broadly mirror those being advanced by the task force in relation to the wider or home internet environment. DfES and Becta officials are part of the task force's machinery, and vice versa.

Using credit cards and other payments systems for illegal purposes

Following representations from CHIS and police advice, the UK payments industry has agreed to seek new legal powers to penalise anyone who is found to have used their credit cards or other facilities to pay for any kind of illegal online transaction. The UK government has also indicated that it is willing to give the payments industry these new powers and the Information Commissioner supports the change.

A new awareness

It is also right to say that, directly or indirectly, the task force has prompted a range of other organisations to think harder and deeper about this whole area. This is particularly true of the ISPs and portals, but the wider media, children's organizations, commercial companies, the judiciary and others have also responded in many different ways to the new climate the task force has helped to create.

Related developments

For the sake of completeness it also ought to be recorded here that, prior to the formal

establishment of the task force, important provisions that touch on the issue of online child safety were also made in the Regulation of Investigatory Powers Act 2000, concerning encryption and other matters. The National Hi-Tech Crime Unit was created in November 2000. Sentences for child pornography-related offences were substantially increased in the Criminal Justice and Court Services Act 2000, and following a report from the Sentencing Advisory Panel in November 2002, the Court of Appeal promulgated new guidelines for judges who were called upon to sentence offenders in child pornography cases. The civil servants who work with the task force also help maintain important links to the G8 on these issues, and to the EU.

The task force's current agenda

There are still several large and important items on the task force's agenda, most of which follow on from some of the earlier successes and achievements listed above. The issues currently being actively pursued are set out below, but it is important to realise that they are each at different stages of development:

- producing a good practice guide on chat and moderated interactive services
- producing an advice note on spam
- with support from OFCOM, working with the British Standards Institute to develop a kite-mark for internet filtering and safety software
- working with the search engine companies to reduce the scope for accessing illegal or inappropriate materials or sites
- co-ordinating safety messages and promoting common safety and awareness messages (also linking in to a large EU-sponsored initiative)
- developing a training initiative for probation, prison and social service personnel
- examining further law reforms

Strategic questions

Political leadership and management

The task force has no budget of its own. It never has had. To obtain resources for its work it has had to rely, on an ad hoc basis, on funds being

available elsewhere that can be switched across. Generally such funds are only available if there has been an under-spend within another budget. On occasions this has meant that resources only come on-stream very late in the spending cycle, sometimes giving officials very little time to consult about the spending plans themselves, or alternatively initiatives have to be delayed until a new financial year arrives. With the current spending review now complete, the task force will not ordinarily be in a position to bid for a budget for another two to three years.

The task force does not have a dedicated secretariat. It never has had. The task force has been lucky to be able to work with some very talented and committed civil servants from the Home Office, but every one of them also has a range of other responsibilities that have nothing whatsoever to do with the task force. It has sometimes been all too apparent that these other duties have taken precedence.

Despite repeated statements that the task force is meant to be spearheading a government-wide policy, with the limited exception of parts of the DfES, there is almost no evidence of this working in practice. The task force has become, in effect, almost entirely a Home Office project.

The absence of a dedicated secretariat and a dedicated budget for the task force are a deadly and deadening combination that greatly exacerbate the problems and difficulties of working inter-departmentally.

As will be clear from many remarks elsewhere, CHIS believes the task force has developed a number of very positive initiatives, but so much more could be achieved, and more speedily, if other government departments were equally engaged and if, across government, there really was a shared approach and a shared understanding of the issues.

The limits of self-regulation

Debates in the public domain about internet regulation were first prompted by the increasing amounts of child pornography that the police started to uncover in a spate of arrests that began in the early to mid-1990s. These arrests were some of the first, outward signs that a new technological era was approaching.

At that time there were very few civil servants or ministers who had any real grasp of what the internet was, about its technical underpinnings, or about how to tackle the unforeseen and unintended consequences of its roll-out into wider society. The number of police personnel who knew about the internet was also very small.

Self-regulation was very much in vogue across central government as a whole and the creation of the IWF in 1996 gave concrete expression to this idea in the internet space. However, looked at in the cold light of day, opting for self-regulation in relation to the internet seems to have been not so much a conscious or deliberate policy choice as possibly the only one available. Perhaps there was also a worry at a political level that any precipitate action taken to regulate or control the new technology might choke off some of its perceived economic potential and put the UK at a disadvantage vis-à-vis our competitors.

That said, the global character of the internet, and the speed at which aspects of the technology can change, does pose special problems for the legislative and political machine in a democracy. No sooner has a technologically-based problem been identified and a response formulated than it has moved on or changed. No one wants to legislate in haste and repent at leisure.

In this area government definitely does need, and generally can only benefit from, the active collaboration and involvement of the internet industry. However, it is very easy for a reliance on the self-regulatory model to drift into a simple failure to have any kind of strategy at all. Policy is therefore reduced to piecemeal fire-fighting and ad hoc departmentally-focused initiatives, often very much led by the media agenda.

Moreover it is also very much the case that while parts of the industry are always willing to respond to voluntary codes and to show leadership, many deeply resent the fact that some of their competitors never seem to respond, or respond slowly. And these unresponsive elements believe they have nothing to worry about because the government is disinclined to legislate, for the reasons given. They can sit it out and ignore the occasional adverse comment.

Equally, there is something fundamentally unhealthy in a democracy for the government to

One third of 9–19 year olds who go online at least once per week report having received unwanted sexual (31%) or nasty comments (33%), via email, chat, IM or text message.

Only seven per cent of parents think their child has received sexual comments, and only four per cent think their child has been bullied online.

Professor Sonia Livingstone, LSE, *UK Children Go Online*, July 2004

be so heavily reliant on technical advice that is provided by the very industry they are meant to be overseeing on behalf of the wider public interest. No doubt similar concerns or issues arise in other areas of public policy or public activity where, to some degree or another, real limits are set by technical factors that, unsurprisingly, are not always widely understood. However there can be few such areas that are quite as immediate or pervasive as the internet and this, it is suggested, puts the matter into sharper focus.

What this points to is the need for the UK government and civil society to be able to develop and sustain their own sources of knowledge and expertise, separate and distinct from the industry itself, so that the debate in future can be conducted on more equal terms. This ties in neatly with a separate but related point.

Capacity building

Insufficient attention has been paid to the importance of developing the NGOs' ability to take part in the processes associated with the task force, and in particular the work of its many sub groups. There can be little doubt that a number of the private sector concerns that attend and take part in the task force's work do so, at least in part, because they believe they are furthering or defending their commercial interests.

The children's charities, on the other hand, are very hard-pressed and are simply unable to divert any more resources away from providing support directly to needy children and their families in order, in effect, to provide a free consultancy

service to big technology companies and the government. The charities are doing the best they can within their limited resource constraints but they are acutely conscious of how much more they could do if the resources were available. For example, within the mobile phone industry there are a range of conferences, seminars, working parties and bodies that operate on a global level that CHIS has been invited to participate in. They are addressing the issue of children's safe use of mobile technology as well as new designs for new products, but for practical purposes it is simply beyond our means to take part. Similar examples have occurred elsewhere. Yet, potentially, huge benefits are available to the industry and society if, at an early stage in the process, issues of child safety are addressed and built-in.

Straight away there is a dilemma. Many of the traditional sources of charitable funds are not familiar with technology issues and so obtaining new resources from them for work in this area can be very difficult. The most obvious source of financial aid is the industry itself but going that route can severely compromise someone's ability to speak as freely or as frankly as the situation might sometimes require. Many people, understandably, find it very hard to criticise someone who has just given them a large sum of money, and whose continued support they might come to rely on.

Sections of the industry, of course, shrink in horror from the notion that anyone but themselves should be involved in discussing technology policy.

The conventional mantra in these matters is *Let the market decide* but when key parts of the market are essentially driven by a mixture of very large producers and huge marketing budgets, it can take a very long time for public policy to catch up and, in the meantime, children may be placed in situations where their personal safety is at risk. In one sense the task force itself is only necessary precisely because the technology companies that have been responsible for the roll-out of the internet and related technologies as mass consumer products did not anticipate and deal with the hazards to children and young people that have since become apparent.

The international dimension to this area of policy has already been referred to several times.

CHIS is beginning to develop its links with NGOs overseas, both inside and outside the EU. Developing the international side is extremely important but, once again, it is very demanding in terms of resources. We need to find new and better ways to strengthen civil society's capacity to intervene in these vital debates.

The internet has changed

One way of thinking about the recent history of the internet is as a process of bringing it in from the wilder libertarian shores of its origins to the mainstream of high street consumerism. Whatever view you take of the desirability of these developments it is plainly no longer appropriate to think about the internet as a predominantly adult medium, where special measures are needed to make allowances for children's occasional or intermittent use. It is now clear that children and young people are major and constant users of the internet. If anything, they are disproportionately or over represented among internet users. Therefore we should seek to establish in domestic UK law that much of the internet is akin to a public space, not a private space. Website home pages should therefore be thought of in the same way as we think about shop windows.

In that connection a new duty should be placed on all web publishers: a sort of cyber equivalent to the Indecent Displays Act 1981. In other words, in this respect there is no need to change the existing laws relating to, for example, obscene publications; it is merely being suggested that if web publishers wish to display certain kinds of images they must take all reasonable steps to ensure that only people who are adults, and only people who positively want to see such images, can do so.

This would mean, for example, on every website where such material was to be displayed, the first page viewed by any visitor, the home page, should state clearly what kind of material lies within.

Ideally one would like to see something that went further and required proof that the person wishing to look at the material was an adult, that they understood what it was they are about to be presented with, and established that they positively want to be presented with it. The

proposition being advanced here is almost identical to the reason for the decision in *R v Perrin* in the Court of Appeal in 2002, but it needs to be further publicised and pursued. The Crown Prosecution Service, the police and the IWF ought to be drawn into more detailed discussions on this point.

It would, of course, be very difficult to enforce such a law in relation to overseas websites, but if the UK were to take up such a position vis-à-vis its own web publishers it might encourage other governments and legislatures to follow suit. The UK would be taking a leadership position that it could then promote within appropriate international arenas.

Alternatively, or in addition, we should investigate the utility of the (relatively new) German law that, in this case, puts pressure on their domestic publishers of legal adult pornography to classify their material in a way that means it can be picked up by filtering software and then be screened out by, for example, parents who do not want it to be available to their children. Following the introduction of the new German law, a publisher of legal, adult pornography who does not classify their images is at greater risk of legal sanction should there later be a complaint.

Giving consent in the digital age

The data protection laws are in need of a major overhaul to take account of the new realities of cyberspace.

For all legal minors between the ages of 12 and 17, all vendors, companies or organisations seeking information from children, or seeking to sell goods and services to children, are meant to satisfy themselves, subjectively, child by child, that the young person understands the nature of the transaction being put to them. To this extent the law broadly mirrors the Gillick principle. However, the crucial difference is that in relation to medical matters or sexual health issues, the usual Gillick terrain, a highly trained professional person almost invariably meets the child face-to-face, perhaps many times, and is therefore clearly in a good position to make an informed judgement about the child's capacity to understand.

CHIS knows of no company currently trading online that even gets close to the position we have described. If they think of it at all, they simply ask for tick boxes to be filled in, or emptied. Moreover it is very hard to imagine how any kind of subjective test could be administered in a remote environment. Neither do the relevant industry bodies offer any advice or guidance as to how, within an online environment, their members ought to discharge their obligations in these respects.

One of the consequences of this absence of any easily available widespread means of verifying a child's age became apparent in research recently carried out by NCH and other partners. Using a Solo card that she had had since she was 11, a 16-year-old girl was able to register to gamble on 30 out of 37 UK-based gaming websites that were tested. Gambling in the UK is restricted to persons aged 18 or above. There are many other age-restricted goods and services that are also widely available online. Perhaps the banks and payments industries should be asked to investigate the possibility of encoding any cards they issue to under-18s so they would indicate to any computer system used by a vendor that the person who owns the card being offered is not a legal adult.

Alternatively, or in addition, CHIS would be keen to ensure that any new technically-based national identity card schemes, or similar schemes, that might emerge in the coming years could be used to enhance child safety in an online environment.

In relation to children aged 11 and below companies are not even meant to ask the child anything at all without first obtaining parental consent. This provision also is honoured more in the breach rather than in the observance. Neither is there any clear research-based evidence to show why, in this context, 11 is of any particular importance or significance. It seems more like a commonsense throwback to the days when children would cut up a cereal box in order to send for a free toy.

Sentencing guidelines

CHIS is concerned that the sentencing guidelines adopted by the Court of Appeal in *R v Oliver* in November 2002 are being used for purposes for

Between 1988 and 2001 the total number of people cautioned or proceeded against for possessing or making child pornography was 3,022. In 1988 the annual total was 35. In 2001 it was 549, an increase of 1,500 per cent over the period.

Offending and Criminal Justice Group (RDS), Home Office (Ref IOS 503-03)

In the summer of 2002 the Americans handed the British police a list containing the names of 7,200 UK residents who, using credit cards, appeared to have bought child pornography through a single website based in Texas. So began Operation Ore.

which they were never intended. No link has ever been established between the level or type of images a person might possess and the likelihood of them being a continuing danger to children. Yet there is much anecdotal evidence to suggest that the police, probation and prison services, and the courts, are operating a crude rule of thumb. Someone convicted of possessing Level 1 or Level 2 images is assumed to be a low ongoing risk to children, whereas someone convicted of possessing Level 4 or Level 5 images is automatically assumed to be a high risk. The position could, in fact, be completely reversed. A reliable form of risk assessment urgently needs to be developed for possession cases.

Filtering solutions

CHIS deeply regrets the fact that there is still no efficient public domain solution that is widely and easily available to parents, and others, that could enable them to screen out unwanted material from the internet, and shield children from unwanted online contacts. Such a solution has been promised by major players in the global internet industry since at least 1999 but it has yet to materialise. One is bound to wonder if it ever will.

This collective failure by the industry, paradoxically, comes at a time when individual companies are, commercially, producing individual internet safety and filtering software products of ever-increasing sophistication.

OFCOM has a particular responsibility in this area, as it relates closely to their work on media literacy. We look forward to them developing a robust approach.

Pre-installation is the best route

As all the mobile phone companies have already recognised, technically-based solutions could play a very valuable role in protecting children, perhaps especially younger children, in the online environment. Therefore CHIS intends to step up its campaign to persuade all computer manufacturers and retailers active in the domestic market to pre-install filtering and safety software on all new PCs.

Such software should, by default, be set to a high level of safety but it could, of course, be uninstalled or disregarded if that is what the owner wanted. However, if at least it was there and working from the first moment the machine was turned on, it would provide some valuable, if minimal, support to parents.

The cost of the software and the installation should be factored into the price of the basic product at the point of sale. Child safety should not be an optional extra.

New technical solutions needed for new problems

CHIS is also keen to persuade the industry to come up with improved technical solutions across a range of other issues in both the mobile and fixed internet world, such as for dealing with the abuse of encryption and peer2peer technologies, including Freenet, or the abuse of cameras within mobile phones, and the abuse of anonymity. CHIS also wishes to encourage all ISPs and mobile phone companies to follow the excellent lead provided by BT in their Cleanfeed initiative. Cleanfeed blocks access to websites that have previously been identified by the IWF as containing illegal child abuse images. So far only Vodafone has indicated publicly that they intend to adopt a similar approach.

Incentives to industry

CHIS wishes to explore with government whether or not the tax regime could be used to provide incentives to different industry players to enhance child safety online, either through the

development of new products or through pre-installing them, or both.

The international dimension

We need to find better ways to bolster and speed up the G8 processes and provide greater support to other international bodies that are trying to advance the child safety agenda. Particular regard should be paid to the processes established under the UN's Working Group on Internet Governance and to the World Summit on the Information Society.

Cracking down on cyber havens

The government should investigate developing new international instruments to pursue cyber criminals, eg to enable the UK authorities to work more closely with countries that wish to co-operate with reducing cyber crime but may lack the technical capabilities and other resources locally. Once identified, if they cannot be extradited, such criminals should be informed that if they were ever to step on to British soil they would be liable to arrest and they should also be informed that their assets in the UK are liable to seizure. The USA continues to be a major source of child abuse images coming to the UK and this situation needs to be addressed.

The banks and payments industries have a large part to play in helping to stamp out illegal transactions online. It is only because different online payments mechanisms exist that a new breed of cyber criminals has sprung into existence.

Location-based services on mobile phones

An investigation is needed into a range of potential new threats posed by the emergence of location-based services linked to mobile phones. For example where, following a separation, a parent has access to their children controlled or restricted by a judicial order, do we need a new offence to establish that using a location service to track a child's whereabouts could put them in breach of it? Ought location service providers be obliged to cross check with the Sex Offenders' Register before they allow anyone to become a locator? Ought the location service providers be compelled to establish emergency procedures for removing someone from a service where, for

example, they have had to go into temporary accommodation, such as a women's refuge, in order to escape a violent partner?

Challenges to policing and to the child welfare system

Participation in wider forums

Ways should be found to strengthen the capacity of UK policing to participate authoritatively and consistently in wider national forums concerned with policy affecting the internet, and in terms of their interface with high tech or other industries developing new products or technologies that have implications for child safety.

Progress needed

By common consent UK policing has developed some highly effective techniques for tracing people who engage in downloading child abuse images from the internet or who distribute such material online. The arrangements the internet industry has made for working with the police through the IWF are among the best in the world. Where we still need to make more headway is in terms of tracing and providing appropriate treatment and support for the child victims shown in the images, and in dealing with reports of crimes that may be in progress within, for example, a chatroom or other live interactive online environment.

Unmet needs

It is not at all uncommon to hear frontline police officers say, with huge regret, how acutely aware they are that the amount of illegal activity harmful to children that is taking place on the internet is so huge they can only cope with part of it. Moreover, all too often investigations are being, effectively, dropped because investigating officers cannot convince their superiors that the child depicted in the image or the child who appears to be in danger comes from their county, or from their police force area.

Future debates about policing internet-related issues must take account of the fact that the

‘It’s like shooting fish in a barrel. We could go out and arrest many more people who were committing crimes against children online, but that’s impossible without many more officers and the back up from forensics. It’s entirely a question of resources. What you put in determines what you get out, and when you get it.’

DI Darren Brookes, West Midlands Police

internet makes not just constabulary boundaries irrelevant but also, very often, national boundaries as well. The Virtual Global Task Force in part acknowledges that many of the high-tech companies, and indeed many businesses of all kinds, organise themselves across trans-national boundaries and find it hard to respond to concerns or issues that are raised within what is, in effect, a sub-market of what is otherwise a single market. And of course the criminals who misuse the internet do so precisely because they know how difficult it can sometimes be for law enforcement to negotiate complex jurisdictional issues and widely varying operational capabilities.

Within the UK the major problems facing the police can be traced to two readily identifiable sources:

Priorities

In the first place child protection is not one of the government’s top policing priorities. It does not feature as one of the nationally prescribed issues that all chief constables’ performance and all county constabularies’ performance is measured against. When the next draft of the National Policing Plan appears, this must change.

Resources

Secondly, partly because of the lack of priority, and because of the added complication of not always being able to relate potentially criminal activity online back to your own geographical area of responsibility, insufficient resources are being devoted to this type of crime. If it cannot be measured, or does not have to be measured, it will inevitably tend to slip down the list while the things that can or must be measured get pushed up the list. Hopefully it will not be necessary to wait for the outcome of the next consultation on

the National Policing Plan for this matter to be addressed. A review can be put in place now. The need is self-evident. Operation Ore almost brought parts of British policing to a standstill.

Forensics

In this overall picture the lack of forensic facilities is a critical feature or result of the lack of resources. It led to some men who were arrested under Ore being bailed for periods of up to a year while their computers were waiting to be analysed.

A new national policing resource

The police make no secret of the fact that they do not want a repeat of Ore, but that is simply another, more muted way of saying that they need more resources to deal with this new and very particular form of criminal behaviour, about which we are all still learning. A new, operational national policing response needs to be created, perhaps to supplement or enhance the existing tasking, co-ordination and intelligence gathering shell provided by POLIT. Never again should chief constables have to, in effect, weigh their local interests and local accountabilities against the interests of children elsewhere in the country, or elsewhere in the world.

In no way would the new national resource we have in mind detract or take away from local

‘UK policing is getting very good at arresting people for possessing child abuse images that have come from the internet or for distributing child abuse images online. We now need to get a lot better at finding the people who are producing those images in the first place and at identifying and rescuing the children depicted in the images. That is not only a challenge for the police, it is also a challenge to local and central government. There simply aren’t enough places at treatment centres that deal with sexually abused children, and now a new stream is being added to the existing overflow.’

Chris Atkinson, NSPCC

people's right or ability to report any and all crime to or through their local police. On the contrary it would enhance and strengthen the overall policing response.

The police and the industry have repeatedly made the case for a One Stop Shop to be established as a national focal point for the industry and public to connect expeditiously with the relevant part of law enforcement, where an issue of some urgency arises, particularly in relation to children's safety. This might be something like a virtual 999 service. Perhaps this could either be part of or linked to the new national resource that we propose, where police and other agencies could develop a model of working together in a multidisciplinary way. More generally such a resource ought also to have the capacity to provide members of the public with appropriate forms of advice, information or support. This could include advice to parents about the quality and performance of ISPs from the perspective of child safety and the quality and performance of internet filtering and safety software.

Working with parents

Such a national focal point could also establish a closer connection with the work of the DfES. Parents have a crucial role to play in keeping their children safe online and this, in turn, feeds directly into crime reduction strategies. More resources need to be devoted to outreach to parents so they can better support their children's use of the internet at home. Teachers ought to play a greater role in teaching internet safety at school. There is also a need to ensure that school-based personnel who engage in multi-agency child protection arrangements are properly trained for this work in relation to internet issues.

Research and information

More research is needed into the new forms of abuse of children that the internet is facilitating, and we need to improve our knowledge of the therapeutic implications of such abuse, in order to provide better information and support to practitioners at a local level. Longer term studies are also needed into the potential effects of the unprecedented, large-scale and protracted exposure of children to a range of pornographic

or violent images and other material that the internet uniquely allows or facilitates. A new national focal point would be very well placed to provide an organising point for work of this kind.

More resources for abused children

The Home Office, Department of Health and relevant parts of the DfES need to develop a shared understanding of and approach towards online child abuse. Placements at appropriate treatment centres for sexually abused children are already over stretched and now the internet is adding to the pre-existing demands. A survey by Barnardo's published earlier this year, *Just One Click*, revealed that Barnardo's alone was currently working with 83 children whose abuse could, in one way or another, be traced back to the internet or to a mobile phone. This was an astonishingly large number for a single agency. It surprised many commentators, yet other research being carried out by other agencies is likely to mirror and therefore confirm the Barnardo's findings.

Of course it is right that large sums of money are spent on the rehabilitation, treatment and control of child sex offenders, but there is a growing sense of injustice that their child victims' needs do not receive commensurate support or recognition.

Legal reforms

Illegal texts

Clarification of or amendment to the current law is needed to make plain it is illegal to publish texts that offer advice on how to sexually abuse children. Where advice is offered on how to abuse children in such a way as to minimise the chances of the offender subsequently being caught by the police or being successfully prosecuted, this should be a separate offence in its own right or, at sentencing, it ought to be an aggravating factor.

Similarly the law needs to be amended or clarified to make plain that texts that promote sex with children are also illegal insofar as they amount to incitements to illegal sexual acts, or are contrary to the provisions of the Obscene Publications Act 1959, or both.

Drawings, cartoons and paintings

Drawings, cartoons and paintings that, had they been photographs, would have qualified as being indecent photographic images, contrary to the Protection of Children Act 1978, ought also to be made illegal.

‘Causing a child to watch a sexual act’

There is a need to revisit s.12, Sex Offences Act 2003. This stipulates that a person is only guilty of the offence of ‘causing a child to watch a sexual act’ if he does it for the purposes of his own sexual gratification. In other words if someone charges money it appears not to be an offence. That cannot be right. The law should be changed to make it an offence ‘for gain, to cause a child to watch a sexual act’. Such a change in the law would have a major impact on how companies sell or promote pornography on the web.

Classifying images

There is a need to clarify the regulatory regime applicable to video clips, and perhaps also still images, made available online, whether through the internet or via mobile phones. Does ICSTIS have enough powers or resources to supervise properly the content made available through the premium rate system? Ought the BBFC, or similar, have a role to play in regulating the content made available via the premium rate mechanism or more generally via the internet?

Spam

The government should investigate creating a new offence to penalise persons who send pornographic and other kinds of spam that may be harmful to children, on the grounds that by sending it indiscriminately they know, or should know, that they are likely to be putting children at risk. Where it could be shown that children were being deliberately targeted then the seriousness of the offence, and therefore the sentence, should be stepped up.

Extending CRB checks

Criminal Records Bureau checks should be compulsory for all chatroom moderators and employees carrying out similar kinds of

moderation services. At the moment CRB checks are merely optional for such employees. In addition the check should be at the enhanced level. The interpretation of who is or is not a moderator should be extended to cover persons who manage moderators and persons who work with moderators in an ancillary or related role that would give them access to any sensitive or personal information a child may have disclosed.

Civil liabilities of ISPs and other online providers

We should seek clarification of the potential civil liabilities of ISPs and other online service providers in terms of their duty of care to children who use their networks and services. For example, at the moment there is a legal fiction that only persons aged 18 or above may open their own internet accounts. This leads a number of ISPs still to claim they therefore have no legal responsibility for what children do on their networks. The proposition is that because children should only be on the network if an adult has given them an account, all risks and all liabilities in relation to the child’s actions when online accrue exclusively to the adult concerned.

Alternatively, or in addition, a greater and more explicit responsibility ought to be placed on ISPs to determine the identity of each principal account holder. A large part of the UK market is still dominated by pay-as-you-go ISPs whose practice varies enormously in terms of whether or not they know who their customers actually are. Where a principal account holder passes on an account to a child, should there be a legal requirement for that person to ensure that the child’s parent is aware of this fact and consents?

Summary of recommendations

Government and parliament

1. The task force should have its own budget and a dedicated secretariat.
2. Steps should be taken to ensure that, across government, there is a shared understanding of the risks to children online.
3. The Home Office, DfES and DOH, in particular, urgently need to formulate an agreed view and response to abuse via the new technologies. New forms of multi-disciplinary and multi-agency ways of working need to be developed around online abuse and crimes against children.
4. In the wider public interest, the government should develop its own independent sources of knowledge of the internet and related technologies.
5. The government must find ways to develop the capacity of NGOs to participate more fully in the work of the task force.
6. A cyber equivalent of the Indecent Displays Act 1981 should be made law and consideration should be given to placing new duties on web publishers to rate their online content.
7. In relation to children and young people, the data protection laws need to be overhauled to take account of the new realities of cyberspace.
8. New ways should be found to ensure that laws relating to the provision of age-restricted goods or services are not flouted in cyberspace.
9. The government should investigate the possibility of using tax incentives to encourage technology companies, computer manufacturers and retailers to develop new contributions to online child safety.
10. A number of specific legal reforms need urgent consideration (see pages 12–13).
11. The DfES needs to step up its outreach to parents to help them help their children stay safe when they use the internet at home.
12. Membership of the task force should be kept under review to ensure that all relevant interests are always represented.

Policing

13. The National Policing Plan needs to be amended to make child protection a key national target. The resources devoted to this work generally need to be reappraised in the light of its new priority status, and especially in relation to its internet dimension.
14. A new or enhanced national operational police resource is needed to deal with internet crimes against children. This or a related body ought also to be able to deal with enquiries from the public and provide advice, information or support, or be able to direct people to other appropriate sources.
15. We need UK policing to improve the number of child victims it identifies and rescues as part of or following online operations.
16. New ways need to be found to crack down on overseas cyber crime havens. More generally the UK needs to strengthen its contribution to the different international bodies working on child protection online.
17. New ways must be found to enable the police to intervene effectively and in a timely manner in a range of policy and technical forums.

Internet and mobile phone industries

18. An effective public-domain child protection package should be widely available.
19. All computer manufacturers and retailers active in the domestic market should, on all new machines they sell, pre-install child protection software set to a high level of security.
20. Software houses need to devote resources to helping parents and the law enforcement

community defeat a number of pressing technical challenges such as the abuse of peer2peer software, the abuse of anonymity and the abuse of encryption.

21. The provision of passive location services through mobile phones to the mass consumer market raises a number of issues that need to be addressed, eg could the use of such services amount to a breach of an access order following a divorce or other family breakdown?
22. Clarification is needed of the civil liability of ISPs and other online service providers for legal minors who use their networks.

Child welfare system

23. More research is needed into the longer term effects of online child abuse, into new forms of treatment and into the effects of the long-term exposure of children and young people to a range of material now readily available through the internet and related technologies.
24. A reliable means of risk-assessing people found guilty of child pornography-related offences needs urgently to be developed.

Appendix

Children's Charities' Coalition for Internet Safety Agenda for action (2003)

We set out below the measures and messages we think are needed to make the internet a safer place for children. These are categorised by the principal audience to whom they are addressed.

Government

- A new and wholly independent body is required which draws together representatives of children's organisations, consumer groups and other categories of internet users, together with representatives of all parts of the internet industry, members of parliament and the government, to lead an informed public debate on public policy towards the internet.
- Ensure that clear, mandatory and comprehensive guidelines are issued governing the safe use of the internet within schools. This is particularly important in view of the fact that it seems shortly the government will meet its target of giving every child attending state schools in the UK their own email address.
- Bring forward measures to parliament to clarify and modernise existing laws to take account of the new possibilities created by the internet for committing crimes against children, or for enabling other forms of civil wrongs which harm children's interests, eg in relation to luring or tricking children into meetings in the real world, in relation to the police's powers of entrapment to combat online crime, in relation to the commercial exploitation of children by online hard-selling techniques, and in relation to data privacy.

Government and internet service providers

- Internet service providers (ISPs) should be required to ensure that any staff employed to moderate children's chat or other child-oriented internet services have been appropriately trained and police-checked.

Internet service providers

- ISPs that allow children onto their networks at all should have safety messages prominently displayed on their home page with a quick link that takes you straight to them on most if not all other pages. These safety messages should include information about where to obtain counselling or support in relation to inappropriate online contacts.
- ISPs that allow children onto their networks at all should prominently advertise the availability of child-friendly search engines.
- Every ISP should bar all access to telephone lines that have blocked Caller Line Identification.
- ISPs should develop chat-free services.

ISPs and other chat providers

- ISPs that allow children onto their networks at all and give access to internet chatrooms or other chat channels should also provide and promote the availability of moderated chat aimed specially at children.
- Chat safety messages should be prominently displayed close to or in chat areas and mechanisms should exist which would allow suspicious behaviour towards children to be noted, reported and dealt with very rapidly.
- Current ISP procedures should be reviewed to include, wherever possible, the recording and storing of chatroom conversations, as is already the practice with premium rate telephone services, linked to the given identities of the participants.

ISPs and other internet-based services

- Minimum standards should be established governing sign up procedures for new internet accounts. These standards should seek to

ensure as far as possible that new account holders are fully aware of the hazards to children online, and that they are passing on this information to any children who might use their account from time to time.

- Greater efforts should be made to verify both the age and the true identity of account holders, and what relationship they might have to any children to whom they give sub-accounts.
- ISPs should not facilitate access to newsgroups containing child pornography on a regular basis, or to newsgroups or chatrooms that suggest or encourage paedophile behaviour.
- Activities across the site as a whole should be kept under constant review so as to eliminate or reduce any and all hazards to children. In particular links which allow easy exits from children's areas to adult areas, or which provide an interface between them, should be closely scrutinised to determine whether they create an unacceptably high risk that children might be encouraged or enticed to move from one area to the other, or that sexual predators could locate children more easily.

ISPs and the wider industry

- Establish a trust to fund research into the new forms of abuse of children which the internet is facilitating, including longer-term studies of the potential effects of the large scale or protracted exposure to a range of pornographic or violent images which the internet uniquely allows or facilitates.
- Establish a well-funded and properly targeted off-line advertising campaign which focuses on education and awareness of internet safety for children and young people.
- Establish and promote 'walled garden' services specially for legal minors.

Internet Watch Foundation

- Secure sufficient funding to allow a major online and offline advertising campaign about the role and availability of the UK's HotLine service.

Retailers and hardware manufacturers

- Any computers sold into the domestic market should have child safety software pre-installed and set by default to a high level of security.
- All computers sold into the domestic market should be accompanied by a document explaining the basics of online safety for children written in language which is accessible both to parents and the young people themselves.

Software houses

- More research and development is needed to provide better, more robust and easier to use labelling, filtering and blocking software and other programmes, which will allow parents and others with responsibility for children to provide a safe internet environment which accords with their own values.

Internet publishers

- All material published on the internet should, as a minimum, be rated using the ICRA system but the use of a diverse range of ratings systems is also to be encouraged.

What is CHIS?

The Children's Charities' Coalition on Internet Safety (CHIS) consists of seven of the UK's largest professional child welfare and child protection organizations: Barnardo's, ChildLine, Children's Society, NCB, NCH, NCVCCO and the NSPCC. More recently the Stop It Now! UK & Ireland campaign also affiliated. Each of the organizations is a charity and some have histories stretching back to the 19th century.

CHIS was established in 1999. It grew out of an already existing collaboration between the seven children's organizations on the national plan to combat the commercial sexual exploitation of children.

CHIS focuses on lobbying and campaigning on internet safety for children, and on the child safety aspects of other interactive communications technologies.



the children's charity



John Carr
Secretary
CHIS
85 Highbury Park
London N5 1UD
Telephone: 020 7704 7159
Email: john.nch@btopenworld.com

www.nch.org.uk/chis

Cover photograph NCH/Paul Cordwell.
Some NCH photographs are posed by models
Produced by NCH 10/2004. 04/05 0671