

Are we Failing our Children?-

An assessment of Internet Safety Initiatives

posted February 2001

Key Note speech by Nigel Williams, Director, Childnet International



There is a well known, if somewhat gruesome story, about a frog being boiled in a saucepan of water. If you just throw the frog into the hot water it will immediately hop out. But if you place the frog in a pan of cold water and heat it on a cooker, the frog will not realize the gradual change in temperature and will eventually die.

I have worked in the area of children's use of the Internet and especially safety for over five years. I have attended many conferences and meetings around the world on this issue. I have participated in many different expert groups and safety initiatives. I feel it is time to take stock, and make sure that those of us trying to protect children online are not like that frog. Have we been swimming in an Internet saucepan where the environment has got more hostile but we haven't noticed it? Has the general approach so many of us have subscribed to of a partnership between Government (including law enforcement); the Internet industry; and parents delivered the hoped for safer environment for children? Have we like the frog become ineffective, limp and ultimately redundant?

Last June I received an e-mail from a parent whose 13 year old daughter had been contacted in an Internet chat room by a man who went on to sexually assault her. The case caused wide spread media attention and public concern and the perpetrator, Patrick Green, is now serving five years in prison. The father's e-mail ended with an impassioned plea that struck me forcibly:

"I have worked in the computer industry for 18 years, latterly with the Internet, and had no idea what went on in these chat rooms. Surely there is some regulatory body that can make the ISPs monitor at least the teenage chat rooms to make sure kids aren't in danger...."

The father's question is so reasonable "Surely there is some regulatory body...." I found myself wondering whether the complex answer I drafted about self regulation, codes of conduct, terms of service, education and awareness was sufficient. That is why I have chosen to use this opportunity today to look again at internet safety approaches, I hope through fresh eyes.

Have the dangers changed?

The first question we need to consider is whether the online dangers for children have changed. My own view is that the three danger categories of Content, Contact and Commerce that Childnet identified, when we wrote our Agenda for Children document in 1997, are still very relevant. But what may have changed is our understanding of the seriousness of these problems and the risk they pose to children.

The amount of illegal and harmful content online has not reduced in the last five years, indeed such evidence as there is suggests it has grown in absolute if not relative terms. Some have made outlandish claims that 70% or more of the Net is pornography. The magazine Nature published a more scientific survey in July 1999 of the nature of content on the Internet, that suggested that just over 1% of web sites were concerned with pornography. I don't think that the real issue is quibbling about the proportion of the net that is pornography - rather the question is how accessible is this kind of material, and other kinds of problematic content like racist and violent sites, to children. So is it now harder for children to see this kind of content?

The answer is that it depends. It depends on whether you have an Internet service provider that offers some kind of blocking software; it depends on how effective that software is, and whether it is kept up to date and whether it is compatible, even relevant to your culture. It depends on whether parents are aware of the issues involved and taken steps to inform their children. It depends on where the child has access to the Internet, and whether the parent or supervisor has implemented the software or other controls. If you are a conscientious parent in Singapore or Australia your child may be protected most of the time. If you are a child in a country where English is not your first language or a latchkey kid accessing the Internet in a busy library in the USA you may not be so safe.

The Nature definition covered all kinds of pornography - what about the kind that directly exploits children - child pornography - has it reduced? Again such evidence as we have suggests a boom in child pornography on the Internet and a worrying shift from more specialist areas like newsgroups and closed chat rooms to commercial web sites. My worry here is not that children may see such material (although that is harmful enough in itself) but the way the net has fuelled a demand for child pornography - which after all is the actual abuse of children. There are web sites where a picture can be ordered that meets the particular fetish of the adult concerned - child abuse on demand.

Should we not be worried that in a small country like New Zealand with a population of just over 3 million that the law enforcement agencies are catching 100 people each year exchanging child pornography in chat rooms? Scale that up to your own country and you'll have some idea of what it means.

Now in the second area that of Contact, we now know from research carried out by the National Center for Missing and Exploited Children in the USA that 25% of teenagers have "received online an unwanted sexual solicitation or approach in the last year". We have had numerous cases in the USA of men (and some women) seeking to meet children for sexual purposes as a result of contact in chat rooms. As in other areas of the Net's development what starts in the US is mirrored elsewhere and recently pedophiles have sought to use the medium in other parts of the world (as the case I started with highlights).

What worries me most is the interplay between different technologies. Contact in chat rooms leading on to Instant Messaging and ICQ; that leading on to mobile phones - or hand phones as they are called in Asia, cell phones in the USA. A recent survey in the UK showed that 75% of 14-18 year olds now had a mobile phone. This change reflects real peer pressure as communication (not only the hardware, but the activity too) reflects your status and becomes a fashion accessory. Parents are often happy to purchase handphones because it will offer a way of keeping tabs on their children and allow the children to phone if they are in danger.. But the combination of the internet's potential for anonymous contact, and the oh so personal nature of mobiles does leave young teenagers in particular vulnerable to contacts they find hard to rebuff.

I fear that the negative downside of the growth of handphones allied with the new mobility of the Internet is not being addressed or studied. Industry is perhaps guilty of rushing headlong into the development of the "killer Appliance" without thinking through whether there are dangers . The social danger is mirrored by the possible physical danger of

radiation from mobile telephones. It feels like the Industry is willing to tolerate a certain degree of risk as long as they can ensure the sale of the first billion units.

The third C is Commerce. The commercial pressures of the Net have not diminished even with the difficulties that dot com companies have had over the last year. The main factors I would identify are:

- E-commerce is here to stay - the internet is an adept medium for marketing and purchasing an array of products from music to travel
- Building a global brand is an obsession of consumer companies and the Internet is a global medium
- Teenagers are viewed as a key sector of the market and their market spend is increasing
- The web allows companies to collect a lot of information about personal buying habits which conventional shops do not.
- The future of mobile Internet potentially leads to even great opportunity for commercial contact to children as access to the market is not determinant on the fixed PC which may at least be subject to some form of parental supervision.

While the Children's Online Privacy Protection Act has made a significant impact in protecting younger children in the USA, it has not changed the general approach of companies to marketing to teenagers. Childnet remains concerned that this commercial aspect of the Internet can be very exploitative of children and teenagers.

What then of the response?

There have been a number of studies and policy documents prepared around the world about how children can stay safe online. We can discern a general strategy which has emerged worldwide in dealing with illegal and harmful content. It consists of four or five main planks, depending on where one draws the line. First, hotlines to receive reports of illegal content from users; then effective law enforcement; industry's role in having codes of practice and supporting the development of filtering and rating systems; and finally, education and awareness. This is the broad approach adopted by the EU in the Action Plan for Safe Use of the Internet. The Bertelsmann Foundation - a German not for profit foundation - undertook a major study with academic experts and came to a similar conclusion as to the broad strategy to be adopted. The COPA Commission in the USA that reported last October backed a similar self-regulatory approach.

Childnet has always been a believer in the concept of partnership to protect children. We have argued that governments, police forces, internet companies (in all their various guises whether ISPs or portals), schools, parents, and other internet users all have a role to play in helping make the Internet a safer place for children. We also have always believed that to work effectively you have to work internationally, however hard it is to ensure that the partnership between the different sectors has a global dimension. Indeed the Internet has made our shrinking global village feel more like a home in which we all have to live. In a very real sense when it comes to children being harmed online we are only as strong as our weakest link.

Nothing that has happened in the last few years has changed that fundamental belief, but what I do believe has been challenged is the effectiveness of individual elements of that response and the failure on the whole of co-ordinated attempts to work together to ensure that safety is a priority. I would like now to present a score card for how I think the different parties who have a role in protecting children online have performed. I will present both successes and failures. I have decided to call the failures "challenges" so that hopefully we can respond and move forward.

I hope the criticism and praise I offer will be taken in the right way. None of us have any

reason to be complacent on this issue. We all need to learn from what has worked well and what has not.

Governments and inter governmental groups Having a clear strategy, clear legal framework and providing resources for education and awareness are the key issues. A tendency to study as a substitute for acting is a significant weakness

Successes:

- Where they have devoted real resources to the issue of internet safety eg EC Action plan; Australian hotline and Netaware organization; Singapore PAGi initiative.
- Where there is a clear legislative framework which sets out roles and responsibilities of industry and government eg Australia, Germany

Challenges:

- Studies, conferences and more studies without implementation eg COPA commission; OECD study which was never even published; even the excellent Vienna conference on combating child pornography on the Internet has had limited follow through.
- Legislation that cannot be implemented and is unrealistic eg the original CDA; parts of the Australian legislation;
- Child pornography legislation an issue in some areas eg Canada
- Failure in some parts of the world for Governments to fund those working on public information awareness campaigns.

Law Enforcement

The general picture is of dedicated officers doing good work on limited resources. Specialist trained squads are the way forward with the challenge to spread that expertise to areas of the world where it is most needed.

Successes:

- Dedicated specialist units focused on dealing with Internet crime eg New Zealand; FBI innocent images
- Well coordinated international operations eg Italy, Russia; Cathedral.
- Individual officers who are really dedicated to the task

Challenges:

- Lack of funding for this area or insufficient priority or technical expertise
- General lack of coordination or rivalry eg UK constabularies; international slow coordination.
- Too few proactive units - especially in priority areas eg Central and Eastern Europe

Hotlines

Involving users in reporting illegal content harnesses the power of Internet users, but unless the outcome of those reports is effective, the effort could be wasted.

Successes:

- Harnessing user's concerns about illegal content; now x hotlines in y countries
- Much intelligence for law enforcement eg Cybertipline
- Removal of a lot of material eg IWF
- The beginnings of strategic co-ordination of hotlines via the INHOPE Association

Challenges

- Hotlines may give an illusion of dealing with a problem eg removing individual articles from newsgroups is really like trying to empty a bath with a tap running
- Some hotlines are more effective than others and many are not well known among the Internet users in their country.
- Coverage of the world is patchy.

Internet Service Providers

Would that all ISPs took safety as seriously as America Online. There is much room for improvement here, especially in promoting safety

Successes

- Some have made safety a top priority and offered a range of tools and advice to parents eg AOL;
- Some have funded safety initiatives eg Getnetwise; ICRA; Hotlines<PR>

Challenges

- Many seem to see safety as a secondary consideration
- Many seem to use funding general initiatives as a fig leaf and a way of not implementing more rigorous safety policies on their own services
- Often links to safety information whether external like Getnetwise or the ISP's own advice are not prominent enough.
- Many make safety services something you have to purchase separately which actually denigrates the importance of safety
- A failure of effective leadership in uniting Industry to work collectively to ensure that children's rights are protected.

Portals, Content Hosts and individual web sites

This is where increasing problems are arising especially with interactive services like chat available from such companies. They are a diverse community - difficult to get joint action

Successes

- Some have begun to recognize that offering access to services which may be dangerous for children requires them to provide safety advice and take other steps to make access more difficult
- COPPA privacy rules have had an impact on sites collecting information.
- There are some good safe children's portals eg Surf Monkey suitable especially for younger children

Challenges

- There are many sites with interactive services that are dangerous for children which have no warnings, no complaints procedure, and sometimes not even contact details
- "Teaser pages" for adult material remain far too accessible to children
- Junk e-mail advertising sites and services unsuitable for children is far too widespread, and is reaching many individual children.

Computer hardware, software and retailing sectors

Apart from the mixed success of filtering software, this sector is an untapped ally in promoting safe use of the internet

Successes

- Some companies have continued to invest in and develop blocking and filtering technology and there is some consolidation in the industry that may produce better programs

Challenges

- There is no widespread recognition of child safety online as an issue for this sector - no significant initiative to issue safety information with PCs as they are manufactured or sold. [Could be argued that this is a failure of child welfare groups to challenge these sectors to undertake such initiatives]

Education

Within some national school systems there is good work being done as we will hear tomorrow, but some governments are failing to match their push to get schools online with adequate safety policies and training.

Successes

- Some very innovative work in some countries eg Australia, to develop school internet use policies which are comprehensive and followed through in individual schools
- Some effective integrated packages offered to schools including filtering as standard eg UK "managed service option"
- Some good training materials eg Media Awareness Canada
- A new project by the European Schools Network to look at internet safety policies in the education sector across Europe

Challenges

- Insufficient teacher training on ICT generally and especially safety
- Resources to promote effective and safe implementation of internet use in schools in less developed countries
- Use of e-mail in schools by individual pupils
- Waiting for government directives and leadership.

Parents

Parents are not organizations, so it is very difficult to generalize. There are some great examples of informed parents making wise choices; and many instances of parents with little or no information on safety issues, and feeling intimidated by cybersavvy

children.

Successes

- Some parents have recognized the balance of opportunities and risks and are taking close involvement with their children, and implemented safety advice at home
- Some consumer groups have been effective at alerting parents to what are the key issues re safety for their children and provided advice - most effective filtering tools etc.

Challenges

- Many parents have not received detailed information or advice on these issues and are only vaguely aware of dangers and what they might do

- Some parents are simply not interested and are intimidated by new technology and almost wanting to believe that their children are safe.

Child welfare agencies

It is only right to be self-critical too.... I think our major challenge is balancing a constructive role in creating new resources and programs on child safety online with keeping partners in Government and in industry on their toes about what they need to do.

Successes

- Awareness initiatives that have highlighted positive steps parents and children can take eg ECPAT book; chatdanger.com
- Effective commentary on new issues arising with lobbying of industry eg US work on privacy; Save the Children Fund organizations in Scandinavia
- Ability to work across sectors and in many areas make a very real contribution to challenging industry, governments and education to do more.

Challenges

- Lack of resource to disseminate and carry through on initiatives and weariness
- Danger of reinventing the wheel and too many uncoordinated efforts
- Weaknesses in dealing with problem areas eg Russia and Eastern Europe.
- Failure to really tackle areas of the world where the Internet revolution is just beginning.

Conclusion

My general conclusion has to be that while there are some bright points in the global picture on Internet Safety, we have really only just begun. In a number of countries parents are now much more aware of the dangers which must mean that the message is getting through. However, helping children to stay safe is not just about telling children what not to see - we need to build into our Internet safety programmes more positive examples of how children can use this wonderful medium creatively.

To return to the story of the frog in the hot water that we started with, I do think the Internet environment can be a hostile one for children. The way I would put it is that while there are now more opportunities for more children to engage in even more exciting activities online, the growth in the dangers has matched the growth in opportunities.

At our peril do we pay lip service to the issue of online safety. I have listed many challenges in this talk. I would like to end by listing my top three hopes or wishes which I believe will contribute most to internet safety around the world.

1. Every internet service provider and web portal to carry prominent and changing internet safety messages linked to a web site appropriate to the culture of the user which provides guidance for parents and children of different ages, and backed up by offline leaflets and guides.
2. Governments to make a proper investment in child safety online through comprehensive programs ranging from the training of teachers to dedicated internet crime units within law enforcement.
3. All web sites to label their sites with the new ICRA labeling system, with the browser companies making the system easy to find in their browsers, with simple culturally tailored user interfaces.

These are not impossible dreams, - they simply require investment and action. Our children deserve no less so that the amazing wealth of good that is waiting them online outweighs the negatives that exist.