Contribution by Peter Robbins - Chief Executive Internet Watch Foundation to the hearing on combating sexual abuse, sexual exploitation of children and child pornography organised by the Civil Liberties, Justice and Home Affairs 28th/29th September 2010 – Brussels.

Good morning and thank you for giving me the opportunity to speak today about the UK experience of Notice and Takedown and about Blocking because the organisation I represent provides a list of child sexual abuse websites to 70 companies around the world so they can protect their customers from inadvertently stumbling across such content.

Notice and Takedown and Blocking websites are tactics designed to help disrupt the distribution of child sexual abuse content to complement the work of the judicial authorities and others in their efforts to rescue children from abuse and to detect offenders who are abusing children or distributing images of child sexual abuse. We understand there will be a time lag between the exchange of information between the various bodies charged with making a decision as to what course of action is to be taken within a national framework and so whilst that decision making process is in chain blocking access to child sexual abuse material helps prevent the further distribution of material and the ongoing repeat victimisation of children in the images that happens whenever someone views their abuse.

So is there any evidence that Notice and Takedown and Blocking work?
In our opinion there is. Two years ago our URL List contained an average of 1,500 URL's a day, a year later it was down to 800 a day and today we are averaging 400 a day and apart from a handful of URL's no URL has been on the List for longer than a month, a substantial difference to two years ago. This has happened as a result of the work of all our partners in speeding up the processes of getting child sexual abuse material removed.

Who is the IWF?
The Internet Watch Foundation is an independent self-regulatory body, funded by the EU and the wider online industry, including internet service providers, mobile operators and mobile manufacturers, content service providers, filtering companies, search providers, trade associations, and the financial sector. We work internationally with INHOPE Hotlines and other relevant organisations to encourage a global response to the problem.

Since 1996 we have managed almost 300,000 reports and have over 13 years' experience tracking and understanding the technologies, trends and movements behind the websites we deal with.

Content Trends
The nature, number, and profitability of child sexual abuse content on the internet are the subject of much speculation. In our opinion this content represents a relatively small proportion of total internet content although it remains a very serious and persistent challenge.

This is an extremely fast-moving environment. Techniques used by criminals who sell, purchase, share or collect child sexual abuse images are sophisticated and are diversifying. Methods of operation appear ever more opportunistic. Distributers are increasingly exploiting apparently legitimate internet services to make the images available: from free or cheap hosting platforms and image sharing websites to social networking areas and hacked websites. We are aware of interrelated networks of child sexual abuse websites and their supporting payment and marketing platforms moving around the world and across hosting services regularly, frequently using automated or randomly generated systems to speed up and complicate hosting arrangements in an attempt to elude investigators.

As the distribution technologies and methods develop, tactics for combating them may become obsolete. Predicting the next distribution trend for the future is difficult. National police agencies have finite resources to carry out long-term investigations into large-scale global activities which span multiple jurisdictions, borders, and continents so it is essential that everyone who has a role in making the internet a safer place works together to tackle the problem.

There are a number of strategies and tactics which are making a difference in minimising the availability of this content but unfortunately, there is no international agreement on tactics so for example, some countries do not, to our knowledge, have an established system for the swift and effective removal of this content. Furthermore, debate continues in some countries regarding what should be taken down, who has the right or authority to notify a company to remove it, and at what point in a potential investigation it should be removed.

One global law enforcement unit

Ideally there would be one multi-national global law enforcement unit dedicated to investigating child sexual abuse websites because the pace at which the trends change are not conducive to traditional regional or national law enforcement and judicial structures.

Whilst there is, of course, agreement that children must be rescued from suffering and child sexual offenders must be investigated and prosecuted, the existence of different approaches to tackling this problem globally cause real challenges, including the fact that content remains available whilst an investigation is in progress.

Network level blocking

Network level blocking has received attention from many quarters in recent years. The IWF has been providing a URL specific list to facilitate the blocking of child sexual abuse content since 2004. This list is now deployed, on a voluntary basis, by over 70 companies across the UK and in many countries around the world including internet service providers, mobile operators, search providers and filtering companies. At least 98.6% of all domestic broadband connections in the UK are covered by virtue of UK ISP's voluntarily deploying our List of child sexual abuse URL's.

We take immediate action to effect the removal at source of child sexual abuse content hosted in the UK. If it is hosted abroad we pass details to our INHOPE Hotline partner or law enforcement colleagues in the hosting country so they can investigate the content in collaboration with the relevant national authorities and within their national legislation.

Whilst non-UK hosted child sexual abuse content remains live we add the URL to our list. The URLs are assessed according to UK law, with each image being categorised in line with published criteria set out by the UK Sentencing Guidelines Council.

Trust and confidence

Facilitating blocking through list provision is an important and trusted responsibility and our work is overseen by an independent Board according to approved policies and procedures, following legal advice and with the ongoing technical guidance of our industry members. Specialist police officers train our staff to assess content and we work within a strict legal framework. The systems and processes involved in handling reports, assessing content and compiling the list are also periodically inspected by a range of independent experts.

I should make it absolutely clear the IWF assesses criminal content only, we have no powers to investigate offenders but our existence in the UK adds value to UK policing effort because the majority of the 40,000 reports processed in 2009 relate to content hosted abroad and therefore outside the jurisdiction of the UK policing authorities. As we receive no funding from the UK government so it follows that we do not benefit from funding intended for policing purposes. The majority of police websites point UK internet consumers to the IWF website to report indecent images of children because the likelihood of the image being connected to the police region where the complainant resides would indeed be very rare.

Collateral damage

It is our view that any list must be URL specific especially as much of the child sexual abuse content known to the IWF is currently hosted on legitimate internet services and so domain level blocking, DNS poisoning or IP address black holing would make significant numbers of otherwise innocent internet services potentially unavailable.

Regular updating

In our experience child sexual abuse content is highly transient and may move hosting company and country every few days. Therefore, to be as comprehensive as possible and to

avoid the blocking of obsolete URLs or updated legal content any list should be refreshed and then redeployed at least once a day.

Transparency

Blocking should be carried out in a transparent way and, in the interests of wider public protection:

i) It is important that there is an easy way for the public to check which companies are blocking.
ii) Appropriate information should be displayed to a consumer when access to a page is denied.

Complaints and appeals

A robust complaints and appeals process should exist to enable anyone with a legitimate association to the content to complain about its assessment and inclusion on a block list.

Scope creep

There is some concern that the infrastructures developed to facilitate the blocking of child sexual abuse content will be abused to block a wider range or criminal or even legal content in the future. Safeguards and commitments should be developed to ensure this concern is minimised and the specificity of the blocking is preserved. In the six years that we have been providing a List in the UK there has been no other types of content included.

Proportionality and cost

Considering the relatively small proportion of internet content that depicts child sexual abuse it is important that responses, particularly blocking, are proportionate and effectively balance online safety and protection with the right to freedom of information and cost of deploying blocking. No-one should have a right to access child sexual abuse content therefore if blocking is done ‘intelligently’ then it could be a worthwhile addition to a range of tactics to disrupt access to the content.

Verification of deployment and self certification

The provision of a list to a company does not help in determining whether that list is being deployed, whether it is being regularly updated and indeed whether it is preventing access to child sexual abuse content on the list and not to other legal content or legitimate services. Therefore, methods for certifying the effectiveness of list deployment by all relevant companies taking the list should be considered and that is something we are pursuing in the UK.

Thank you.