children's charities' coalition on internet safety

The UK's Children's Charities' Coalition on Internet Safety brings together twelve professional, national children's and young people's organizations with specialist knowledge and expertise across a broad range of child welfare, child development and child protection interests. The charities all share a great enthusiasm for the digital revolution which was triggered by the emergence of the internet. We can see the tremendous advantages and possibilities which a converged, always on and always available internet could deliver. We want every child and young person, in all parts of the world, to have full and equal access to the huge benefits which the new technologies can bring, within the safest possible environment.

We are grateful for the opportunity to comment on the European Commission's Green Paper *"Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values" Brussels, 24.4.2013 COM(2013) 231*. Its publication is most timely. The paper correctly anticipates the magnitude and importance of a series of changes which are already clearly visible on the near horizon. Public policy making institutions generally struggle to keep up with the consequences of technological change. For once, instead of simply reacting or playing catch up, we may be in with a chance of shaping events.

Areas of interest

There are two key dimensions to the views CHIS wishes to express in relation to the emergence of a fully converged audiovisual world. These concern

- the growth and spread of wireless connectivity to the internet linked to the availability of ever greater numbers of easily portable devices which can make use of it

- the emergence of internet connected TV sets in family homes and other environments where children and young people are likely to be found

The growth and spread of wireless connectivity to the internet

Practically every new electronic device which is likely to be used or valued by a child or young person is easily portable and comes with WiFi built in as standard[1]. This means the child or young person can connect to the internet from any of many millions of "WiFi hotspots" which are available in public and semi-public places in the UK[2]. The high quality of the graphics and sound linked to the speed and falling costs of the connections mean there are, in principle, no barriers to accessing any kind of audiovisual material that might be available on the internet.

Once the internet is in a child's pocket or school bag and they can connect to it in any burger bar or coffee shop, or in any railway station, the possibility of meaningful parental supervision and support of the child's or young person's internet usage becomes a wholly impractical proposition. Potentially anything and everything that is "out there" is available to the child or young person.

"Anything and everything" on the internet includes not only illegal and unlawful content but also legal content which is highly age inappropriate. The child or young person need not go looking for such material intentionally. Even wholly innocent searches could take a child or young person to places that are not at all suitable for them.

The 2008 Eurobarometer survey found[3], *"parents of 6-17 year olds in the (then) EU27 were rather or very worried about their child seeing sexually/violently explicit images (65%), being a victim of online grooming (60%), getting information about self-harm, suicide or anorexia (55%), being bullied online by other children (54%), becoming isolated from other people (53%) and giving out personal/private information online (47%). A quarter of parents worry about all of these risks. And parents worry more about girls and about younger children (though, as was seen above, boys and teenagers encounter as many or more risks online)."* Many surveys since have shown similar levels of parental concern.

So what are parents to do in a world of wireless connections? Bear in mind in a typical family home with two or three children there might be upwards of twenty portable WiFi enabled devices coming and going, being used, borrowed, loaned, repaired or rested at any one time. While games consoles, tablets, smartphones and laptops are the most common of these, if the technical press is to be believed they will soon be joined by internet enabled wrist watches, spectacles and other wearable devices. These gadgets might have been manufactured by five or six different companies each using their own particular terminology, icons and approaches. Could parents reasonably be expected to turn off or, an on-going basis, manage the availability of WiFi connectivity on their children's portable devices? CHIS does not think that is realistic and in any event it contradicts part of the point of having WiFi at all.

---

[1] http://stakeholders.ofcom.org.uk/market-data-research/market-data/communications-market-reports/cmr12/internet-web/uk-4.22. Shows patterns at 16+.
http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/online_access.pdf shows 7-16.

[2] BT alone claims to have in excess of 4.5 million in the UK

[3] http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20(2006-9)/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf

Given the central importance of internet access to education in the 21st Century and to young people's social, cultural and family lives we are way past the point where it is any longer realistic or in any way desirable to argue that a modern child or young person should be deprived of access to the internet either permanently or for any protracted period of time. That is a counsel of defeat.

CHIS believes we need protective solutions that operate at network level, in ways which work with all equipment manufacturers' products. We appreciate that some might see this as letting manufacturers off the hook but putting in protective solutions at network level is likely to be much more efficient and will more effectively ensure the measures have the desired reach. CHIS is certainly not opposed in principle to controls also being pre-installed on the devices themselves and there may be individual instances where that is the better answer.

Specifically in relation to TV channels, as more and more of them present their content online, in a wireless world any notion that a parent can help determine what should and should not be watched by younger viewers evaporates.

With the BBC iPlayer, 4OD and other catch up or on-demand apps, watersheds can become meaningless. Many parents will not even know if their children have downloaded them and, up to now at any rate, the age verification and authentication components of catch up and on-demand apps are so weak as to be almost worthless. The distinction between linear and non-linear content ceases to exist.

The same is likely to be true with streaming services even though the mechanisms are different. Unless these too are associated with strong age verification systems they are likely to open up adult or restricted content to youngsters who could not buy the same materials in a shop or view in a cinema.

In the end this argues for every user to have an individual log in which has been age verified and for the content or services which they can access to be configured around their individual profile. Of course there should be a parental override but that too should be linked to a robust age verification or identity authentication system to ensure they are the ones making the override decision.

Parents very much want to exercise some control over the sort of content and services their children can access online yet many have found that the filtering tools presented to them hitherto (principally by ISPs but also by others) have been bewilderingly complicated[4] and therefore too difficult to implement. This was the primary inspiration behind the UK Government's decision to encourage ISPs to present filtering options to parents in the simplest possible way, as a default, and for UK WiFi providers, also by default, to screen out all adult content in public spaces where children and young people are likely to be found.

Default on delivers simplicity. It also means the protective tools being referred to can be provided to children and young people in families where, for any number of reasons e.g. poor educational attainment levels on the part of parents, inability to understand the local language, such measures might otherwise never be invoked.

[4] http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/annex2.pdf see page 21

In our view convergence and ubiquity shout out for much greater harmonisation across all digital media platforms in relation to the tools which will help parents to keep their children away from age inappropriate, unlawful and illegal content.

Parents should not have to jump through hoops to make devices safe or appropriate for their children. If parents want to learn how to make the device less safe, if they want to reconfigure, liberalise or to abandon the tools altogether that is a matter for them and they should of course be free to do so, but it should work that way around, not the other.

- WiFi, 4G and other wireless technologies are now a fact of life. When linked to the growth of WiFi enabled portable devices this makes close or on-going parental supervision of the whole of a child's or young person's internet usage a practical impossibility. This means high tech suppliers have a larger responsibility to devise mechanisms to compensate for that inevitable loss of parental engagement.

- This points towards the need for "family friendly" network level controls which are turned on by default. Any reconfiguration away from the defaults should be strongly associated with individual log-ins which have been age verified in a robust way.

  It is accepted that "family friendly" is a rather elastic term with potentially a significantly high degree of cultural specificity. Local law might also be relevant in certain contexts. However, a framework could be developed which either met a broadly accepted standard or allowed for a level of flexibility at national level. Any family friendly environment ought to incorporate mechanisms which block access to known illegal and unlawful sites.

The emergence of internet connected TVs

Turning to internet connected TVs: in our view this is a major, radical development which is absolutely guaranteed to push the question of internet regulation centre stage in every country where it reaches critical mass.

At the moment, how children and young people use the internet, knowledge about the sort of content they are accessing, can all too often slip under the parental radar if most of the internet usage takes place via a portable device up in a bedroom, out in the garden or on the street. Once the internet is available through the big TV screen in the family living room potentially the whole of the internet is available in that same room. Donald Duck, Pirate Bay and pornhub.com will coexist on the same screen, separated by only a few accidental or deliberate clicks of the remote.

Bear in mind that the family TV is likely to be watched most frequently by younger children, often with Mum or Dad in the room and controlling the remote, but perhaps just as often when they are not. Parental anxieties about the sorts of images and sounds that might be accessible on that TV screen are likely to increase by several orders of magnitude.

Thus the risk is, on such a sensitive issue as child protection, if measures with a wide level of acceptability among parents are not taken at European level the demand for national Parliaments or elected Assemblies to act within a given country will become irresistible. It would be a brave local politician who pleaded that they were helpless to do anything to protect British, French or Spanish children because their hands were tied by Brussels. The political damage to EU institutions could be considerable, particularly if, as would be likely, national newspapers decided to weigh in.

- Either within the TV itself or at the level of the router or set top box that delivers both linear and non-linear content to the screen, controls should be put in place by default which will present and preserve a family friendly and legal environment.

- It should be possible for every family to reconfigure the defaults or to abandon them altogether. However, any such changes to the defaults should be linked to a robust age verification mechanism which ensures it is an adult making the decision.

Peer2Peer networks

As CHIS we have had a longstanding concern about the abuse of Peer2Peer networks. We also have concerns about the misuse of different types of filesharing sites and the wider Darknet but Peer2Peer deserves to be considered in its own right as it is used by substantial numbers of people who do not have the technical knowledge or determination to engage with TOR clients, encryption and the like or may not yet have found their way to other forms of filesharing environments.

Many children and young people have been using Peer2Peer software to obtain unlawful access to and use of IP infringing content such as music, software and films from pirate sites.

Data published by the BBFC and the Industry Trust for IP Awareness not only documents the harm to the UK economy and jobs that can be caused by this type of piracy it also outlines more immediate hazards to children's and young people's welfare.

The research shows that over a third (37%) of children aged 11 and 12 admitted to having recently downloaded or streamed a film rated 15 or above from a pirate site. More than a quarter of 11-15 year olds (27%) say their parents don't know what films they are watching online, and a third (32%) wouldn't feel comfortable with younger siblings copying their viewing habits. Almost one in five young film fans (18%) admit they have been disturbed by the movies they have watched on pirate sites and two thirds (65%) wish they had checked the film's official age rating first.

But it is not only IP infringement that Peer2Peer software can facilitate. Our main interest in Peer2Peer historically has been in relation to its role in facilitating the widespread, large scale distribution of child abuse images (child pornography). It is very unlikely that children or young people would engage with Peer2Peer software in that way but many parents will be unsettled by the fact that such material is often accessible on the same networks.

In addition, many Peer2Peer users who are not involved with child abuse images will allow persons using the same programme to access a wide range of material that they might have collected. We have had reports, for example, that via Peer2Peer young people have been exposed to videos of decapitations carried out by terrorist groups, of them coming across images of bodies which have been severely mangled or squashed in road accidents, or of lynchings being carried out by the KKK. Such pictures could have a terribly scarring effect on even mature, rounded adults, never mind younger or more fragile minds.

The point about Peer2Peer is that while it is a difficult, resource intensive business to police it, to the best of our knowledge, because the file sizes can be extremely big, by and large in the past its use has been limited to downloads over faster fixed internet connections, typically in the home, to devices with capacious hard drives. With the emergence of 4G and soon even faster wireless connections, and with the development of cloud computing with its acres of free or cheap storage, it will become ever more practical to use Peer2Peer outside the home on exactly the sorts of devices huge numbers of children will be carrying around.

We are not arguing for a ban on Peer2Peer software. It has many perfectly legitimate uses but wherever possible, by default, access to Peer2Peer programmes should be turned off at the point of first connection on all devices likely to be used by children and young people and on the family TV's internet connection. There needs to be a substantial public awareness raising campaign which highlights the malevolent ways in which Peer2Peer networks are being used. We need to get across to parents that Peer2Peer is not just about ripping off Hollywood or the Rolling Stones. It can pose a very real danger to children's health and well-being.

- Within any "family friendly" online environment by default access to Peer2Peer programmes should be turned off.

- If there is no technical way of blocking Peer2Peer programmes as a group a list of the principal programmes should be created as the basis for blocking. The list should be updated automatically. The ability to turn on Peer2Peer access should only be available to an age verified adult.

- A major public awareness campaign should be mounted drawing attention to the various drawbacks and hazards to children and young people of Peer2Peer and other filesharing environments. Included in the campaign should be references to the role of these programmes in providing access to illegal content and IP infringing content.

---ooo---

John Carr OBE
Secretary
Children's Charities' Coalition on Internet Safety
10, Great Queen Street
London WC2B 5DD
14th August, 2013

john.carr49@btinternet.com
www.chis.org.uk