ISPA response to the parliamentary inquiry into online child protection

ISPA

The Internet Services Providers' Association (ISPA) UK is the trade association for companies involved in the provision of Internet Services in the UK. ISPA was founded in 1995, and seeks to actively represent and promote the interests of businesses involved in all aspects of the UK Internet industry.

ISPA membership includes small, medium and large Internet Service Providers (ISPs), cable companies, web design, hosting companies and filtering vendors. ISPA currently has over 200 members, representing more than 95% of the UK Internet access market by volume.

ISPA was a founding member of EuroISPA, the European Internet Service Providers Association based in Brussels, which is the largest umbrella organisation of ISPs globally.

Introduction

The internet industry has devoted considerable attention and resources on ensuring that its customers can use the Internet in an enjoyable, safe and appropriate way. This is particularly true of children and the industry has, through its work in bodies such as the UK Council for Child Internet Safety and the provision of various filtering solutions, actively contributed towards making the internet environment safer. Ultimately we believe that the final responsibility for protecting children online falls to parents who are best placed to monitor and control what their children are doing online, to decide precisely what content should be available to their particular children, and at what age, and to teach appropriate behaviour to their children. We view technical measures as an aide to good parenting, not as a viable alternative. The appropriate role for industry is therefore, in our view, to raise awareness amongst parents and to support and empower parental decision-making, not to seek to supplant it.

A great deal of work has been conducted in this area in the last few years – including the Byron Report, Culture, Media & Sport Select Committee and most recently the Bailey Review. Bailey made a number of recommendations on online child safety and set out a timetable for action. Industry is reviewing the recommendations and responding by updating parental control offerings whilst other ISPs have agreed an industry code of practice that will give customers an active choice and a ministerial summit has discussed this initial response.

Although some of the questions put by this Inquiry relate specifically to pornographic content, we note that there are various categories of content that parents may consider inappropriate for their children to view. Our members are committed to supporting and empowering responsible parenting in relation to Internet use generally, not exclusively in relation to material of a pornographic nature.

1. To understand better the extent to which children access on-line pornography and the potential for harm that this may cause

The Inquiry will be aware that the research base on the extent children access pornographic content and how much harm this may cause is quite small. Recently, the EU Kids Online

research project recently demonstrated that 11 per cent of 9-16 year olds have seen sexual images online in the UK.[1] This compares to an EU average of 14 per cent and it should also be taken into account that the offline exposure to pornographic content is still higher than the exposure online.[2] Whilst it is clear that young people access inappropriate content online, research suggests that this may not be as widespread as often claimed.

The research basis for assessing the potential harm that this causes is limited, but our understanding is that age and style of parenting are mediating factors. There is a difference between 12 year old or a 16 year old accessing adult content and active parental mediation will also have an effect. This does not imply that there is no harm involved but, in the interest of evidence-based policy making, further research may be necessary before restrictive policy measures are contemplated. The EU Kids Online research project also suggests that "since risk increases as use increases, it might seem simple to call for restrictions on children's use of the internet. But online opportunities and digital literacy also increase with use, so there is no simple solution. Rather, ways must be found to manage risk without unduly restricting opportunities."[3]

2. To determine what British Fixed Internet Service Providers have done to date to protect children online and the extent and possible impact of their future plans in this area

ISPA members have done a great deal to make their customers' online experience safer and will continue to offer their customers the tools to equip themselves online. The empowerment and protection of customers is a challenge on which industry works with a range of stakeholders, including industry partners, government, charities, NGOs and law enforcement.

ISPA members build their understanding of potential risks from a variety of sources, including customer complaints, customer care reports, information-sharing with peers and partners, independent research and in-house user and market research. This is then used to tailor and update existing safety and security services and options.

To prevent inappropriate access to adult content, ISPA members provide parents with a number of products, controls and solutions to allow them to make informed decisions about what content their children access. These (often free) solutions enable parents to block children's access to inappropriate or potentially harmful material online. There are two types of solutions for fixed ISPs: those where filtering is done on each individual device – such as a PC - and those where filtering is done on the network. Filtering tools at the device level can be set to different levels, depending on the user's preferences, and so offer a means of controlling risk in a more personalised, flexible and effective way. Network-based tools allow all devices in the household to be covered and may allow each household to configure what they want to block (though it cannot be tailored to each device/user). This can be through the ISP's network or through a home router.

[1] http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/Final%20report.pdf
[2] http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/D4FullFindings.pdf
[3] http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/Final%20report.pdf

The UK has a very competitive broadband market with ISPs able to differentiate themselves by offering competing security products as part of their overall offering. Examples of security tools offered by consumer broadband providers for free include:

- BT - BT Family Protection, an opt-in, device-based service offered to customers provided by MacAfee Parental Controls
- Orange Home – offers all customers on all broadband packages MacAfee Parental Controls, device-base, free and opt in on up to 3 PCs. Orange has a range of educational materials that are available in-store and online
- o2 - offers customers MacAfee Parental Controls free to on an opt-in basis
- Plusnet – offers customers Plusnet Protect, an opt-in, device-based solution provided by a third party
- Sky – offers customers McAfee Parental Controls, free for as long as they are needed on up to 3 PCs in the home, on an opt-in basis
- TalkTalk – HomeSafe, an opt-in network level solution. Device-based also offered.
- Virgin Media – offers customers parental control device-based software for their PCs on an opt-in basis

A number of other free device-based solutions are readily available, including Netnanny and K9, both available as free downloads.

In summary, ISPs in the UK have – and will continue – to put effort and resources into making their customers online experience safer. There are a number of different options currently available provided by ISPs that allows users to choose the right tools for them. Some Fixed ISPs may choose to do this at the network level, others feel that device filtering on PCs, routers or phones provides more effective protection. Either way, there is a choice in our highly competitive market for parents to make an informed, empowered decision.

A number of expert witnesses, including John Carr, stated that parental controls will never be effective for all children in all situations. Therefore equal importance must be placed on the need for safety education for children and information and advice for parents and teachers. Ofcom's recent market research into children's online behaviour shows that parents without filters place more reliance on speaking with their children about their online use especially those with older children.

3. To determine what additional tools parents require to protect children from inappropriate content

ISPs know their customers and if feedback from users shows that additional tools are required, ISPs will respond to this accordingly.

However we do agree with the panel that parental controls should be available to all customers, actively promoted and easy to use. ISPs are reviewing their offerings and where necessary will make improvements in these areas whilst other ISPs have agreed an industry code of practice that seek to improve consumer education and awareness and offer an active choice to customers.

As stated in question 2 there is a plethora of options available, from free to paid-for solutions provided by a customer's ISP to independent vendors. The UK, in comparison with European neighbours, has a relatively high take up of parental control filtering.[4] If greater take up is required, there may be a need to increase awareness of existing products and services.

The internet sector is by its nature innovative and to reflect this, companies are constantly developing new services and products and updating advice. Industry has a role to play in empowering users to ensure that children are protected online and will continue to do so. This is a joint challenge for industry, government, parents and carers and forms part of the challenge laid down by Bailey that industry is currently responding to.

4. To establish the arguments for and against network level filtering of content that would require an 18 rating in other forms of media

It is important that parents and carers can choose an ISP that offers the right solution, whether that is software on an access device, hardware run and controlled within the home, a service provided by the ISP (or other 3rd party) or a combination of the above, and that there is healthy competition between ISPs to provide them with the best service possible. The UK market provides for this.

Both network level and device based filtering can help parents and carers control access to content online and it should be viewed as a technologically neutral issue. Device-based software offered by ISPs is PC-based, ie: it is installed on to a PC as a download or via a CD. Network-level filtering can be through an ISP's network or via a home router. It would be a mistake to mandate one solution over another or view one as a silver bullet

Both network and device filtering are configurable to block different types of content, require a degree of parental activity, once activated automatically update and are relatively easy to set up and configure. In particular customers only need to click on a link to activate downloadable parental controls. In addition parents can choose to alter these settings, add/delete websites and limit when children can go online.

Features offered by PC-based filtering include:

- can be tailored to individual devices and individual users offering greater flexibility in the home for multiple users (e.g., to provide separate settings for adults and children, or for children of different ages);
- protects children when they take a laptop outside of the home;
- can record and allow parents to review chat sessions and other applications to prevent inappropriate communication.

Features of network-level filtering by an ISP or on the home router include:

- covers multiple devices in the household meaning it only needs to be set up once;
- is generally quicker to set up

[4] http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EUKidsII%20(2009-11)/AnnualReport2010.pdf

Taking the above into consideration, overall, we feel that device based filtering (such as software downloaded or installed onto a PC) offers more advantages than network-level[5]. However, whether it is device or network level control, we believe that the key to successfully protecting children online is that parents are in full control and actively decide to activate filters.

Active parental controls and mediation play an important role in reducing the potential harmful effect of children accessing inappropriate content, and we believe that filters that are turned on by default will reduce the degree of active interest and parental mediation. This could lead parents into a false sense of security, thinking that all 'bad' things cannot be seen.

It is also worth considering that unlike other forms of media, ISPs do not have direct control over the content that their customers are accessing online. Online content consumption is demand-led and customers should be in control over whether legal content should be blocked on their connections.

5. To recommend to Government the possible form of regulation required if ISPs fail to meet Recommendation no.5 from the Bailey Review.

As the committee is aware, the Industry is reviewing the recommendations and responding by updating parental control offerings whilst other ISPs have agreed an industry code of conduct on online child safety that provides for harmonisation of advice material to parents and commitments to introduce active choice for parental controls and an independent review. ISPA feels that by offering active choice in this way, Bailey's fifth recommendation will be met. It will be seen over the coming months how effectively these new measures will be implemented and there may be a debate to be had around how we should measure success.

However, as recognised by Byron and Bailey parental controls can never be 100% and equal importance must be placed on the need for safety education for children and information and advice for parents and teachers. A wealth of existing parental controls already exists that allows content to be filtered at the network level or on individual devices. With the recommendations of the Bailey Review and the competitive nature of the broadband market, industry will promote these tools so that customers can continue to choose the provider that offers the security solutions they require.

[5] This view is not shared by TalkTalk, an ISPA member, who consider the best proposition to be both device and network-based are offered