Written evidence submitted by EU Kids Online [OLS0030]

Preamble

We note with interest that the Culture, Media and Sport Committee has decided to investigate a number of aspects of online safety that are currently raising concerns, in particular:

• How best to protect minors from accessing adult content
• Filtering out extremist material, including images of child abuse and material intended to promote terrorism or other acts of violence
• Preventing abusive or threatening comments on social media

This response is written by Professor Sonia Livingstone, on behalf of the EU Kids Online network.[1] This response may be made public. The address, for a copy of the Committee's report, is S105, Department of Media and Communications, London School of Economics and Political Science, Houghton Street, London WC2A 2AE.

Much of EU Kids Online's work has focused on scoping the nature and consequences of the online risks of harm encountered by children aged 9-16 years old in Europe. The detailed recommendations below relate to the European findings detailed on our website.[2] For UK-specific findings, see Livingstone, S. et al. (2010) *Risks and safety for children on the internet: The UK report*. At http://eprints.lse.ac.uk/33730/

Summary

The strength of a cross-national study is that it reveals how the UK measures against other European countries. In many respects, the UK has been a leader in protecting children against online risk of harm. However, EU Kids Online's cross-national analysis also reveals that this protection has often come at the cost of empowering children to benefit from the digital skills and opportunities of new online technologies. Specifically, we found that European countries divide into four main groups, based on children's risk profiles: Supported risky explorers; Semi-supported risky gamers; Protected by restrictions and Unprotected networkers.

In Belgium, France, Germany, Greece, Ireland, Italy, Portugal, Spain, Turkey, **and the UK**— the 'protected by restrictions' countries, parents tend to overprotect their children, significantly reducing their online opportunities. Researchers are concerned that both too much parental restriction and the lack of support for children's online use might lead to higher levels of harm when risk is encountered. Hence the EU Kids Online network consistently emphasises that policy to encourage opportunities should accompany policy to reduce risk of harm.

Main points

1. Children have the right to protection and safety online but they must also take responsibility for keeping safe and respecting the rights of others online.
1.1 New means of internet access, less open to adult supervision, are increasingly evident in young people's internet use. Nearly half of all children in Europe go online in their own bedroom where it is unrealistic to expect parents to monitor their safety.
1.2 Children need to be encouraged to develop self-governing behaviour in which they take greater responsibility for their own safety in the use of the internet.
1.3 Awareness-raising should emphasise empowerment rather than restriction, and appropriate, responsible behaviour with regard to technology use.

2. A new focus is needed on internet safety for younger users.

2.1   It is important to balance protection of younger users with opportunities. It is important not just to make the online world safe by stopping their use of internet services, but also to ensure their participation in safe ways.

3. Safety messages should be adapted to new modes of access.

3.1   33% of children now go online via a mobile phone or handheld device. Laptops, mobile phones, game consoles and other mobile devices allow children to go online anywhere, anytime, away from parental supervision. Emerging services (such as location-based ones) may lead to new risks.

4. Children's online opportunities and skills need human and financial investment.

4.1   Not only do younger children and girls not progress as far up the 'ladder of opportunities' as teenagers and boys, many never reach the final set of activities at all. Only half of 9-10 year olds progress further than basic content-related activities.

4.2   Promoting more creative and skilled applications is essential to ensure all children avail of online opportunities.

4.3   Schools play a pivotal role in digital skills development, mitigating forms of digital exclusion. However, teachers are often inadequately resourced and trained to carry out the functions entrusted. Country differences in online skills point to the need for targeted educational interventions where there is evidence of a digital divide.

4.4   Since opportunities and risks online go hand in hand, efforts to increase opportunities may also increase risks, while efforts to reduce risks may restrict children's opportunities. A careful balancing act, which recognises children's online experiences 'in the round', is vital.

5. Positive online content for children should be made a policy priority.

5.1   Provision of appropriate – high quality, diverse content online should be a priority.

5.2   The "European Award for Best Children's Online Content" is a valuable step in this direction, but such provision could also be supported by high profile national initiatives.

6. Digital safety skills are needed to build resilience online.

6.1   Inequalities in digital skills persist – in terms of SES, age and, to a lesser degree, gender, so efforts to overcome these are needed.

6.2   Younger age groups need to be a particular priority for parents and teachers. Secondary level schools to date have been the main providers of ICT skills training but new interventions are required at the primary level.

6.3   Encouraging children to do more online will also improve their digital skills as well as their overall confidence and/or increasing children's beliefs in their abilities to use the internet. Similarly, teaching safety skills is likely to improve other skills, while teaching instrumental and informational skills will also improve safety skills.

6.4   Given uneven digital skills, particularly safety skills, across Europe and the discussion among stakeholders about the need to identify more precisely the kinds of skills required, an inventory and agreed framework for digital safety training would provide a valuable resource for educators, awareness-raising and civil society groups.

6.5   Schools are uniquely placed to reach the maximum number of children. They are regarded by parents as the most trusted source of information and, as the second most common location for going online, they provide children with a very important point of access.

7. Social networking service providers need to ensure that maximum protection is provided for the accounts of minors

7.1   If SNS age restrictions cannot be made effective, the de facto use of SNS by young children should be addressed so as to ensure age-appropriate protection.

7.2   Privacy/safety settings and reporting mechanisms should be far more user-friendly. If they remain difficult to use, privacy/safety settings should be enabled by default.

7.3 Digital skills to protect privacy and personal data should be strongly supported among children of all ages.

7.4 It should also be noted that one in three parents (51% of parents of 9-12 year olds, 15% of parents of 13-16 year olds) did not wish their child to use SNS.

7.5 The review of data protection legislation at a European level needs to be considered from the point of view of children's privacy.

8. Awareness-raising in relation to online risks should be balanced and proportionate, and targeted at those most at risk of harm.

8.1 Children are concerned about a wide range of online risks. Efforts to manage these risks, and to support children in coping with them, should maintain a broad and updated view of these risks.

8.2 As 9% of 9-10 year olds have been bothered or upset by something on the internet in the past year, it is important to promote awareness-raising and other safety practices for ever younger children.

8.3 Awareness-raising among teenagers and their parents and teachers remains a priority since upsetting experiences rise with age and the array of risks keeps changing.

9. Parental awareness of risks and safety online needs to be enhanced.

9.1 Without being alarmist or sensationalist, parents need to be alerted to the nature of the risks their children may encounter online. Awareness-raising should try to encourage dialogue and greater understanding between parents and children about young people's online activities.

9.2 Increasing parental understanding of risks is particularly important in those countries where awareness of children's risk experience is lowest.

10. Responses to young people's exposure to online sexual content needs to be proportionate and should focus on those most likely to be distressed or harmed by such exposure.

10.1 Although public concern over online sexual content is justified, the extent of children's exposure should not be exaggerated, and nor should it be assumed that all children are upset or harmed by such exposure.

10.2 Although the internet makes sexual content more readily available to all, with many children reporting exposure via accidental pop-ups, the regulation of more established media (television, video, magazines, etc.) remains important.

10.3 Private access also matters – children who go online via their own laptop, mobile phone or, especially, a handheld device are more likely to have seen sexual images and/or received sexual messages. Similarly, those who go online in their bedroom, at a friend's house or 'out and about' are more likely to see sexual content online. The early advice that parents should oversee children's internet use must be revised, and new safety tools are needed.

10.4 It seems that popular discourses centred on teenage boys' deliberate exposure to sexual content makes it harder for parents and others to recognise the distress that inadvertent exposure may cause girls, younger children and those facing psychological difficulties in their lives.

11. Sensitive responses to bullying are required with equal attention to online and offline occurrence.

11.1 In countries where there is more bullying overall, there tends to be more bullying online. This suggests that as internet use increases, so will bullying online. Thus anti-bullying initiatives should accompany efforts to promote internet use.

11.2 Online and offline bullying should be seen as connected, part of a vicious cycle in which perpetrators reach their victims in diverse ways and victims find it hard to escape.

11.3 Those who bully may also be vulnerable, and they are often victims themselves, so sensitive treatment is required.

11.4 Although children have a range of coping responses, cyberbullying upsets them, and more support and awareness-raising is needed. Fewer than half tell a parent or other adult, and fewer than half know how to block the person or delete their messages.

12. Parents need to be more aware of the practice of offline meetings with contacts first made online.

12.1 It is important to distinguish making new contacts online – a common occurrence – from going to meet new online contacts offline. It is equally important to recognise that for the most part, meeting online contacts offline is harmless, probably even fun.

12.2 But for a minority of children, meeting online contacts offline is harmful, and these children tend already to be the more vulnerable.

12.3 Since their parents are often unaware of what has happened, awareness-raising efforts should be increased so that parents of younger and/or more vulnerable children recognise the risk, but without this undermining the chance for most children to have fun making new friends online.

13. Policy makers need to be alert to new risks that affect children and young people, especially arising from peer-to-peer contact.

13.1 As well as conducting surveys, qualitative work based on listening to children is vital to learn what new risks they are experiencing.

13.2 Addressing risks associated with peer-to-peer conduct (user-generated content and personal data misuse) poses a critical challenge to policy makers.

13.3 While younger children have fewer resources to cope with online risk, they are also more willing to turn to parents for help. Meanwhile, teenagers face particular risks that worry them and that they may struggle with alone, so they need particular coping strategies and support.

14. Awareness-raising should highlight effective coping strategies in safety messages, emphasizing social supports such as talking to parents, friends and teachers, as well as the use of online tools.

14.1 Policy makers have long advised children to tell someone if they've been upset online, and it seems such messages have been heard.

14.2 Children try some proactive strategies more than others and few are fatalistic. This suggests a desire to cope as best they can and a readiness to adopt new technical tools if these are accessible.

14.3 When asked which strategies really helped the problem, children say that reporting the problem to an ISP was effective with sexual images but less so for sexual or bullying messages: this suggests that better solutions are needed for peer-to-peer risks.

14.4 Mostly, children said the approach they chose helped in up to two thirds of cases, but this leaves room for provision of better support and/or tools.

14.5 It seems that efforts to promote children's digital citizenship—in terms of online safety and good practice—are bearing some fruit, and should be extended. There may be many reasons why solutions children try, when upset, do not help the situation, but one possibility is that the technical tools are flawed or difficult to use, and another is that adults—professional or personal—are unprepared or unable to help children.

14.6 The 'knowledge gap' phenomenon—in which the information-rich learn from available advice and guidance more rapidly than the information-poor—means that efforts to promote digital citizenship will disproportionately benefit the already-advantaged. Targeting less privileged or more vulnerable children is a priority.

14.7 Overwhelmingly, children tell a friend, followed by a parent, when something online upsets them. Rarely do they tell a teacher or any other adult in a position of responsibility. Their apparent lack of trust in those who may have more expert solutions is a concern.

15. Practical mediation skills for parents should be a part of the overall effort to build awareness among parents of risks and safety online.

15.1 Parents appear to have got the message that it is valuable for them to engage with their child's internet use, and they employ a wide range of strategies, depending partly on the age of the child. But there are some parents who do not do very much, even for young children, and there are some children who wish their parents to take more interest. Targeting these parents with awareness-raising messages and resources is thus a priority.

15.2　Cynicism that what parents do is not valued, or that children will evade parental guidance, is ungrounded: the evidence reveals a more positive picture in which children welcome parental interest and mediating activities while parents express confidence in their children's abilities. It is important to maintain this situation as the internet becomes more complex and more embedded in everyday life.

15.3　Parental restrictions carry a significant cost in terms of children's online opportunities and skills, but they may be appropriate if children are vulnerable to harm. Parental efforts to empower children online seem to enhance their opportunities and skills, though there is little evidence that they reduce risk or harm. Since there are no easy answers, parents should be supported in judging what best suits their child.

16. Filtering technologies and parental control software need to be far more usable and transparent and take into account the needs of parents in order to improve uptake.

16.1　Across the 25 countries surveyed by EU Kids Online, less than one third (28%) of parents were found to filter the websites visited by their child. It is clear that many parents find them such software either too complicated or ill-suited to their needs.

To be effective, parental controls need to incorporate all of the issues that concern parents about their children's internet use. Thus, in addition to filtering out adult or unsuitable online content for children, controls may also need to include features such as the amount of time spent online, filtering of user-generated content and blocking of commercial content.

While there continues to be debate about the appropriateness of parental controls in all situations, they continue to be a valuable resource particularly for those who may lack skills or knowledge in advising on and guiding their children's internet use.

Parental controls are also available as an integral element of some internet services and do not need to be separately installed. An industry-wide agreement on the design and features of safety and parental controls built into web-based services could provide parents with better opportunities to consider adopting them. Training in the use of tools should also be made readily available to deal with lack of confidence and knowledge on the part of parents.

17. Levels of teacher mediation are high but could be higher, as a large minority of children are not reached by teacher guidance. Since schools have the resources to reach all children, they should take the biggest share of the task of reaching the 'hard to reach'.

17.1　The youngest children (9-10 years) report the least mediation from teachers: as this age group now uses the internet widely, primary schools should increase critical and safety guidance for pupils.

17.2　The benefits of supporting peer mediation are easily neglected but could be constructively harnessed, especially as children are most likely to tell a friend if something bothers them online. Peer mentoring schemes have a valuable role to play.

17.3　When something has bothered them on the internet, 36% of children said a parent helped them, 28% a friend and 24% a teacher. The ideal may for children to have a range of people to turn to, depending on the circumstances. A minority of children has no-one to tell when something upsets them.

18. Industry needs to be much more proactive in promoting internet safety awareness and education. In order to increase trust, the management of safety, identity and privacy settings of internet services used by children needs to be transparent and independently evaluated.

18.1　The overwhelming majority of parents would like to receive information and advice about internet safety. Most, however, get it from firstly from family and friends (48%) rather than from the providers of internet services. Traditional media (32%) and the child's school (27%) are the next most common sources of information about internet safety. Internet service providers (22%) and websites (21%) are much less evident as sources of advice.

18.2　There is considerable scope, therefore, for industry to improve its own awareness raising and provision of safety advice. Internet safety advice should be provided in an accessible and user-friendly way at the point of access on web services used by young people. Internet service

providers (ISPs) should play a more prominent role in providing online safety resources for parents as the primary account holders.

18.3 Traditional media sources – press, radio and television – also have a major role to play in promoting online safety awareness as supporting greater media literacy among the adult population. They are best positioned to reach all adults and, crucially, are influential in forming parents' attitudes towards opportunities and risks on the internet.

18.4 Evidence repeatedly shows that children still struggle with user tools, safety devices, privacy settings and policies, reporting mechanisms, etc. even though the industry claims they have been improved and made easier. Independent evaluation of progress by the industry is crucial, to measure whether improvements have been made (against benchmarks) but more importantly, whether those improvements work - i.e. are they actually sufficient for children to manage their safety, privacy, identity and risk online?

September 2013