Comments on the House of Lords Science and Technology Committee's 5th Report of Session 2006-7 on Personal Internet Security

1. The Children's Charities' Coalition on Internet Safety (CHIS) very much welcomes and endorses the broad sweep of the conclusions and recommendations of the House of Lords Committee on Science and Technology in their 5th Report of 2006-7, on Personal Internet Security.

2. We agree with the idea that changes need to be made in the way data is collected on crimes so as to indicate whether or not an internet enabled device e.g. computer, mobile phone, games console, or TV, played a significant part in the origination or commission of the offence. At paragraph 8.3 the Select Committee refers to "e-enabled crime". CHIS thinks that term is rather apt.

3. A new symbiosis appears to be emerging between the real and the virtual worlds. Children's and young people's online behaviour is both being shaped by and in turn is shaping their online and their offline conduct.

4. While much of this new behaviour is likely to be positive, some of it is very unlikely to be. For example, the relative anonymity of the internet appears to be making certain forms of inappropriate sexual banter more commonplace in cyberspace, but increasingly this is spilling over into real world situations e.g. the playground.

5. Forms of bullying and a growing culture of making and distributing inappropriate images also seem to have been fed by trends in cyberspace, perhaps feeding off and at the same time feeding into a contemporary growth in so-called "Reality TV" where everyone can get their 15 minutes of fame, particularly if they do something outrageous or gross.

6. For very many children and young people today the real and the virtual worlds are becoming a seamless whole which they inhabit with great and equal ease. It is hard, if not impossible, to say where the influence of one medium begins and the other ends. Moreover there could be both practical and ethical obstacles to testing or proving some of the concerns or hypotheses which are increasingly being expressed. However, where there is any reasonable doubt

CHIS would suggest that public policy ought to err on the side of caution with respect to children and young people.

7. There is consequently a clear need for systematic and sustained monitoring or research into the forgoing and also into other possible harms to children, falling short of being specific crimes, which the new technologies are bringing in their wake e.g. into the way the internet seems to have enabled prolonged and persistent exposure to certain kinds of sexual imagery. It would be useful to know more about the possible longer term consequences of this phenomenon in terms of how it might be shaping the attitudes of today's children and young people towards sex and sexuality.

8. At paragraph 8.7 the Select Committee asks for a reappraisal of the "end-to-end-principle". They say (paragraph 8.8) "The current assumption that end users should be responsible for security is inefficient and unrealistic." The implications of this statement are truly radical but they are implications which CHIS wholeheartedly supports.

9. Essentially the Select Committee is saying that, through their lack of knowledge, even a small number of end users can compromise the integrity of the internet as a whole (and that is unacceptable to wider society). Through their lack of knowledge of the online hazards to children, parents can similarly also put their children at risk. That too is unacceptable. CHIS shares the Select Committee's view that one way of dealing with this situation might be to re-examine the legal liability of the vendor (paragraph 8.15).

10. There are several large manufacturers and retailers who aim squarely at the domestic market. As part of their sales pitch, they extol the educational and other advantages which having ready access to the internet at home can bestow on children. Yet at the moment, when a hardware vendor sells an internet enabled device into the domestic market, to a parent or guardian for use by a child, they are trusting to luck that the parent or guardian

   a. will know or find out that there are safety related issues which ought to be addressed in relation to their child's use of the device

   b. will know or find out what needs to be done to address them

   c. will actually do them

   d. will do them properly

   e. where appropriate will maintain them and

   f. where a financial cost is involved, that they will be able to afford it

11. As Professor Sonia Livingstone's study "UK Children Go Online", (LSE, 2004), and other studies have shown, the reality is very different for huge numbers of parents. That is precisely why CHIS has advocated that all new internet enabled devices sold into the domestic market should come with child

safety software preinstalled and set to the highest appropriate level of security. In fact this is currently the basis of a campaign by NSPCC to ensure that all new machines on the UK market have internet safety preinstalled and set to a high level of security. The campaign is based on an online petition which so far has attracted over 45,000 signatures.

12. Using technical measures, such as child safety software, is by no means a complete answer to keeping children safe when they go online, but in CHIS's view it offers a great deal.

13. The best protection a child can possibly have is their own knowledge and awareness of the hazards of the internet: what they are and how to avoid them, or how to handle them should they nonetheless present themselves for whatever reason.

14. However, technical solutions can play an important part in helping to protect children, perhaps particularly younger children, by blocking access to certain areas of the internet or by filtering out certain types of content or contacts. Many safety packages these days also contain a range of tools that can help parents or guardians to monitor their child's use of the technology or predetermine the amount of time the child might spend on it.

15. Technical solutions such as safety software can therefore help reduce the level of risk, although they will never eliminate all risks completely. They can also be adapted over time to reflect the evolving capacities and development of children and young people as they move towards adulthood.

16. Pre-installing safety software in the manner described is intended to create a safety net. It is meant to underpin and reinforce exactly the same values and patterns or modes of behaviour which parents and guardians are anyway seeking to encourage in their children and which the internet companies are trying to encourage in their customers.

17. Moreover if the safety issues are presented appropriately at the point of sale, at the moment when the device is turned on for the first time, or the service is first accessed, that in itself can be an extremely valuable learning opportunity for both child and parent or guardian alike.

18. At the point of sale, or from the moment the machine is turned on for the first time, the device itself should be as safe as it possibly can be. If a parent or guardian wishes subsequently to vary the safety software settings or components they should, of course, be free to do so. But they should not have to go through hoops to make it as safe as it can be in the first place.

19. Vendors might object that this will inevitably lead to an increase in calls to their help lines, as some people struggle to vary or understand the settings. However, CHIS considers it is far preferable that people have to struggle to make something less safe than they have to struggle to make it safer.

20. What role should ISPs have in these matters? They are, after all, the companies that actually provide the internet connectivity?

21. The old idea of an ISP was of a company that only or principally provided connections to the internet. There are fewer and fewer such companies. These days, particularly within the domestic market, internet connectivity often comes bundled with a piece of hardware so, for very many people, buying the hardware and obtaining access to the internet are really all part of the same process or transaction. With mobile phone and TV companies increasingly moving into the same space that ISPs used to occupy, this multi media convergence is becoming a daily, and often bewildering, reality for millions of people in all kinds of households.

22. To the extent that a company is involved in providing internet access to the domestic market, either as a stand alone product or as part of a larger offering, the internet component should always be provided, by default, with safety software pre-installed and set to the highest appropriate level of safety.

23. It is important to bear in mind that there can be a high rate of "churn" within this market i.e. large number of people who switch between internet access providers. However, if all companies providing internet access follow the same policy in relation to default safety settings, the rate of churn becomes an irrelevant consideration in this context.

24. Then there is the role of companies or organizations that provide key services on the internet but are not necessarily involved in any way in providing access or connectivity e.g. social networking sites. What responsibility do they have?

25. In such cases CHIS would once again advocate that greater security be provided by default, so that at the point where the service or device is first turned on, or when the site is first accessed, the relevant safety settings are fixed at the highest appropriate level.

26. The risk with turning on safety settings by default is that, in a sense and among other things, it may give parents a false sense of reassurance. It might mean many parents never trouble to find out anything at all about internet safety, so if something unexpected happens later they will flounder. Parents might start to believe that the machine or service is guaranteed to be 100% safe all of the time so they just dismiss the issue from their minds believing they never have to think or worry about it again. All of these things are bad and undesirable, but the opposites are worse.

27. It is also very important that pre-installing safety software is not seen as being an alternative to reaching out to parents and educating them about risks. Pre-installing safety software is something that needs to be done in addition.

28. Pre-installing safety software is also not an alternative to continuing to reach out to and educate children and young people themselves about the hazards of the internet and about the importance of behaving appropriately when online.

29. The only company in the UK CHIS knows about that has ever followed the sort of approach suggested here is Comet, the electrical retailer. They preinstalled a safety package on their own brand machines in such a way as to make it an unavoidable first screen following the machine's initial boot up.

30. In discussions with computer manufacturers CHIS learned that, within the manufacturing process, the cost of doing the pre-installation was so small it was impossible to compute. At the time, the reasons given by other manufacturers or suppliers for not doing pre-installation were either commercial e.g. the makers or vendors of the devices wanted to agree revenue sharing terms with the companies selling safety products before they would agree to put them on to their machines, or they were to do with the absence of an officially recognised standard i.e. the makers or vendors did not want to be put in the position of having to choose or decide what was a "good" software package and what was a "bad" one. When the joint OFCOM-Home Office safety software kitemark project is completed, at least that part of the dilemma will have been resolved. The completion date is expected to be in or around late November, 2007.

31. CHIS also supports the idea of developing a kitemark for secure ISPs (Recommendation 8.8) and the notion that in the longer term ISPs' liabilities ought to change to make clear their central role in maintaining the integrity of the network (Recommendation 8.10).

32. CHIS further considers that all ISPs should be blocking access to child abuse images and this has been the basis of a recent campaign by NSPCC. CHIS and the NSPCC will continue to work to ensure that all UK domestic and business ISPs are blocking access to such images.

33. On a broader point the Committee's reference to changing the "mere conduit" status of an ISP (paragraph 8.10) opens up a discussion of an aspect of the E-Commerce Directive which CHIS believes is very unsatisfactory.

34. One purpose of the E-Commerce Directive was to put ISPs and web based companies into a position similar to that already enjoyed by telephone companies. The fact that a bad person did something criminal over a BT line did not mean that BT was an accessory. They could not have had any knowledge of what the criminal was doing. However, if BT became aware of the way in which their line was being unlawfully abused, and they chose not to do anything about it, or they failed to act reasonably promptly to curtail the unlawful activity, then they could become liable.

35. Under the E-Commerce Directive ISPs and web based companies were given similar protection e.g. if child abuse images, or something that was defamatory of a third party, were posted on a website, that alone would not make the ISP liable for it. Once notified, however, the ISP was expected to remove the offending item reasonably promptly or else risk becoming liable as a knowing publisher of the material. The key thing was that ISPs could only be liable if it could be shown that they had actual knowledge of the material

complained of. They were deemed to have that knowledge once properly notified of its existence.

36. However, some judicial comment in the UK and elsewhere has suggested that where an ISP or web based company chooses "to police" its own site, by looking for undesirable material which it believes breaches its terms of service, then they in effect become the publisher of everything that remains. The assumption is that if they haven't removed it, they must have approved it. This shows a lack of understanding of how ISPs and web based companies operate. It has also had the perverse effect of introducing an incentive for ISPs and web based companies to do nothing.

37. If a company does nothing, and simply waits to be notified of any unlawful material on its site, it can never be liable for it. On the other hand if a company proactively tries to root out such material it could end up in court. CHIS is aware that, for these reasons, many corporate lawyers have advised their clients not to police their sites proactively, and some of their companies have accepted this advice. In other word the E-Commerce Directive provides an alibi for inaction.

38. CHIS strongly suggests that the UK Government engages with the EU to amend the E-Commerce Directive in such a way as to make clear that, for any liability to arise, it is still necessary to show actual knowledge or agency. Companies that make good faith efforts to enforce their own content standards on their web sites or services must be given a safe harbour against potential claims of criminal or civil liability.

39. CHIS supports the notion (Recommendation 8.23) of developing a kitemark for social networking web sites. The Good Practice Guide being developed within the Home Office Taskforce subgroup on social networking services could provide the basis of a kitemark of this kind.

40. As will be evident from earlier remarks, CHIS entirely agrees about the importance of finding new and better ways of reaching out to parents and guardians to help them gain a better understanding of online security and safety (Recommendation 8.24) so that they can, in turn, better support their children. While schools must play a key part in such an initiative, for this idea to work it will be important not to rely solely on schools, particularly in relation to the parents of secondary school children and young people. In that connection it might be important to emphasise to parents and guardians just how much they themselves might benefit from improving on or increasing their own knowledge of the internet.

41. While the Select Committee did not refer directly to the situation within schools, or what was happening in the education sector generally, there is one very recent development which ought to be referred to here because it adds considerable moment to some of the Select Committee's wider observations.

42. Every state school in England now has broadband access to the internet. Within schools the risks associated with internet use are addressed by a range

of technical, educational and other provisions and policies which have been in place and developed over several years.

43. The internet is increasingly being integrated into all parts of the curriculum. It is now widely considered that children and young people who do not have ready access to the internet at home are increasingly at an educational disadvantage. There is a growing body of evidence which appears to show that children and young people who learn within an internet rich environment are enhancing their grades and with that their life opportunities.

44. A central idea of the "Home Access Initiative" initiative, which is currently being developed within DCFS, is to ensure that every child engaged in education has ready and convenient internet access at home. A range of estimates exist which give various approximations of the numbers of children and young people who do not have internet access at home at the moment.

45. Households with children and young people in them are much more likely to have internet access than households without children and young people in them. In 2004, according to the ONS, around 50% of all households in the UK had internet access. In her study, "UK Kids Go Online", also carried out in 2004, Professor Sonia Livingstone found that around 71% of households with 9-19 year olds had internet access. In 2007, according to the ONS again, 61% of all households now have internet access so it is likely that the proportion of households with children that have internet access has also risen in line with this trend, but there still remains a significant gap.

46. In delivering the "Home Access Initiative" the Government accepts it has a responsibility to establish an appropriate safety framework for children and young people who will benefit from it. The initiative will potentially benefit all children in all families, but an early priority will be given to ensuring that among the first to gain will be those children and young people in families where, currently, there is no internet connectivity of any kind at home. Many of the families who fall into that category will also be among some of the most excluded groups in society so the importance of the safety aspect of the initiative is self evident.

---ooo---

John Carr
Secretary
Children's Charities' Coalition on Internet Safety
c/o NCH
85 Highbury Park
London N5 1UD

Tel 07717 512247
Email john.nch@btopenworld.com