

Submission to the Joint Select Committee on Cyber-Safety by Electronic Frontiers Australia

Introduction

It is generally agreed that as well as for parents and educators, it is appropriate for government to offer guidance to the community about keeping children safe online. To this end, various Australian governments are allocating resources to investigating the best ways to do this, or funding actual programs such as the CyberSmart portal for children and parents.

Electronic Frontiers Australia does not disagree that government has a role to play. Of course, any resources spent on cyber-safety are not available for other purposes, such as other educational needs or safety programs. It is then always appropriate to ask: are the resources allocated commensurate with the risks to children? Other submissions and testimony the Committee will receive will doubtless canvas the harms that can befall children online. These harms are often presented as anecdotes, such as reports in the media of terrible things that have happened to individual children, or instead merely take for granted that the harm suffered by certain activities is grave. We do not question that children face risks and harms online, but in this submission do wish to bring the focus back to solid evidence-based policymaking.

Electronic Frontiers Australia was conceived as a civil liberties organisation, and throughout our history we have often found ourselves opposing attempts to regulate the Internet that are predicated on protecting children. We take no issue, however, with seeing that Australia's young people are equipped with the skills and tools they need to become safe and active online citizens. We support any cyber-safety initiative that is consistent with the research - that is to say, consistent with the actual benefits and harms experienced by young people online.

To this end, in this submission we wish to bring to the Committee's attention some relevant data, and pose the question: how do we quantify the risks to children online? Any serious attempt to improve cyber-safety programs must bear this question in mind.

About EFA

Electronic Frontiers Australia Inc. ("EFA") is a non-profit national organisation representing Internet users concerned with on-line rights and freedoms. EFA was established in January 1994 and incorporated under the Associations Incorporation Act (S.A.) in May 1994.

EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting online civil liberties. EFA members and supporters come from all parts of Australia and from diverse backgrounds.

Our major objectives are to protect and promote the civil liberties of Internet users and of those affected by their use and to educate the community at large about the social, political and civil liberties issues involved in the use of computer based communications systems.

EFA policy formulation, decision making and oversight of organisational activities are the responsibility of the EFA Board of Management. The elected Board Members act in a voluntary capacity; they are not remunerated for time spent on EFA activities.

EFA has presented written and oral testimony to State and Federal Parliamentary Committee and government agency inquiries into regulation of the Internet and online issues.

Risks and Harms

Some of the best research to date on the risks to minors online has been conducted by the EU Kids Online project¹. Their recent report, "Risks and safety on the internet", is based on a survey of 25,142 European children between 9-16 years of age and their parents. It is perhaps the first, and certainly the most rigorous, attempt to properly assess and quantify the *harms* experienced by children as well as identifying the *risks* inherent in using the Internet. The report's authors point out that in many aspects of life, we tolerate a significant amount of risk to children as it is outweighed by the perceived benefits, and gives children the opportunity to grow and explore; they cite the example of cycling by analogy. It is useful to bear this analogy in mind when putting the risks of online activity into the correct context.

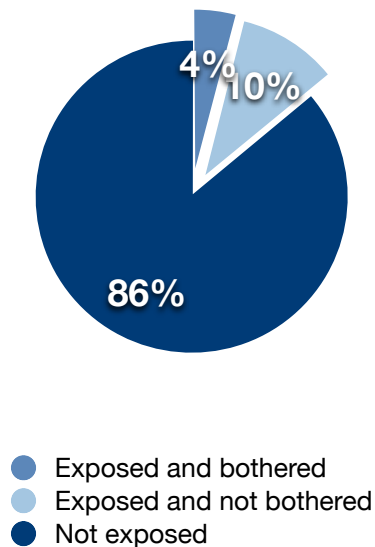
¹ <http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx>

Here we present a summary of some of the report's findings, as an illustration of how valuable a focus on harms can be in directing both research and resulting policy.

Exposure to inappropriate content

Much of the discussion of cyber-safety revolves around the potential exposure of children to inappropriate material, particularly pornography and violent images. There's no question that the internet makes access to such material easier. A report from the Internet Safety Technical Task Force, on behalf of the USA's attorneys general, did point out that "The Internet increases the availability of harmful, problematic and illegal content, but does not always increase minors' exposure."² Other research also indicates that offline exposure to such material is still common.³

Fig. 1: Exposure to sexual material online



A reasonable amount of research has been done into the incidence of such exposure. An Australian study estimates that 84% of boys and 60% of girls in Australia have been accidentally exposed and 38% of boys and 2% of girls deliberately exposed.⁴ This is significantly higher than the numbers reported in the EU Kids Online study, and so probably reflect significant methodological differences. The European numbers report that 14% of 9-16 year olds have seen sexual material online in the previous 12 months.⁵

Either figure represents a significant fraction of internet-using youth, and suggests that the risks to children of exposure to pornography are significant. This probably doesn't count as much of a significant revelation. An appropriate policy response, however, should take into account the harms that this risky behaviour could bring about. Is exposure to inappropriate material harming children?

² Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force (ISTTF) To the Multi-State Working Group on Social Networking of State Attorneys General of the United States, p. 5

³ Risks and Safety on the Internet: The Perspective of European Children (EU Kids Online) p. 49

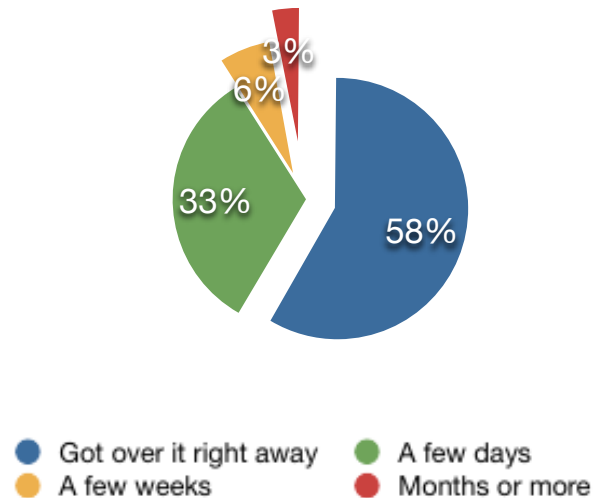
⁴ Dooley, J.J., Cross, D., Hearn, L., Treyvaud, R. 2009. Review of existing Australian and international cyber-safety research. Child Health Promotion Research Centre, Edith Cowan University (ECU), Perth. p. 11

⁵ EU Kids Online. p. 50

This question not something that can be ethically explored in scientifically controlled conditions, but the *EU Kids Online* study did ask children whether they were bothered by such exposure, how much it bothered them, and for how long.

Approximately one third of children exposed said the exposure had bothered them, equivalent to about 4% of the children surveyed. Of those, 56% said that they were “not at all upset” or “fairly upset” by the experience. And they recovered quickly - 59% of children bothered by the experience reported they “got over it right away”, with only 9% reporting that it bothered them long-term. To summarise: Of the 25,142 children surveyed, 0.36% reported an experience that was upsetting and bothered them for more than a few days.⁶

Fig. 2: Bothered by exposure - for how long?



This suggests that a cyber-safety initiative focusing heavily on blocking and filtering is likely to be counter-productive. Instead, education and resources that would help those children better cope, and equip all children to could likely be more effective. Of the children who were bothered, only 22% “tried to fix the problem”⁷; it seems likely that a properly focused campaign could significantly increase this number.

Cyber-bullying

Another high-profile cyber-safety issue is that of online bullying. This is often considered to be the most directly harmful to children, as most of us have some experience with the trauma of childhood bullying. Several tragic cases of suicide by young people who experienced such bullying has helped drive this point home.⁸

Once again, the research in this area is improving. The data does not support the notion that there is an epidemic of cyber-bullying, but would rather seem to confirm that online bullying is simply a subset and different facet of regular real-world bullying.

⁶ EU Kids Online, pp. 49-60

⁷ EU Kids Online, p.59

⁸ For instance, Megan Meier: http://en.wikipedia.org/wiki/Suicide_of_Megan_Meier

Of the children surveyed by EU Kids Online, 6% reported receiving hurtful or nasty messages online.⁹ This contrasts with 19% who say such behaviour has occurred offline.¹⁰ In the Australian context, research so far suggests that the numbers are similar, with the Edith Cowan University literature review quoting a figure of “less than 10%” for Australian children and cyber-bullying.¹¹ In the EU study, only 5% of children surveyed indicated they are bullied more than once a week, whether online or off.¹²

6% is still a significant number of children, which is to say most children would appear to be at risk of experiencing cyber-bullying. But once again, can we quantify the harms - how damaging is the experience to children? The EU data is again revealing, and indicates that bullying is a reasonably upsetting experience. 55% of children surveyed indicated that the last time they received a nasty or hurtful message online, they found the experience “very” or “fairly” upsetting. Only 15% reported that they were not at all upset by the experience. However, the children reported being reasonably resilient. 62% of those bullied reported that they “got over it right away”, with a further 31% remaining upset for a few days - only 8% reported long term effects, or 0.48% of the total number of children surveyed.¹³

It would appear that these children were able to cope fairly successfully with the problem, and they were asked about their coping strategies. 36% of children reported that they “tried to fix the problem”, whereas 24% hoped the problem would go away by itself (which, the report notes, may be a sensible response). 46% of children reported blocking the person who sent them a hurtful message, and 41% deleted the offending content, numbers which suggests children are already far from powerless.¹⁴

Encouragingly, 77% of those bullied reported that they talked about the incident with somebody - 52% with a parent, 52% with a friend, and 16% with a teacher or other adult.¹⁵ This may partly explain why 6% of parents reported that their children had been bullied on the internet, with 6% of children self-reporting the same thing.¹⁶ (However, the agreement between parents and children’s accounts may be highly correlated since the vast majority of both parents and children said that bullying had not occurred.)

⁹ EU Kids Online, p. 62

¹⁰ *ibid.*

¹¹ ECU p. 11

¹² EU Kids Online, p. 61

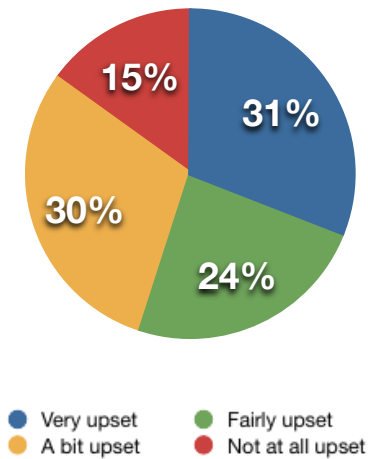
¹³ EU Kids online pp. 61-72

¹⁴ *ibid.*, p. 70

¹⁵ *ibid.* p. 71

¹⁶ *ibid.*

Fig. 3: Online bullying - how upset?

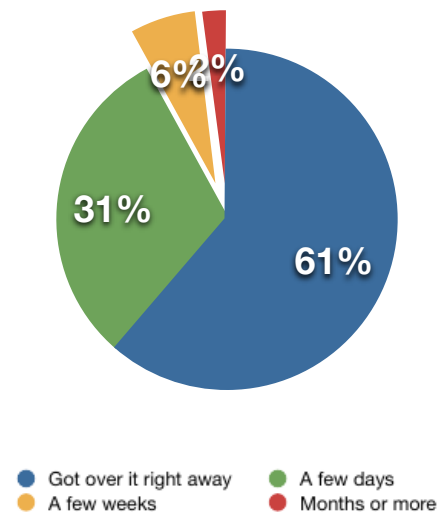


This data leads to some encouraging conclusions. Most significantly, it appears kids are willing to seek help if available. This would suggest, for instance, that Facebook’s recent addition of a “social reporting” feature, which enables children to safely communicate with a potential bully or to report content to a trusted adult, is likely to be effective.¹⁷

Most importantly, it would be a mistake to tackle cyber-bullying in isolation. When online bullying occurs, it is likely an extension of something occurring offline, for instance in the schoolyard. (In Australia too, research

suggests that victims of online bullying know the perpetrator.¹⁸). While it may not be true of adults who came of age before the advent of the Internet, children do not draw a clear distinction between the online and offline worlds. Cyber-bullying is bullying, and will never be eliminated until schoolyard bullying itself is - no easy task. Once again this suggests the focus should shift away from technical measures and more on education and resources for parents and teachers.

Fig. 4: Online bullying - how long upset?



Implications for Policymaking

Keeping children safe, whatever the context, is something our society values greatly. Any perceived threat can generate considerable anxiety and instant momentum for decisive action. Which action to take, however, should be based on an actual assessment of the harms incurred. A different response is warranted if children are being traumatised or placed in physical danger, than if they are temporarily bothered by something they encounter online.

¹⁷ <http://latimesblogs.latimes.com/technology/2011/04/facebook-rolled-out-a-few-new-security-tools-on-tuesday-that-aim-to-improve-how-users-to-report-bullying-fake-profiles-and-o.html>

¹⁸ ECU p. 11

Investigating the harms visited upon children is obviously difficult, but asking the children themselves about their experiences gives us the best data we can reasonably hope for. It may be counter-intuitive to some, but the evidence suggests that children are quick to recover from upsetting experiences online, and are ready and willing to seek help when these experiences are sufficiently upsetting.

It is also important to note that when the risks are not too high and the harms manageable, significant benefits can accrue. Young people need to be able to explore on their own, and a moderate amount of risk-taking is a normal and healthy way of developing resilience and growing into confident citizens online and offline. With any new friendship comes the possibility of hurt and betrayal (as young people well know), but it certainly doesn't follow that children should be protected from getting to know their peers.

Using the Internet is inherently safe, as sitting at a keyboard carries no significant physical risks. We therefore suggest that the default attitude to cyber-safety issues should be focussed on allowing minors the freedom to learn, play and make friends while equipping them with the means to get help and advice when they seek it out. Measures which are overly restrictive or censorious, technologically-focused, or concentrated solely on the online experience are likely to be ineffective at best and harmful at worst.

In particular, it is universally acknowledged that exposure to pornography, hate speech, or violence online is a danger children should avoid. Does it follow that all such material should be banned? Doing so would be a technologically complex and highly expensive endeavour, likely to fail. If the evidence suggests that children who encounter such material and are disturbed by it are able themselves to block or ignore it, and recover just as quickly from the experience, then a better approach would be simple education so children are empowered to do this with confidence and assurance. When it comes to such content risks, we believe that this is indeed what the evidence shows, and that education is the preferred response.

We therefore suggest that promising areas for further investigation and resourcing would include:

More research in the Australian context to quantify the risks and harms online;¹⁹

¹⁹ We understand that researchers at Edith Cowan University are planning a limited replication of the methodology of the EU KIDs Online study locally.

Evidence-based policymaking requires evidence; working with industry to develop tools to empower children and parents, and to provide safe environments and age-appropriate content;

Adequately resourcing schools, including enhancing their ability to provide resources to parents and digital skills to students.

Conclusion

Recent evidence suggests that it is possible to measure both the risks - the chances of exposure to undesirable experiences - and the harms which children face online. Analysis of these risks and harms would suggest that:

- Children are more resilient than we might think when it comes to upsetting experiences online, with only a tiny minority of children reporting long-term upset.
- A focus on technological measures is likely to be ineffective.
- Children, if properly equipped and educated, will reach out to parents and other adults when they need help.
- Especially with regards to social risks such as cyber-bullying, treating the online and offline aspects of the problem differently is likely to be counterproductive.

In summary, children should be encouraged to take an active role in managing their own safety and thereby growing into competent online citizens. EFA supports any measures that help and support our kids to do just that.

Should the Committee require any further input we would be happy to answer questions.

Colin Jacobs

Chair

On behalf of the EFA Board of Management